HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

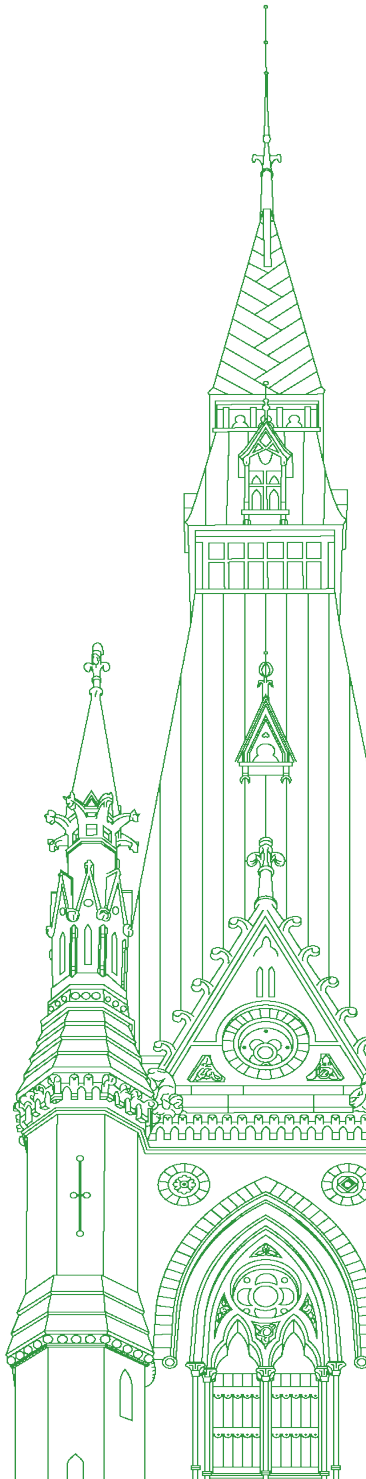
Standing Committee on Science and Research

EVIDENCE

NUMBER 066

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Wednesday, November 22, 2023



Chair: Mr. Lloyd Longfield

Standing Committee on Science and Research

Wednesday, November 22, 2023

● (1630)

[*English*]

The Chair (Mr. Lloyd Longfield (Guelph, Lib.)): I call the meeting to order.

Thank you, everyone, for being here—especially our witnesses.

Welcome to meeting 66 of the Standing Committee on Science and Research.

Today's meeting is taking place in a hybrid format, pursuant to the Standing Orders. Members are attending in person in the room and also remotely on Zoom.

I would like to make a few comments for the benefit of the witnesses and members.

Please wait until I recognize you by name before speaking. For those participating by video conference, click on the microphone icon to activate your mike, and when speaking, please speak slowly and clearly.

When you're not speaking in the room or on Zoom, your microphone should be turned off or on mute, and for the benefit of the interpreters, please keep your earpieces away from the microphone, because that can cause injury through feedback, and we certainly don't want to do that. We want to make sure our interpreters are as healthy as they were when they came here.

I remind you that all comments should be addressed through the chair.

Pursuant to Standing Order 108(3)(i) and the motion adopted by the committee on Tuesday, June 6, 2023, the committee resumes its study on the use of federal government research and development grants, funds and contributions by Canadian universities and research institutions in partnerships with entities connected to the People's Republic of China.

It's now my pleasure to welcome, from the Canadian Security and Intelligence Service, David Vigneault, the director of CSIS, and Nicole Giles, senior assistant deputy minister, policy and strategic partnerships. Welcome back.

From the Department of Public Safety and Emergency Preparedness, we have Shawn Tupper, deputy minister, and Sébastien Aubertin-Giguère, associate assistant deputy minister, national and cyber security. You're in a supporting role for Director Vigneault.

Director Vigneault, you have six minutes for your opening remarks, after which we will proceed to our rounds of questioning.

The floor is yours for six minutes, please.

[*Translation*]

Mr. David Vigneault (Director, Canadian Security Intelligence Service): Thank you very much, Mr. Chair.

Members of the committee, good afternoon.

It is an honour to join you today and to have the opportunity to contribute to your important discussion on the use of federal funds in partnerships with entities connected to the People's Republic of China.

My goal today is to supplement the testimony given by my colleague a few weeks ago on what we do at the Canadian Security Intelligence Service, or CSIS, to ensure the security of Canada's research against foreign threats in Canada.

[*English*]

As this committee is well aware, academia and the research sector are often targeted by foreign threat actors seeking to advance their interests at our expense.

This can take many forms, from covertly influencing research agendas or peer review processes to engaging in funding arrangements in which details about the source of funds are deliberately obscured or misrepresented. Through perceived partnerships and collaborations, vital research and novel intellectual property is stolen. The PRC is by far the greatest perpetrator of these activities.

These examples evidence an evolution of the threat landscape, as they starkly differ from historical attempts at foreign interference, which would exclusively target government officials and institutions.

With private industry and research now holding valuable intellectual property and potential for economic prosperity, threat actors have shifted to include non-government targets in their foreign interference campaigns.

I recently reflected on how we are working collaboratively with universities during a panel discussion at Stanford University, where I recalled my first meeting with universities five years ago.

Going into that first meeting, there was discomfort on openly engaging with CSIS, but we have come a long way from these first meetings, as after continued and genuine engagement, these institutions now proactively reach out to the service for ways to work together to protect research security and to counter foreign interference threats, demonstrating the evolution of our relationship.

CSIS is committed to maintaining these strong lines of communication for the benefit of our partners and Canadian national security interests.

[*Translation*]

In 2022 alone, CSIS conducted 113 stakeholder engagement activities and met with representatives of academia, community organizations, civil society, advocacy associations, research and innovation institutes and Indigenous leaders, as well as representatives of provincial and municipal governments. CSIS has also presented at a number of academic conferences, and has held various in-person briefings and workshops on university campuses.

These relationships have proven critical to building national security literacy and resiliency in the increasingly complex threat landscape that we are facing here in Canada. CSIS provides non-secret security briefings and mitigation strategies to university officials and faculty on the threat environment, and research institutions share their concerns, which inform our strategies to counter threats.

. I am confident that the strength of these relationships will be our best defence against the aggressive and coercive attempts at foreign interference that we are seeing today, and that we will undoubtedly continue to see in the future.

● (1635)

[*English*]

Unfortunately, this activity only grows in sophistication as states seek to exploit Canada's open and collaborative research ecosystem for their own interests, to the detriment of Canada's.

Needless to say, as state actors become more sophisticated, these threats become harder to counter. It is therefore imperative that Canadians work together. This effort begins with informed and trusted discussions among communities, academia, business and governments at all levels.

In order to remain a committed partner in this effort, CSIS will continue to leverage its authorities under the CSIS Act to investigate, provide advice to the government and, where appropriate, take measures to reduce these threats.

CSIS will also continue to invest in significant efforts in building relationships with individuals, communities and institutions to establish and sustain trust and to offer support and partnership in protecting Canada's national security and future prosperity.

I will conclude by noting that in order to protect the safety and security of Canadians, I cannot publicly comment on operational matters and requirements. Nonetheless, I would welcome this opportunity to have a frank and open discussion and to try to elucidate any of the questions you may have with my colleagues present here.

[*Translation*]

Thank you.

[*English*]

The Chair: Thank you, Director Vigneault, for coming, especially given the circumstances we're facing today. It's great to have you here.

I hope we can get full rounds of questions in on this, because we've all been very anxiously waiting for you to come here.

We will move over to Mr. Tochor for the first six minutes, please.

Mr. Corey Tochor (Saskatoon—University, CPC): Thank you, Director Vigneault.

On Monday I asked Minister Champagne if he agreed with the expert witnesses we heard at this committee who said that since 2017 the PRC's activities in the sector have come to represent an existential threat to Canada, but the minister, unfortunately, would not accept this position. Do you view the PRC's activities as an existential threat to Canada, yes or no?

Mr. David Vigneault: The role of CSIS is to advise government on threats to national security. We look at all vectors of how these threats can manifest themselves. We have been more open publicly, specifically about the PRC's activities, but also about other threat actors in terms of the impact on our sovereignty and our security and future prosperity.

From that point of view, I think the People's Republic of China has been very clear in their intent, and their actions have demonstrated the level of their capability to be a threat to our national security as well. I would say that indeed the PRC is one actor that represents a threat to the country.

Mr. Corey Tochor: By definition, then, would that be a threat or an existential threat?

Mr. David Vigneault: Mr. Chair, I understand the member's question. In my position I don't make the distinction between a threat or an existential threat. I have said publicly, and I repeat it here, that the PRC, in the context of a threat to our economic security and research security, is by far the most sophisticated actor that we're dealing with.

Mr. Corey Tochor: Mr. Vigneault, that's deeply troubling. You've recently made unprecedented appearances, along with other Five Eyes allies, that have been characterized by the media as “because they're alarmed by China which they say is the greatest espionage threat democracy has ever faced”. Those were your words or your signature on a Five Eyes document—if I'm speaking correctly on that—specifically referring to the theft of our technology and secrets.

If you're willing to say with the other Five Eyes that this is an existential threat, I'm concerned that you're not sharing that view domestically, versus the international statement that you guys put out—

Mr. David Vigneault: Mr. Chair—

Mr. Corey Tochor: —or should it be the role of the minister to say whether, with the briefings you would have provided, this is an existential threat or not?

Mr. David Vigneault: Mr. Chair, I think that's a very valid a point. I would not want to leave the impression that I would have messages in Canada that were different from messages abroad. I think the context of the Five Eyes message, which was unprecedented—it was the first time in history that we appeared in public together—was to essentially send that signal. Those words were chosen carefully to say that, so I do fully endorse, of course, what I'm saying.

In the context of the work that we do in Canada, in the context of what CSIS's role is in advising government, and to complement what the minister said in his appearance on Monday, I do not see a distinction. I understand that these are not necessarily the same words, but I do stand by the statement that I've made with my colleagues about the threat that China represents.

● (1640)

Mr. Corey Tochor: Have you personally briefed the minister on the activities of the PRC?

Mr. David Vigneault: Mr. Chair, I'll be careful about the nature of the briefings I'm giving, but I do believe that it has been said publicly that I have personally briefed Minister Champagne. I have briefed a number of other ministers. I'm saying that with the caveat that I cannot confirm or deny all of the briefings I've given. However, in the context here, it's been said that, yes, I have briefed Minister Champagne directly in the past.

Mr. Corey Tochor: If both you and Minister Champagne won't pronounce this as an existential threat, who will? Obviously the minister also has all the information that you have on the activities of the PRC. Would that be a rough generalization?

Mr. David Vigneault: Mr. Chair, the minister is receiving a lot of information, of course, mostly from his department. He's also receiving information through his participation in different committees, and that includes receiving intelligence from CSIS.

I do understand the member's question. Again, I just want to reiterate that I think the words I've used in this committee in my opening remarks and the words we've used in our public report and in previous public appearances here in Canada have spoken very clearly about the magnitude.

I may not have used the term “existential threat”, but I can tell you that we are seeing it from that point of view. If the chair is indulgent, I would say that one of the issues we have to be very clear about is that the PRC, under the leadership of Xi Jinping, has essentially created an environment in which all of the resources of the state have been combined under the leadership of the chairman to essentially create the tools for the PRC to succeed. That, indeed, includes—

Mr. Corey Tochor: I'm going to run out of time here shortly.

I have one last question that I do want to get the answer to: Do you believe that all entities associated with the PRC should be banned from receiving taxpayers' money through research grants at universities in Canada? Give me a yes or no.

Mr. David Vigneault: Mr. Chair, I think what is important is to look at the threat specifically. I would say that there is a gradation in terms of the different activities and the institutions that are engaged in these activities.

Mr. Corey Tochor: To clarify, then, they could be associated with the PRC and still get funding—

The Chair: We're out of time now. Thank you for your answers.

We'll go over to Ms. Bradford, please.

Ms. Valerie Bradford (Kitchener South—Hespeler, Lib.): Thank you, Mr. Chair.

Thank you to our witnesses for coming on such a very busy day.

I am wondering if you can tell us what improvements you've seen in Canada's ability to identify national security threats in research.

Mr. David Vigneault: Yes, I will, and I'm sure my colleague will also have some others.

I think what we have seen over the last number of years are changes, both in terms of tools and in terms of how the government is looking at these issues. If you look at the Investment Canada Act, you will see that there have been changes over the years. I believe that the House sent a bill to that effect to the other chamber earlier this week. I think this is a good example that shows that there is a realization that the threat is evolving and that therefore the need to have different tools has evolved.

I think there have also been a number of other innovations under the leadership of the public safety department.

I don't know, Shawn, if you want to jump in on this.

Mr. Shawn Tupper (Deputy Minister, Department of Public Safety and Emergency Preparedness): Indeed, I think part of the massive improvement is just increased transparency. The increased work that we're doing with stakeholders and with universities in particular and the creation of a research security organization within my department allow us to make a concentrated effort, do concentrated work and develop frameworks that have allowed us, over the last four or five years, to progressively address these issues, identify where there are threats, have resources dedicated to making sure that people have awareness of those threats, and then engage with industry and academia around how we can collectively address the threats we have.

● (1645)

Ms. Valerie Bradford: Thank you.

How has Canada's approach to research security evolved over the last years as the technology becomes more sophisticated?

Mr. Shawn Tupper: I think part of that comes from paying more and more attention to the technologies. The government hasn't yet released, but is intending to release, a list of sensitive technologies that we want to focus on. We want to make our partners in those areas aware that they need to secure the work they're doing against espionage and against foreign interference.

As soon as the government is able, I know that it intends to release a list that will identify those areas of work that we think industry and academia should be concerned about and pay attention to. We also want to release a list of institutions that we identify as having close affiliations with the military and the national security and government agencies in regimes that we consider threats to our national security.

Ms. Valerie Bradford: What methods do malicious foreign governments or entities associated with them use to gain access to Canada's research ecosystem?

Mr. David Vigneault: Mr. Chair, this is part of the complex environment, and this is why it's so important to work with the institutions.

We've seen attacks through traditional espionage activities. We see it through cyber-espionage. We've seen it through collaboration on research projects. Sometimes we'll have people with different affiliations come in overtly and have access to information that should probably be kept a bit more discreet. We also have seen people misrepresenting themselves to have access to that information.

What you're looking at is an ecosystem with the clear intent of trying to get information, and whatever tool is at the disposal of the foreign state will be used to get to that information. I think this is what represents the most significant challenge for all of us: We need to be able to address and mitigate the threat coming from many different vectors at the same time.

Ms. Valerie Bradford: How does CSIS support the work of the granting agencies?

Mr. David Vigneault: Since the government's introduction of new guidelines and regulations, we have done a few things.

One, we have done a number of engagements with the research councils to share with them our perspective of the environment and of the threat. Also, Mr. Chair, we have done part of the review process, so the granting councils are referring a number of the applications to the government. We at CSIS are part of the review, from a national security point of view, to determine if they are indeed risks to national security and if potentially critical information would be leaving the country if such an application would be granted.

I would describe it as a very good relationship now, a productive relationship, and I would venture to say that in a number of years to come, we will see an improvement in and a deepening of that relationship to continue to address those threats.

Ms. Valerie Bradford: What role do the post-secondary institutions play in ensuring the security of Canadian research when they plan to collaborate with international research partners?

Mr. Shawn Tupper: I think that's part of the importance of the framework and the guidance and regulations that we have put in place. It informs and educates the universities on the kinds of indicators they need to look at when they're investing in research and identifying partners. It is helping them to understand those threats and to make informed decisions in terms of who they partner with.

As we move forward in terms of identifying external institutions and identifying those sensitive areas, that will further equip universities to make sound decisions in those areas.

The Chair: We're just about done on time. You have about five seconds.

Ms. Valerie Bradford: Okay. I'm fine. Thanks.

The Chair: Thank you.

[*Translation*]

Mr. Blanchette-Joncas, you have the floor for six minutes.

Mr. Maxime Blanchette-Joncas (Rimouski-Neigette—Témiscouata—Les Basques, BQ): Thank you, Mr. Chair.

I want to welcome the witnesses who are joining us today for this important study.

Mr. Vigneault, I have a fairly simple question for you: can you confirm that China directly or indirectly funds Canadian universities and provides private funding?

Mr. David Vigneault: Mr. Chair, as I mentioned in my opening remarks, there are limits to what I can reveal publicly.

That said, we are more concerned with research than with general university funding. In fact, we can see examples in the public domain of the various tactics of the Chinese government. More importantly, there are more and more third parties trying to hide their affiliation in order to be able to donate money and contribute to research projects that can lead to threats to Canada's security.

● (1650)

Mr. Maxime Blanchette-Joncas: Thank you very much, Mr. Vigneault.

I understand that you cannot confirm everything for us today, but I imagine that, if you warn a university, as you have done recently, it is because there is a threat. That's my understanding.

I would like to quote what you said in a CBC article published on October 17:

[*English*]

“We have the Chinese government engaged in the most sustained, scaled and sophisticated theft of intellectual property and acquisition of expertise that is unprecedented in human history”.

[*Translation*]

My question is quite simple. In the face of intellectual property theft and blatant predatory behaviour, do you feel that the federal government is doing enough to protect Canadian universities, researchers and discoveries?

Mr. David Vigneault: Mr. Chair, I thank the member for his question.

I believe that was said by one of my colleagues from the Five Eyes at the meeting described in the article. Having said that, I fully support the argument that's being made.

There are indeed threats to Canadian universities. In Canada, we are very fortunate to have cutting-edge universities. People come from all over the world to study at our universities. That has to be maintained. It is thanks to this international collaboration that we make advances in research.

The problem we have, especially with regard to the People's Republic of China and the government of Xi Jinping, is that all parts of that government are involved in seeking information, either openly or surreptitiously, in order to serve the interests of the Chinese Communist Party. Unfortunately, that also includes reviewing all the technologies to see if there is a way to modify them for the military purposes of the Chinese People's Liberation Army, which is a direct threat to Canada.

Mr. Maxime Blanchette-Joncas: Thank you, Mr. Vigneault.

You're well informed. Yes, that was a quote from Mike Burgess, head of the Australian Security Intelligence Organization.

The federal government announced last February that it was going to draw up a list of high-risk institutions. Eight months later, we are still waiting for that list. I asked the minister about this last Monday, as well as the people who were here today. Witnesses come and go, the committee keeps on holding meetings, and everyone expresses their concerns, but the delay in publishing this list creates uncertainty for applicants and for the protection of Canadian research.

Why do you think that list hasn't been published yet? Do you work with international partners that have such lists?

[*English*]

Mr. Shawn Tupper: First of all, the collaboration is extremely important, and with our Five Eyes partners we absolutely collaborate and try to learn from our respective best practices in this area. Absolutely those discussions occur.

We are indeed preparing advice. As I mentioned earlier, the government has stated its intention to release both an institutions list and a sensitive technologies list. That work is under way. I cannot steal the thunder of my minister in terms of when that announcement will occur, but suffice it to say that work is well under way.

[*Translation*]

Mr. Maxime Blanchette-Joncas: Can you clarify what your organization is currently doing to keep sensitive information from leaking out?

Mr. David Vigneault: Mr. Chair, I thank the member for that very important question.

First of all, CSIS works with a lot of federal government agencies. Specifically, CSIS works directly with universities and some researchers.

We provide information directly to universities and research centres, to the extent possible, within the limits imposed on CSIS by the Canadian Security Intelligence Service Act. We also conduct international investigations with our partners, the Five Eyes, of course, but also with many other partners around the world. We also do threat mitigation.

CSIS's mandate allows us to take direct action to mitigate threats. This is very important. We will never be able to reduce all threats, but, as I said in my opening remarks, teamwork is essential. Everyone has to work together to mitigate threats as much as possible.

● (1655)

[*English*]

The Chair: Thank you very much. That's six minutes. Now it's over to Mr. Cannings for the final six minutes on this round.

Mr. Richard Cannings (South Okanagan—West Kootenay, NDP): Thank you to everyone here today, especially Mr. Vigneault. Thank you for coming on such a day.

During this study, over the past number of weeks we've heard a lot of concerns about Canadian research and IP leaving the country—being stolen or leaking out in various ways. We've heard a lot from the university "ecosystem", as we've been calling it, and though the tri-council about this business of whether we should fund, or how we can stop funding, risky researchers.

A lot of research is, obviously, carried out by the private sector. I'm wondering how you monitor that. Is there a direct way you do that with industry groups? I read something in the media about Hydro-Québec having an incident with a Chinese researcher.

Without divulging secrets, what kinds of measures do you take to ensure that those very important research results and IP stay in Canada where they belong?

Mr. David Vigneault: When we look at the way the theft of intellectual property through state-sponsored activity occurs, we realize we need to address all aspects of the ecosystem, to use your word.

One thing CSIS has been doing is talking about this issue more publicly. I welcome the work of this committee to enlighten Canadians about this phenomenon.

We work directly with industry associations. We also work with some specific elements of the economic sector. I'll give you a very concrete example.

During the pandemic, we knew through our own intelligence—I think it was also fairly evident—that threats to the health research sector, in terms of pandemic research being done for a vaccine and so on, would become increasingly problematic. At CSIS, we were able to work with partners and map out the key industry companies and research labs in Canada involved in this work. We reached out to them directly and gave them some fairly practical advice. We didn't necessarily know a threat was coming to them specifically, but we said, "This is the modus operandi. If you were to be a victim of it, this is how it would likely work." I can tell you that within a few weeks of those briefings taking place, we were approached by one of these companies. They told us the PRC had indeed used the exact modus operandi for this crime. Because the company had taken the right steps to protect themselves, they were able to prevent the theft of their intellectual property.

It is a multiple-partner engagement, I would say.

Mr. Richard Cannings: Sir, perhaps I can jump in.

This may go to you, Mr. Tupper.

I'm interested in how you find out what the key information is. Who is advising you? Do you have scientists within CSIS, or are scientists in other public sector agencies interacting with CSIS? How does that work? How do you figure out what's important and what may be irrelevant?

Mr. Shawn Tupper: I think part of the work of the Research Security Centre is exactly that.

It's a whole-of-government endeavour. Our key partners beyond our portfolio would include ISED, Health Canada and other science departments. We want to pay attention to their expertise and capacity to give us advice. There is a whole-of-government structure that allows us to come together and collaborate on how we identify those areas.

Through the centre, we do a lot of public engagements. I have half of my centre here and half across the country. It's not a huge bunch of people. We do a ton of outreach as well. We're working with universities and industry. We run workshops and whatnot. This allows us to identify areas of priority external to government. Through this whole-of-government approach, we're able to build those bridges.

● (1700)

Mr. David Vigneault: Mr. Chair, can we add one point, please?

Mr. Richard Cannings: Sure.

The Chair: It's up to the member.

Dr. Nicole Giles (Senior Assistant Deputy Minister, Policy and Strategic Partnerships, Canadian Security Intelligence Service): Just to maybe put a couple of numbers around that, CSIS has briefed more than 200 organizations and 1,000 individuals about possible threats, so it's a continuous engagement that's absolutely critical.

We're also leveraging our expertise and our footprint in every region in the country to make sure that we're raising awareness, and we're doing a number of publications, including in local languages. This document, for example, is “Protect Your Research” in Inuktitut.

Mr. Richard Cannings: Just to finish up here—I don't have much time—you mentioned that the PRC is by far the biggest threat, and this is why we're studying it specifically. Can you perhaps let us know what other countries are of concern? Is Russia? Who is active in this space?

The Chair: You have about 15 seconds.

Mr. David Vigneault: I can add quickly that yes, Russia is, of course, of concern, It is less so in terms of sucking up all of the information the way the PRC does, but it is much more specifically a concern for technology that is right now under sanctions. They're trying to go around sanctions to get access to those technologies.

The Chair: Great. Thank you.

It was a really good round of questions and answers, and having both of you here is really helpful for our study. This is the last hour of our study. We hope to have a report generated by our analysts, and you're really helping with that.

We'll go to Mr. Soroka for five minutes, please.

Mr. Gerald Soroka (Yellowhead, CPC): Thank you, Mr. Chair.

Thank you to the witnesses today for coming.

Director Vigneault, why do you think it is taking so long to get a high-risk entities list from Minister Champagne, and how critical do you view such a list for Canada's national security integrity for academic research?

Mr. David Vigneault: I think that Minister Champagne was here earlier in the week to explain, so I would not want to put words in his mouth. I figure the minister's testimony is on the record.

On the second part of your question, sir, I think that it is very important that we identify risks, both in terms of protecting and in terms of transparency. That's transparency with us, transparency with foreign investors who are looking to engage with us and transparency with universities that are trying to determine how they should devise their own systems to protect their own systems. Yes, it is very important.

Mr. Gerald Soroka: Given Huawei's extremely recent patent filings in collaboration with Canadian universities in sensitive areas like 5G and AI, how does CSIS assess the risk these partnerships pose to national security in Canada?

Mr. David Vigneault: This is, I think, the crux of the issue here. The PRC has been very transparent in its approach. It has put in place new legislation that forces any company, any organization and any person of Chinese origin to collaborate with the intelligence service. In the case of a company like Huawei, irrespective of their intent—I will not speak about their intent at the moment—they are under an obligation, if required, to share their information.

If we go a little above and beyond this organization, I think that any kind of data they access, including every kind of personal identifying information about Canadians in different research projects like facial recognition, is of concern, because what we know both through intelligence and through open sources is that there is an organized system to take all of this data, to collate it, to apply artificial intelligence algorithms against it and to develop an advantage for the PRC that is then turned to aggressive tactics and also to the development of military technology to turn against us.

Mr. Gerald Soroka: We're basically giving them the information to fight us with the research that we're doing, so that is very concerning.

Minister Champagne also claimed, during our last meeting, that creating non-binding guidelines is somehow better than just banning entities that pose risks to national security. Does CSIS believe that non-binding guidelines are enough to protect against high-risk entities?

● (1705)

Mr. David Vigneault: Mr. Chair, I think what is important here is the behaviour of the people.

Right now, we have seen a change in behaviour. Everybody on the granting councils and in universities wants to work together. Everybody understands the threat, and if you develop an ecosystem of compliance, I think the people who do not want to comply will become fairly evident in all of this, and we'll be able to direct our activity more specifically at these people.

I'm agnostic, from a national security point of view, as to whether they are voluntary or not.

Mr. Gerald Soroka: I'm very concerned about the fact that universities seem to be more concerned about getting money from partnerships than national security. Do you feel this is also potentially true?

Mr. David Vigneault: Shawn, do you want to take this question?

Mr. Shawn Tupper: If I may, part of that challenge is changing the culture. There's a long history. Our universities have established partnerships for quite some time. Part of what we're doing, and part of why we have non-binding guidelines and why we've been engaging for a period of time, is to start that education process. As I said earlier, it's to make sure that people are able to make informed decisions on their own and not rely solely on the government.

I think it's an incremental approach to getting toward those areas where we say these institutions and these technologies are the most sensitive and need to be dealt with.

Mr. Gerald Soroka: Director Vigneault, at the Five Eyes conference, you raised warnings about Beijing's actions in Canadian universities. Where, specifically, is the Liberal government falling short in countering these threats?

Mr. David Vigneault: Mr. Chair, thank you for the question.

I will focus my comments on a national security point of view. I would say that what we have seen is a fairly significant change in the last four or five years. It's not just from an intelligence point of view and with us sharing more, but that everybody else is realizing that the environment has changed. The threat coming at us has changed in its intensity, in its velocity and in the number of actors.

I am, on the one hand, comforted by the fact that people are taking this very seriously; on the other, I'm very nervous about the intensity of that threat.

The Chair: Thank you.

It was a bit over, but it was important to get that thought on the table.

Thank you for the question, Mr. Soroka.

We'll go to Mr. Turnbull for five minutes, please.

Mr. Ryan Turnbull (Whitby, Lib.): Thanks, Chair.

Thank you, Mr. Vigneault, and the whole panel here, for attending today. It's a very important conversation.

Mr. Vigneault, I appreciate the work that you do. I know you testified at the procedure and House affairs committee when we did extensive work on foreign interference. I really appreciated your and Ms. Giles' testimony there.

You mentioned an increasingly complex threat environment, which I think we can all agree is the case. Really, it is at the heart of where our concerns are coming from. I think you said the PRC is the most sophisticated actor. You've also mentioned an ecosystem approach.

I think sometimes people are looking for a very simple solution for a very complex problem and a very complex risk environment that are evolving quite quickly. This is what I've heard from you in the past. I've heard you reiterate that today.

Could you speak, Mr. Vigneault, about the importance of that ecosystem approach and why that's more effective than, say, something like a blanket ban, which is perhaps not the most effective approach?

Mr. David Vigneault: I think we are in a world where some of what matters—the information and the data—resides in government hands, but most of it does not. With the way the technologies are evolving and the way the research is evolving, what we need is.... Even if you were able to build a Fort Knox in one area, if you leave the back door open, it's not going to work.

From that point of view, when I talk about the more complex threat environment, we're dealing with actors that are extremely agile in understanding our system. They have access to a lot of expertise, both inside and outside the country, to understand how our system works. We see these attempts to adapt their tactics and their techniques to what we are doing.

Here's a concrete example from the not so recent past. After Parliament changed legislation, we saw some indications of some actors being able to understand how that legislation works. They were essentially finding a way to be able to accomplish their objective through bypassing the new legislation. It's a bit of a cat-and-mouse environment in which we need not just the intelligence service or the federal government to be on their toes very quickly; it requires all of the members of that ecosystem to be on their toes as well.

● (1710)

Mr. Ryan Turnbull: I appreciate that response, because it relates to things you've also said about the importance of deepening the relationships and about the importance of behavioural change from various different actors in that ecosystem to effectively neutralize the threats or to respond effectively.

Would you agree with that?

Mr. David Vigneault: Yes, Mr. Chair. I would agree with that.

Mr. Ryan Turnbull: Okay. Great.

When we had NSERC here, they talked about having reviewed about 2,000 applications for alliance grants. They referred 62 of them—less than 4% of those applications—to Public Safety Canada for an in-depth review. I assume that CSIS gets involved at that point. I note that 34 of those were denied, so it's a little more than half. That's an interesting statistic.

Without getting into details that you of course wouldn't be able to reveal, how does CSIS utilize intelligence and how does it collaborate with Public Safety Canada to do that review?

Mr. Shawn Tupper: That speaks to that whole-of-government approach.

We lead that work at Public Safety Canada. We engage with our partners. We review the applications that are referred to us. We do assessments of the technology and the issues that come to the floor. We look at the partners and we give advice back. That is based on a collaborative effort that is based on an intelligence perspective. It also looks at our economic interests and our economic security. Those things all come into play as we assess and give advice back, and in some cases, as you note, we deny the applications.

Mr. Ryan Turnbull: Thank you.

Is there a threshold that you use for the risks when you assess?

I'm also interested in how the intelligence is used. I know, Mr. Vigneault, that in past conversations you've expressed how one piece of intelligence is not all that useful, and that it's a compilation over time that takes quite a bit of time. I know CSIS holds a lot of that information and gathers quite a bit of that intelligence. How do you utilize that, and what's the risk threshold? Those are my two questions.

The Chair: Be very brief. You have 15 seconds.

Mr. Shawn Tupper: There are no specific thresholds, because we have to do individual assessments on a case-by-case basis. We have to look at the parameters, the elements, of each and every file to make that determination.

The Chair: Thank you very much.

[*Translation*]

Mr. Blanchette-Joncas.

Mr. Maxime Blanchette-Joncas: Thank you, Mr. Chair.

Mr. Vigneault, I understand that there is no such thing as zero risk and that your organization is making efforts to counter various threats from around the world.

Personally, I get the impression that you are trying to fight with one hand tied behind your back. I'll tell you why. Canada's national security policy was established 20 years ago, in 2004. The policy does not include the word “China” or the word “Russia”. The federal government has asked you to conduct audits of organizations working in sensitive areas in order to be aware of current and emerging economic and security threats. But you don't even have the legislative authority to do that.

In addition, you say that everyone has to work in the same direction, but there is information that you cannot even pass on to businesses, municipalities or university institutions. So there is a breach of trust between the private sector and the government.

I would like you to tell us about the need to modernize the current policy, which is not only flawed, but also outdated.

Mr. David Vigneault: Thank you, Mr. Chair.

There are two aspects to your question.

Although no new documents have been published, the way in which national security issues are managed is constantly evolving. The most recent example is the Prime Minister's announcement concerning the National Security and Intelligence Committee of Parliamentarians. This will allow the right ministers and government agencies to give specific advice to the government on current challenges. I think this is a new component that shows that things are changing even though there have been no new documents.

With regard to the Canadian Security Intelligence Service Act, I believe that our public reports were quite clear. The threat has changed, as have Canadians' expectations and those of our partners. In the context of the committee's study, the universities are asking us for more information. They have been given an idea of the threats, but they need more concrete information.

The Minister of Public Safety publicly acknowledged that he was working on making changes to the act.

● (1715)

Mr. Maxime Blanchette-Joncas: Thank you, Mr. Vigneault.

I can tell you what Minister LeBlanc mentioned. In fact, he did not want to explain why—

[*English*]

The Chair: Unfortunately, we're at the end of the two and a half minutes.

[*Translation*]

Mr. Maxime Blanchette-Joncas: —his government does not want to update the national security policy.

[*English*]

The Chair: Thank you.

Mr. Cannings, go ahead for two and a half minutes, please.

Mr. Richard Cannings: Thank you again.

I think I've asked this question before during this study, but I'd just like to get a sense.

I feel as though I should be asking Mr. Lametti, because I'm wondering about the legal framework under which you operate. It's all very well to be working with researchers who may be unaware of what's been leaked and what they're losing to China, but what if you come across a researcher who is just a pure scientist who wants to do the research to discover the results and who doesn't mind that he's being paid by China to do that research and is outside the tri-council system? Is there some legal line that he might cross that would lead you to say he can't do that, or are there any powers you have to shut that down?

I'm wondering where that line is or where the lines are, because there might be several.

Mr. David Vigneault: Thank you, Mr. Chair, for the question.

CSIS does not have enforcement powers. We do not have those powers ourselves.

Sometimes when you have a discussion with CSIS and you are told about a number of elements in how your research or collaboration could be creating a risk to national security, it is impactful. That's on the one hand.

On the other hand, we would never want to have the intelligence service deciding what type of research gets done and who the researchers and the people are that universities can employ. However, I think it is a fair question to ask universities to make sure they have the right mechanisms in place to police themselves to determine if it's in their interests to have those types of relationships.

Finally, I would say that if there are activities that are covert and potentially violate the Criminal Code, we work very closely with the RCMP as well. I believe, Mr. Chair, that the member referred to a case recently with Hydro-Québec, in which criminal charges were laid against an individual, so the system is working. We probably just need to make sure it works in overdrive a little bit more.

Mr. Richard Cannings: Thank you.

The Chair: That's terrific. Thank you.

We've been efficient with our time. We can go to the Conservatives for five more minutes and then for five to the Liberals.

Mr. Tochor is starting off.

Mr. Corey Tochor: Director, you've just said that it's working—that the system is working and that it just needs fine tuning. Is that correct?

Mr. David Vigneault: I think I said that we need to put it in overdrive.

Mr. Corey Tochor: In overdrive....

There are patents that have been filed in Canada in association with Huawei and the University of Toronto this year. Obviously, that's not working, right? Would that be an example of this not working?

Mr. David Vigneault: Mr. Chair, I have a level of awareness about the transaction, but not enough detail to speak specifically to it. I think we have to be careful not to look at a specific activity and determine that it is nefarious in and of itself, but I would not have enough details to share with the committee today to say if those specific patents filed, you know—

Mr. Corey Tochor: Just on Huawei, are you saying that CSIS is comfortable with some research dollars from the taxpayers of Canada going to Huawei?

Mr. David Vigneault: Mr. Chair, I believe that I have not said that. What I have said, however, to a previous question, is that we are very concerned about organizations that are subject to the legislation of the PRC, and that, if and when forced to do so, will be able to share and will be acting on behalf of the government of the PRC. From that point of view, we do have a very high level of concern, which is why we've been speaking publicly and redirecting many more of our investigative resources to countering that threat.

● (1720)

Mr. Corey Tochor: To go back to this one company, obviously you're well versed on the dealings of Huawei. There's a list that's been promised to come out that will ban different entities from working with universities in Canada with taxpayers' dollars for funding. In what world would Huawei not be on that list?

Mr. David Vigneault: Do you want to take that?

Mr. Shawn Tupper: Well, first of all, the list isn't out, so you will have to wait—

Mr. Corey Tochor: I'm assuming there is an internal list that's getting compiled, right?

Mr. Shawn Tupper: That's the entities list.

Mr. Corey Tochor: Yes.

Mr. Shawn Tupper: Yes. That list is being compiled. Advice will be given to the government, and the government will release that list when it is ready to do so.

Mr. Corey Tochor: The government has that list, you're saying...?

Mr. Shawn Tupper: I'm saying that we are developing advice and have given advice to the government, and the government will release that list when it's prepared to do so.

Mr. Corey Tochor: The problem is that the government didn't act on the list you provided, and now we have another submission of different funding applications that have been approved this fall. Do you not see the problem here? You've briefed the government on this list and they're not acting.

Why wouldn't we just...? If it's that difficult to make a full list, we could start with a partial list. Why wouldn't Huawei be number one on that list and be banned from receiving an additional nickel from the taxpayers of this country?

Mr. Shawn Tupper: I won't comment right now on who or what companies are or will not be on that list. I do think it's important to remember that we are a country of laws, and Huawei exists in Canada in a legal way, so we can't completely ban the activities of Huawei as long as it exists within Canadian law.

We do need to pay attention to your earlier point about whether taxpayer funding and money goes towards organizations that may or may not be on that list. I think that is what the government is grappling with right now. It's trying to find ways it can construct that list in respect of who operates in this country, in respect of—

Mr. Corey Tochor: Thanks for that.

I'm going to pass my time over to my colleague.

The Chair: You have about one minute and 20 seconds.

Mr. Gerald Soroka: Thank you.

Considering the leaks from within CSIS about Beijing's interference in Canadian elections, how do you reconcile this information with Minister Champagne's claims that there is a great dialogue with Canadian security departments?

Wouldn't the leaks actually suggest a significant communications breakdown with the government, rather than great dialogue?

Mr. David Vigneault: For the record, Mr. Chair, if you allow me, I want to be clear that there has been information unauthorizedly released from CSIS documents; I don't think it has ever been concluded that is was a leak from CSIS. I wanted to make that distinction.

In our system, the way it should work is that the intelligence service is the right entity to be providing that information to the government in terms of what we see, what the concerns are, and so on. Public Safety Canada and other departments are also providing advice to the government on what needs to be done.

That is how we're looking at that—

Mr. Gerald Soroka: I need to interrupt you. Sorry.

You're saying that the leak never came from CSIS. Are you saying the leak came from the government?

Mr. David Vigneault: Again, to be very clear, it was not determined that the leaks were coming from CSIS. I think I will leave it at that.

Mr. Gerald Soroka: Then it did come from government.

Mr. David Vigneault: The record—

The Chair: Thank you.

Next we have Ms. Jaczek for the last five minutes, please.

Hon. Helena Jaczek (Markham—Stouffville, Lib.): Thank you so much to all the witnesses for coming today and enlightening us.

One of the things that Minister Champagne told us was that the list is being prepared with the other Five Eyes countries. When the list is fully developed, will it be shared with the other Five Eyes countries? Is there any possibility that the Five Eyes will use the same list?

Mr. Shawn Tupper: I think countries will make choices for themselves, depending on who is active in those countries and the kinds of things they feel they need to protect. Canada will make its own choices based on our ecosystem.

Certainly, that information is shared. As I said earlier, we try to learn best practices from one another in that respect.

Hon. Helena Jaczek: How often will the list be looked at again? Monsieur Vigneault has said that the situation is constantly evolving. Will there be a time frame for review?

Mr. Shawn Tupper: With that respect, the list will remain evergreen. We will be constantly looking at entities that are operating in our environment and looking at the technologies that come to the fore. We will keep that list evergreen.

Hon. Helena Jaczek: Perhaps for reassurance, I assume that the list is focusing not only on China but that it is in fact country-agnostic.

Mr. Shawn Tupper: That is correct.

Hon. Helena Jaczek: Thank you.

In terms of your outreach to industry and the private sector, Monsieur Vigneault, you did allude, as did Ms. Giles, to a lot of consultation around some of the emerging potential threats. You've mentioned vaccines.

Clearly, I'm very interested in the health side of things. Are you looking at previous investments in research in Canada by these industries, or are you casting a wider net to brief the private sector?

● (1725)

Mr. David Vigneault: The way we look at it is twofold.

First it will be from an assessment point of view: We will look at the past behaviour of different actors and determine how they would adapt their tactics, given the intent that they have. We would then be able to zero in on the types of companies or research sectors that may be at risk. That is one approach. We would be using the information we already have.

The other one, of course, is through our own investigation and through partnerships with our international partners. I can tell you that all of the discussions that I have with the.... At CSIS, we have official relationships with over 300 different organizations and intelligence services around the world. A lot of these discussions revolve around exchanging information to better understand the specific threat vectors, so we use both the analysis of previous information plus new information we collect in Canada ourselves or from abroad, as well as information from international partners.

That's what builds the environment that gives the opportunity for our great analysts at CSIS to work with all of our partners to then determine the right places and the right actors to provide the most impact in our engagement to mitigate that threat.

Hon. Helena Jaczek: Once the list has been established, will there be any thought to look back retrospectively, supposing there is a specific institution that is on the list? Is there any thought to look retrospectively at previous or ongoing research to assess whether there is a potential threat from that ongoing research?

Mr. Shawn Tupper: We are conscious that the playing field is going to change all the time, so we need to be looking not just forward but also at what's going on now to make sure we fully assess the threats to Canada that may exist.

Hon. Helena Jaczek: I think that's a very important point, actually. We've been hearing about applications to the alliance granting agencies, etc., but surely there is a risk from something currently in process.

Mr. Shawn Tupper: It could be a risk from something that is ongoing, yes.

Hon. Helena Jaczek: Thank you very much.

How much time do I have?

The Chair: You have 30 seconds.

Hon. Helena Jaczek: I think I'll just cede it.

The Chair: That was a great line of questioning.

Thank you, again, to all the witnesses who have been here to help us conclude the witness portion of our study.

Now the analysts have some work to do, and we'll be reviewing the findings we've had from these very enlightening discussions.

Thank you, Director Vigneault, Dr. Nicole Giles, Shawn Tupper and Sébastien Aubertin-Giguère, for being here and for your testimony and your participation in relation to this study.

If there is additional information, please submit it. If there is information to come to us, we will need it in a timely manner because we will be reviewing the analysts' work soon.

We'll suspend briefly now to allow our witnesses to leave and to have our audiovisual check. We will be in camera and we're not going to be broadcasting the next portion of our meeting.

Thank you again.

We'll suspend for a minute.

[*Proceedings continue in camera*]