HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

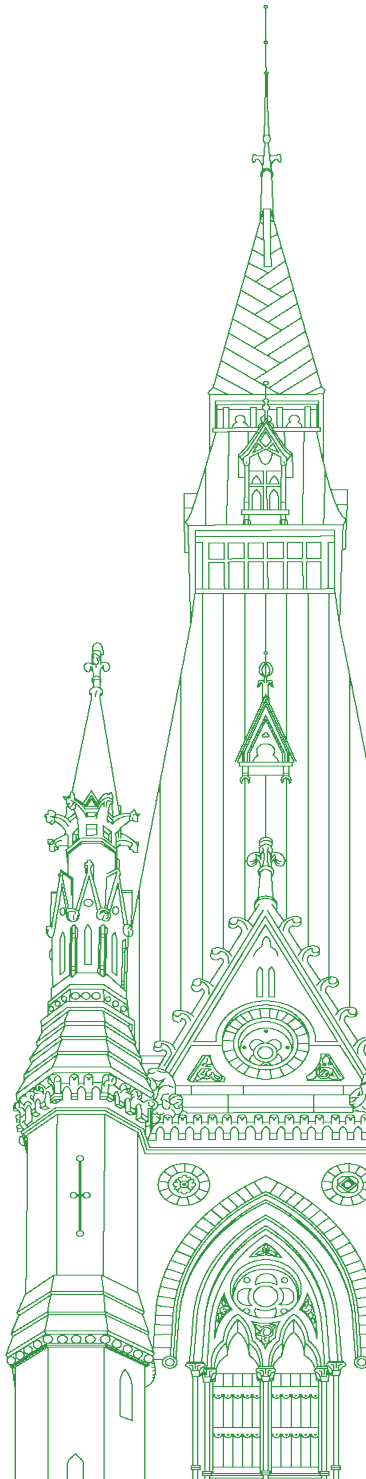
44th PARLIAMENT, 1st SESSION

Special Committee on the Canada–People's Republic of China Relationship

EVIDENCE

NUMBER 036

Monday, April 8, 2024



Chair: Mr. Ken Hardie

Special Committee on the Canada–People's Republic of China Relationship

Monday, April 8, 2024

● (1835)

[*English*]

The Chair (Mr. Ken Hardie (Fleetwood—Port Kells, Lib.)): I'll call the meeting to order.

Welcome to meeting number 36 of the House of Commons Special Committee on the Canada–People's Republic of China Relationship. Pursuant to the order of reference of May 16, 2022, the committee is meeting for its study of the Canada–People's Republic of China relationship.

As a substitute member today, we have Mr. Cooper subbing for Ms. Lantsman. I'm sure the shoes are killing you.

We also have MP Ellis substituting for MP Seeback and MP Naqvi for MP Oliphant, and Mr. Desjarlais is in for Ms. McPherson.

It's good to have you joining us.

Today's meeting is taking place in a hybrid format. Members are attending in person in the room and remotely using the Zoom application.

Please wait until I recognize you by name before speaking. For those participating by video conference, click on the microphone icon to activate your mic and please mute yourself while you're not speaking.

For interpretation, those on Zoom have the choice at the bottom of the screen of floor, English or French. Those in the room can use the earpiece and select the desired channel.

I'll remind you that all comments should be addressed through the chair. For members in the room, if you wish to speak, please raise your hand. For members on Zoom, please use the "raise hand" function. The clerk and I will manage the speaking order as best we can. We appreciate your patience and understanding in this regard.

Per the motion adopted on March 26, 2024, we're hearing testimony in relation to the matters revealed in the Winnipeg lab documents.

I'd now like to welcome the Honourable Mark Holland, Minister of Health, and, from the Department of Health, Nadine Huggins, assistant deputy minister and chief security officer, corporate services branch.

From the Public Health Agency of Canada, we have Heather Jeffrey, president. By video conference, we also have Dr. Guillaume Poliquin, vice-president of the national microbiology laboratory.

We see everybody present.

Minister, you may commence with a five-minute opening statement.

Hon. Mark Holland (Minister of Health): Thank you very much, Mr. Chair.

It's wonderful to be here. I appreciate the committee giving me the opportunity to answer questions and to make some brief opening remarks.

Let me start by saying the action of the two former employees at the national microbiology laboratory are reprehensible and deeply disturbing. The two Canadian citizens, two eminent scientists who were well known throughout North America for their contributions in the field of therapeutics, vaccines and virology, lied. They misrepresented themselves. These were employees who were hired in 2003 and 2006, respectively, and who made great contributions outside of this. Appropriately, the Public Health Agency identified them. They were fired, and they are now the subject of an investigation.

The second thing I'd like to do at the onset is recognize the extraordinary world-class work done by the national microbiology laboratory. Its surveillance work in the area of infectious disease, in emergency outbreak preparedness and response, in training and in research and development helps keep Canadians safe. We're extraordinarily lucky to have some of the greatest scientists in the world working in that facility. Their work is absolutely critical to the continually evolving health environment we're in, which necessitates international co-operation.

I will also recognize that in the past five or six years, not only have we had a global pandemic, but the threat environment we live in is different. Countries such as China are implicating themselves in our domestic processes in a way that would have been unimaginable just five years ago. As such, we have to respond, and we are. I'm happy to talk about some of those responses.

I think it's important for context to talk about how we got here today.

I was a member of the public safety and national security committee. I was its vice-chair. We had an opportunity, going back, in 2006, 2007, 2008 and 2011 to say to the government of the day, the Conservative government, that the recommendations of Justice Iacobucci and Justice O'Connor were essential. One of the main recommendations in both of those processes was to have a committee of parliamentarians that had the opportunity to look at all documents.

It's important to note in this particular case with the employees who were hired in 2003 and 2006 that the only thing that would be different today if there weren't a Liberal government is we wouldn't be having this meeting and you wouldn't see the documents. The Conservative government of the day refused to allow parliamentary oversight.

In 2021, when this matter was before the House of Commons, there was a battle in Parliament, a disagreement about how these documents should be looked at. At the time, the offer was made for NSICOP to be given an opportunity to look at this so parliamentarians of every political party would have the opportunity to look at the documents in their totality without redactions. After the 2021 election, the comment was made to me when I was the House leader that the opposition parties had a concern that this would mean if they disagreed with redactions, they would have no challenge function to those redactions. Appropriately, they asked for the ability to challenge redactions.

At that point in time, as House leader, I worked with other parties—initially it was just the New Democratic Party, but eventually, many months later, the Conservatives and the Bloc also joined us—to have an ad hoc process of independent arbiters who were able to look at the documents, and where there was disagreement on redactions, they could make a decision about what should or shouldn't be released. That committee and the independent panel of arbiters appropriately were asked to err on the side of public disclosure and to make sure the maximum public view into the documents would be made available. That's precisely what occurred.

We're not just talking here about national security in these redactions. The Public Health Agency also obviously has to consider confidential employee information. Quite rightly in this case, the normal protections around confidentiality of employee information were waived, given the serious security breach these two Canadian citizens engaged in. That's why we're here today.

With that, Mr. Chair, I'm pleased to take questions from the committee.

● (1840)

I appreciate the opportunity to appear before you today, and I'll turn it back over to you.

The Chair: Thank you, Minister Holland.

We will begin with Mr. Cooper for six minutes.

Mr. Michael Cooper (St. Albert—Edmonton, CPC): Thank you very much, Mr. Chair.

Thank you, Minister, and thank you to the officials who are here.

Minister, three weeks ago when you appeared before the health committee and were asked about the massive national security breach at the Winnipeg lab, you stated that PHAC at all material times acted in the “highest order” and that with respect to accountability, no one at PHAC will be fired. Do you stand by that?

Hon. Mark Holland: Well, in the first order, these two employees were fired. They were held to account for their actions and for the lies they told. However, I believe, as I stated then, that the Public Health Agency acted appropriately throughout the process in responding to those lies and the misinformation.

Mr. Michael Cooper: No one else will be fired. Is that correct?

Hon. Mark Holland: I am not aware of anybody else being fired. The people who were responsible—

Mr. Michael Cooper: Okay, thank you, Minister—

Hon. Mark Holland: —for engaging in that activity have been fired.

Mr. Michael Cooper: I want to ask you some questions about decisions that PHAC made surrounding this massive national security failure. Canadians themselves can judge whether PHAC acted in the highest order, as you stated three weeks ago before the health committee.

First, why in October 2018 did PHAC enter into a material transfer agreement with the Wuhan Institute of Virology to transfer, from the Winnipeg lab, Ebola and Henipah, two of the most deadly pathogens? Why did that happen?

Hon. Mark Holland: In 2018, we were working collaboratively with China on developing therapies and interventions with respect to Ebola. It is a serious global pathogen, and the efforts at that point in time were to collaborate with China in a partnership—

Mr. Michael Cooper: Okay. In October—

Hon. Mark Holland: —to take action with respect to Ebola.

Mr. Michael Cooper: Minister, I asked you a question and I'm going to build on it.

October 2018 is significant. This material transfer agreement was initiated by none other than Dr. Qiu, one of the two scientists.

In October 2018, at the time that material transfer agreement was entered into, PHAC was already aware that Dr. Qiu was named on a Chinese patent that was highly suspicious and had been flagged to CSIS by the head of the Winnipeg lab as a potential national security threat. Why in the world, with that knowledge, would PHAC transfer deadly, dangerous pathogens to Wuhan at the request of a scientist that PHAC knew at the time was a potential national security risk?

Hon. Mark Holland: As you know, it was in the fall of 2018 that this matter was first flagged as a concern, and we have due process. The transfer you're talking about was done with the full knowledge and the full co-operation of the Public Health Agency in the interest of advancing the protection of our species against the infectious disease Ebola. At that point in time, because Ebola doesn't know boundaries, the effort was to work collaboratively with China and other countries. It is deeply disturbing, obviously—

Mr. Michael Cooper: Minister, I only have so much time.

Mr. Peter Fragiskatos (London North Centre, Lib.): Chair, I have a point of order. This is the third time now that Mr. Cooper has interrupted the minister, who is here as a witness.

He's answering in good faith, and I think Mr. Cooper is asking questions that he's perfectly entitled to ask. However, I would ask, Mr. Chair, that the usual, the typical and the collegial back-and-forth that we expect here at committee be allowed to take place rather than interruptions, because I'm trying to get a sense of the answers as well, and interruptions get in the way.

The Chair: Thank you for that, Mr. Fragiskatos.

Minister Holland, I think you should do your best to keep your answers concise, given that there is limited time for questions.

Mr. Cooper, allow the minister to complete his answers.

Go ahead. We stopped the clock. You're good to go.

Mr. Michael Cooper: Thank you, Mr. Chair.

Minister, you are right that it was in the fall of 2018 that red flags were first raised about these two scientists. A preliminary investigation wasn't undertaken until December 2018. That's months after the first red flags were raised, and in the interim, a material transfer agreement was signed with Wuhan at the request of one of the scientists who was deemed to be a potential national security threat.

Why did it take so long to launch a preliminary investigation? Three or four months is a long time.

● (1845)

Hon. Mark Holland: In this instance, the nature of that patent and the reason the patent hadn't been disclosed were being investigated, and there is due process.

It is indeed sad for the world that we are no longer able to cooperate closely with countries with respect to deadly pathogens that represent a clear and present threat to the human race. The fact that there are countries engaging in activities that would endanger not only our country but all human beings is profoundly disturbing.

Mr. Michael Cooper: Minister, the preliminary fact-finding report was issued on March 23, 2019. It identified that the two scientists had engaged in multiple security and intellectual property breaches, that they had engaged in unauthorized transfers, including to Wuhan, and that they had engaged in unauthorized research collaboration with the Beijing regime, including the People's Liberation Army.

What did PHAC do next? PHAC then transferred Ebola and Henipah to Wuhan.

Hon. Mark Holland: You're making a connection between two completely separate things.

In the first order, the transferring and working with China at that point in time to try to protect our species from Ebola was something we were doing earnestly, with the belief that China shared our desire to protect human beings from a deadly pathogen.

In the second order, when you're talking about the individuals—the scientists who were fired—you have to remember that these individuals were hired in 2003 and 2006. They are published throughout North America. They are eminent scientists. They are Canadian citizens—

Mr. Michael Cooper: Minister, it's amazing that you cannot see how reckless this is—

Hon. Mark Holland: Sir, if I could finish—

Mr. Michael Cooper: —and not only that, Minister, but—

Hon. Mark Holland: Mr. Chair, if I could be afforded.... I think it's a key point.

Mr. Michael Cooper: —it took another three and a half months—until July 5, 2019—before the two scientists were finally marched out of the Winnipeg lab, scientists who in March had been identified as working with the People's Liberation Army.

This is Canada's highest security lab. Is that really an instance of PHAC acting in the highest order, as you said?

Hon. Mark Holland: Let me say that—

Mr. Michael Cooper: Is that Mark Holland's definition of PHAC acting in the highest order?

The Chair: Mr. Cooper, you are over time, but I will give the minister an opportunity to respond.

Hon. Mark Holland: Due process is incredibly important. These individuals worked with the Public Health Agency. One was hired in 2003 and one was hired in 2006. They were published and renowned across North America for their work in vaccines, virology and therapy. They were seen as leaders in helping to save lives.

If you are making an accusation against somebody, these people's careers can be, rightly, destroyed. Before you destroy somebody's career, they are entitled to due process. Due process is important in this country.

Mr. Michael Cooper: Minister, are you saying that they are eminent scientists or eminent spies?

The Chair: Mr. Cooper, I'm sorry, but your time has expired.

When we speak over each other, it makes it very difficult for our interpreters to do their jobs.

We will now go to Mr. Naqvi for six minutes or less.

Mr. Yasir Naqvi (Ottawa Centre, Lib.): Thank you very much, Mr. Chair.

Minister, welcome to this committee.

I want to pick up the conversation where Mr. Cooper left it because I think he's throwing out quite a few dates and perhaps muddling the facts.

Canada, I'm assuming, has had a long-term relationship in working with China and other countries when it comes to finding a cure for deadly pathogens, as you put it, and other matters. Can you walk us through the kinds of relationships, arrangements and agreements that Canada, through the Public Health Agency of Canada, goes through and develops with other countries like China?

Hon. Mark Holland: The collaborations we engage in internationally are critically important to protecting our population and to protecting human beings all across the world. As I mentioned, pathogens don't know international boundaries, and they certainly aren't interested in politics, so the ability to share best practices, science and the latest evidence of what actions we can take, be they in therapies or vaccines, is critically important. Where new information arises, we want those partnerships.

I think it's deeply tragic, frankly, that the relationship with China deteriorated such that we can't collaborate on these issues any longer. It is unfathomable that a country would place its interests as a nation ahead of the interests of the health of our species.

That's what we encountered here. We're at a very different place now than we were five years ago, and that's deeply tragic. However, that is separate and apart—and I think we have to be very careful because there is an attempt to conflate these things—from the actions of Canadian citizens who lied. They were in their jobs and completely misrepresented themselves to the Public Health Agency. That's reprehensible.

They were rightly fired. They're rightly subject to investigation. It is certainly a very serious matter, but we have to be careful, I think, in the characterization of that to not conflate things.

● (1850)

Mr. Yasir Naqvi: Obviously, what happened in 2018 and 2019 with these two particular scientists is that they essentially lied to their employer, the national microbiology laboratory.

Can you walk us through what steps have been taken by the national microbiology laboratory to ensure that safety and security are enhanced and that nothing like what happened in 2018 and 2019 can happen again?

Hon. Mark Holland: Look, anytime somebody misrepresents themself and engages in behaviour of this nature, you learn. Certainly, the threat environment for Canada has changed over the last five years. There have been very critical actions, and I can go into more detail. I know we don't have a lot of time.

With respect to physical security, facility access, employee communication, engagement technology, partnership and research affiliations, and governance oversight, it's a process of continual improvement. When it comes to national safety, unfortunately we don't always—or even most often, in fact—share the same values as some of our adversaries. They're willing to go places and do things that are unimaginable to us. I think it would have been unimaginable that a country like China was potentially willing, in this instance, to use pathogens that threaten humanity in order to advance their geopolitical agenda. That's no longer unimaginable, so it changes how you respond.

Looking at how employees communicate.... Even incredibly eminent, well-published scientists who are Canadian citizens recognize that we have to dig more and ask more questions. In the past, that would have been deeply insulting to scientists. Now, in light of this, scientists understand that they can't be taken at their word and that we have to question other relationships they have and probe into their lives in a way that would have seemed entirely inappropriate and crazy before.

That's the advantage of hindsight when somebody does something unthinkable. It changes your framing and disposition. Then we as a society have to accept something that's more invasive. That's certainly true for scientists today.

Mr. Yasir Naqvi: Thank you.

How much time do I have left, Chair?

The Chair: You have one minute.

Mr. Yasir Naqvi: Perhaps in a minute I can ask the officials to outline what kind of process both the Public Health Agency of Canada and the national microbiology laboratory went through to enhance their safety and security protocols after 2018 and 2019.

Ms. Heather Jeffrey (President, Public Health Agency of Canada): I can respond to that question.

In addition to enhanced physical security and access control measures, all policies at the national microbiology laboratory and the agency were revised. These are secret-level facilities requiring clearances under the Human Pathogens and Toxins Act. There is continual training and review of our guard services, as well as our personnel. We have strengthened protocols for deliveries in shipping and receiving, including mandatory controls around documentation and verification of infectious materials. There are requirements for material transfer agreements and collaborative research agreements, and enforcement of their use.

Comprehensive threat and risk assessments for the physical and IT environments have been undertaken to ensure that all of our security measures are complete and up to date. In addition, we have updated our policy on affiliations and collaborations with academic, research and health care organizations, and we have a new student hiring policy with additional controls.

These are designed to respond to the threat environment we face.

The Chair: Thank you, Ms. Jeffrey.

We have finished with Mr. Naqvi's time.

We will now go to Mr. Bergeron for six minutes.

[*Translation*]

Mr. Stéphane Bergeron (Montarville, BQ): Thank you, Mr. Chair.

Thank you, Mr. Minister, for being here.

Listening to your answers to Mr. Cooper's questions, I found it very naive when you said that, at the time, you still believed that the Chinese authorities considered deadly viruses like Ebola to be at par with how important you consider protecting humanity to be.

I find these comments all the more naive given that, in an article posted on the Radio-Canada website on February 29, you said that China's influence on the Canadian scientific community "was not as widely known as it is today".

However, in an article published in Le Journal de Montréal on January 29, 2024, we learned that the Canadian Security Intelligence Service, or CSIS, released a report in 2010 explaining China's growing economic power, its growing confidence and its aggressive new agent recruitment policy, which suggest that it has the will and resources to enhance its intelligence activities more and more.

In short, for over 20 years, CSIS has been alerting government authorities to the fact that the People's Republic of China is being much more aggressive and is intensifying its intelligence activities, particularly in terms of technological research and biomedical advances.

Therefore, why claim that China's influence was not as widely known as it is today?

● (1855)

Hon. Mark Holland: First, I must say that the issue of public safety is extremely complex, because it has many dimensions. In the case of a virus that threatens the population in general, we first expect the government to do everything it can to protect the public, including cooperating to find solutions. We expect that if a solution exists elsewhere in the world, the government will take action. First of all, we try to work with all scientific communities around the world to find a solution. This is really important, because if a tragic event were to occur, other types of questions would be asked. People would ask the government what it's done to protect the public and whether it has sought a solution. So it's important to cooperate as much as possible.

However, the world has changed a great deal over the past five years. Five years ago, we certainly had a problem with China. That was absolutely the case. However, for me, it's terrible to think that a country could play with a virus for geopolitical reasons. To me, that's something else. As Minister of Health, I have a lot of objectives on my mind at the same time, because many threats are still present. I'm very concerned about that.

So we have to cooperate with all countries as much as possible. It's therefore extremely unfortunate that we can now no longer work with a country as big as China. China has a lot of incredible scientists; they have enormous potential to find solutions for their country, for our country and for people in general. It's very sad that our interaction with a country like that is coming to an end. That has major implications, not only for Canada, but for the world.

Mr. Stéphane Bergeron: It must be recognized that it's a laudable objective to want to work with all countries to prevent the spread of viruses that can be catastrophic for humanity. However, given that CSIS has been warning the Canadian government for over 20 years that the People's Republic of China's scientific espionage is a problem. Don't you think we were a bit reckless to continue sharing our secrets or scientific information with scientists who were then passing it on to the Chinese authorities?

● (1900)

Hon. Mark Holland: You're right, when we share information, there is a risk that a country could use it to gain an economic advantage. However, that carries far less risk than threats to our public safety and national security. Five years ago, China or scientists in China might have used the information for an economic advantage. However, the consequences of that are not really serious compared to using a virus as a weapon or as a threat to the global population, which is a completely different ball game. As I already explained, I find it extremely unfortunate that it's now impossible to cooperate with a billion people on viruses.

So, they are two very different things.

[*English*]

The Chair: Thank you, Minister.

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

Mr. Blake Desjarlais (Edmonton Griesbach, NDP): Thank you very much, Mr. Chair.

I want to thank the minister for being present for a very important piece of work. It concerns something that I think most Canadians are concerned about—the safety and security of not only our country but also our information. In an age of digital technology, when both companies and countries are participating in the exchange of information and the withholding of information, it could be, to put it in terms of bad actors, a battlefield. In this particular instance, I think Canadians are concerned that should we find ourselves in an "informational battlefield", we would be disadvantaged by the reality of the knowledge being seen in this very troubling case.

Minister, I think you alluded to the fact that it's important for there to be accountability. The two individuals who did this are no longer there, of course, but what isn't known is how co-operative other officials could have been, or other persons or personnel. What information have you or your ministry reviewed, maybe in coordination with CSIS, on the safety and security of other persons in PHAC, particularly in its work on information, science and technology?

Hon. Mark Holland: I hope everybody gets an opportunity to visit the national microbiology laboratory and meet the scientists there, who are on the front lines of looking at potential nightmare scenarios. COVID was bad, but it could have been much worse. In so many instances, we were very lucky as a population that we didn't have a pathogen with a much higher mortality rate.

That remains a risk for our population at any given time. We charge the Public Health Agency and the national microbiology laboratory with finding solutions to nightmare scenarios and co-operating with and listening to scientists and engage wherever possible, because if God forbid anything ever happens, people will ask, "What did you do to find an answer?"

As I said, when you take one billion people off the planet and can no longer co-operate with hundreds of thousands of scientists who themselves are leading in the area of virology and finding solutions, that is a terribly tragic day for humanity. When I look at it, and I would encourage you to look at it too, the threats that the Public Health Agency is trying to navigate.... Think about this. These were employees engaged in—

Mr. Blake Desjarlais: I'm sorry, Minister. It's just that the time is really short.

Hon. Mark Holland: Sure. Go ahead.

Mr. Blake Desjarlais: Just to go back to the question, have you reviewed or have you met with CSIS to review the existing personnel in the agency to see whether the security clearances are in fact appropriate?

Hon. Mark Holland: I am not responsible for that. I think the Public Health Agency—

Mr. Blake Desjarlais: You haven't met with them on it.

Hon. Mark Holland: I would not meet with CSIS.

In terms of the security reviews of employees, I would turn to the officials on that—to Madam Jeffrey, if I could. That would be on her side of the fence.

● (1905)

Mr. Blake Desjarlais: Go ahead, Ms. Jeffrey.

Ms. Heather Jeffrey: In the first instance, this situation came to light in these cases as a result of a security awareness briefing provided by the Canadian Security Intelligence Service in regard to the threats against Canadian research and the potential vulnerability of Canadian scientists to pressure. That awareness-raising continues in regular meetings with our security services and ongoing reviews. I would note that the RCMP investigation into these cases remains ongoing, as they have said publicly.

Those contacts have been regularized and are constant and ongoing, as is appropriate given the nature of the ongoing evolving risk situation.

Mr. Blake Desjarlais: Thank you for that.

To get to the crux of the issue, I think it's important that PHAC and other agencies within the government have security processes for really important information like this. It is a bit concerning to know that CSIS was the only agency that identified this information vulnerability prior to PHAC. I believe that Canadians expect, in an agency that has an immense amount of information on individuals, particularly personal information, that there be some kind of security oversight internal to the ministry.

I think this could have been largely prevented by way of the recent changes that you've discussed publicly, Minister. Those changes could have been made much sooner, I believe, which could have reduced some of the risk that's present to this case.

In one quick answer, if you could do this whole thing again, would you have released the documents sooner?

Hon. Mark Holland: No, because the process by which we released the documents was incredibly important.

Maybe I can rest on this moment for a second. National security is not the only issue present here. There's also consideration for protecting employee privacy, and if you're going to waive that.... The people who serve in the public service have that right—as in any job, by the way. I was head of Heart and Stroke. We let people go. Sometimes it was painful, because they would have a story of why they were let go that was completely inaccurate, but I wasn't allowed to comment. The reason I'm not allowed to comment is that employee confidentiality is extremely important. To waive that is a big deal. When we waive it, I think we have to think through these issues.

What I liked about this process was that a weakness was identified in NSICOP—challenging redactions. We were able to create a process in the ad hoc committee that allowed those, through an independent arbiter, to be released with maximum transparency while protecting the partnerships we have with our Five Eyes partners to make sure that employee information and national security are protected.

What I think is worth doing—

Mr. Blake Desjarlais: Do you think that has impacted, however, our credibility to our allies at NATO and to the Five Eyes, for example?

Hon. Mark Holland: I think the fact that we were so cautious in dealing with this issue and that we worked through a way of ensuring both transparency and public interest and making sure that we still maintained our commitments to protect our processes—

Mr. Blake Desjarlais: I don't know if we did that, though, because it was an information breach.

Hon. Mark Holland: There are two different questions.

Maybe I misunderstood your question. I apologize. I thought your question was on how we handled the release of the documents—

Mr. Blake Desjarlais: That was the first question. The second question was related to the impacts on our allies.

Hon. Mark Holland: Right. On the second question—and I think this bears thinking about—these employees were long-term employees, from 2003 and 2006, published—

Mr. Blake Desjarlais: I think that's why it's concerning, though, Minister.

Hon. Mark Holland: It is for me too. These are Canadian citizens, eminent scientists.

Mr. Blake Desjarlais: Has it impacted our allies to know that we—

Hon. Mark Holland: Yes, it has and it has in this way.

Mr. Blake Desjarlais: Yes, I think—

The Chair: Gentlemen, I need to intervene because Mr. Desjarlais' time has expired.

Mr. Blake Desjarlais: Thank you, Chair.

The Chair: It's time to go to Mr. Chong for five minutes.

Hon. Michael Chong (Wellington—Halton Hills, CPC): Thank you, Mr. Chair.

Was the identification of two patents registered in China the first red flag that went up about Dr. Qiu?

Hon. Mark Holland: That's correct.

Hon. Michael Chong: Can you tell us why Dr. Matthew Gilmour suddenly resigned eight weeks into a global pandemic in May 2020 and why Tina Namiesniowski, the president of the Public Health Agency of Canada, suddenly resigned on a Friday afternoon in September 2020?

Hon. Mark Holland: I don't know that I'm in a position to comment on that.

Madam Jeffrey.

Ms. Heather Jeffrey: I would say that for both of them, it's not really appropriate for us to comment. I think they both reflected that they resigned for personal reasons not associated with this issue.

Hon. Michael Chong: Not associated with this issue at all....

Ms. Heather Jeffrey: I'm not privy to their reasons, but that was what—

Hon. Michael Chong: You know that they resigned for personal reasons. That's what you're telling us.

Hon. Mark Holland: Perhaps I can respond. I think one of the challenges—and I got into it earlier—is that anytime we're talking about information with respect to an employee—

Hon. Michael Chong: I know what you're going to say, Minister.

● (1910)

Hon. Mark Holland: —we have to be very careful.

Hon. Michael Chong: With respect, you are wrong on that. The Privacy Act exempts parliamentary committees and other judicial proceedings from the terms of the Privacy Act. That's stated in the opening clauses of that act, which is an act of Parliament. We are exempt from the provisions of the Privacy Act and we're asking questions in respect of employees of the Government of Canada. We went through that in the previous Parliament on this very committee, actually, when we were asking for these documents.

If you don't know the reasons why they resigned, that's fine. I'm just asking the questions. I take it that you don't—

Hon. Mark Holland: Madam Jeffrey responded to the fullest extent that I could have provided as an answer.

Hon. Michael Chong: Okay, thank you.

Is there any collaboration between the national microbiology laboratory in Winnipeg and entities in the PRC presently?

Hon. Mark Holland: No.

Hon. Michael Chong: Are there any scientists working for the Government of Canada who are participating in the thousand talents program?

Hon. Mark Holland: I would refer to Madam Jeffrey to make sure that I'm not....

Ms. Heather Jeffrey: This case is the only one that I'm aware of where our scientists were participating in this program, and I'd refer you to our security services for information. This was an undeclared collaboration—

Hon. Michael Chong: That's right; you're correct. The Government of Canada stumbled upon it.

Has there been a review or a proactive request on the part of management within the Government of Canada to ensure that all government scientists are complying with the policies of the government in declaring their participation in the thousand talents program?

Hon. Mark Holland: Yes, and I think it's deeply unfortunate. Again, these are Canadian citizens. They were long-time employees and well-published, eminent scientists, known well throughout North America, who lied to the Public Health Agency. That changed things materially, so at that point in time, you had to ask questions and dig into people's backgrounds in a way that would have been seen as invasive and inappropriate before.

Hon. Michael Chong: Just to clarify, there is no collaboration presently going on between the national microbiology laboratory in Winnipeg and entities and individuals in the People's Republic of China?

Hon. Mark Holland: That is correct.

Hon. Michael Chong: Thank you.

Hon. Mark Holland: I would say, just further to the other point, that there's a requirement, and there always has been a requirement, to declare any affiliations or outside work. That's one of the reasons these people were fired. They lied about that.

Hon. Michael Chong: Yes, agreed. Thank you.

I have a question about non-Canadian citizens. The documents that we received revealed that non-Canadian citizens, specifically PRC nationals, were given access to the lab.

My first question is, who in the Health Canada or in the Public Health Agency of Canada is responsible for granting security clearances at the NML in Winnipeg?

Hon. Mark Holland: I'll go to Madam Jeffrey.

Ms. Heather Jeffrey: The security screening process begins with reliability status checks that are conducted by the security department of the agency. They are then referred to the RCMP and the Canadian Security Intelligence Service for secret clearances.

Hon. Michael Chong: CSIS doesn't grant clearance. CSIS, the RCMP and others provide advice. There is an individual within either Health Canada or PHAC who grants the clearance. Who is that individual?

Ms. Heather Jeffrey: It's granted by the security department of the Public Health Agency.

Hon. Michael Chong: It's a departmental security officer or some similarly titled person.

Why did they grant access to PRC nationals for a level 4 lab, which is contrary to government policy?

Hon. Mark Holland: I think the engagement and the correct....

Go ahead, Madam Jeffrey.

Ms. Heather Jeffrey: Access for those students was through a research affiliate program with the University of Manitoba. Those students did not have clearances under the Human Pathogens and Toxins Act and therefore were not involved in level 3 or level 4 lab work, or in any of the restricted pathogens and toxins.

Hon. Michael Chong: They required top-level clearances to get into the lab.

The Chair: Mr. Chong, I'm sorry, but your time has expired.

Ms. Heather Jeffrey: Yes, they required a security clearance.

Hon. Michael Chong: I have one final, quick point on this.

The Chair: Make it very quickly.

Hon. Michael Chong: It wasn't just students. A senior technician at the Wuhan Institute of Virology—a PRC national—was also granted access to the NML. That was also contained in the documents. They were identified as “individual number 2” in the documents.

Again, it was somebody in the department. It was not the two scientists in question because they're not granting security clearance for their own lab. Somebody else in the department granted them security clearances.

Why are they not being held responsible for that gross negligence in protecting our security?

● (1915)

Hon. Mark Holland: Perhaps I can answer at the back of the next question.

The Chair: Yes, I think maybe in subsequent answers you can cover that.

We'll now go to Ms. Yip for five minutes.

Ms. Jean Yip (Scarborough—Agincourt, Lib.): Thank you for coming tonight.

Did you want to answer the question?

Hon. Mark Holland: I will. Go ahead and ask your question. I can put it at the end.

Ms. Jean Yip: Sure.

Just to be clear, does Canada have bilateral research collaboration with the PRC's scientists?

Hon. Mark Holland: Today it does not.

Ms. Jean Yip: People have approached me with a number of concerns regarding the security research guidelines and the new named research organizations lists. Some Chinese Canadian scientists feel uneasy or targeted or that their careers could be limited due to having a Chinese name. They're worried about being under a cloud of suspicion.

How do you balance the national interests of security with the concerns of some in the Chinese community?

Hon. Mark Holland: Thank you very much for that question. I think it's an important one.

It's important to distinguish the action of an individual from making collective statements. In this instance, these were two Canadian citizens who engaged in reprehensible actions that are reflective of them and only them. I think we have to be very careful, when we're talking about scientists or any individual, not to ascribe anything to anyone other than the people who were responsible for taking those actions.

In this geopolitical environment, with tensions being where they are with China, it's very difficult to separate out the actions of the Government of China from those of the citizens of Canada who happen to have Chinese ancestry or, for that matter, people living within China. There are unbelievable numbers of wonderful Chinese scientists doing incredible work for the betterment of humanity in China now. We cannot allow the actions of the Chinese government to colour our view and create the kinds of distortions that you're talking about. We have to root that out.

I would suggest that we need to step back and consider very carefully how we address these issues. I always think of first principles. The first principle, as everybody in this room agrees, is that protecting our nation from foreign interference is our top priority. We have to protect this country. Beyond that, we have to protect democracy.

We would secondarily agree that any attack on the scientific community or on the domestic affairs of this country is an attack upon all of us. Every member of Parliament is equally affected by that.

Thirdly, the actors engaging in this are separate and apart from any community. They are either a government actor or individuals making these decisions. We have to not view them in the context of a community.

We have to think very carefully because we've seen, historically, that when broad characterizations are made and we are not careful with the brush we paint with, we hurt a lot of very innocent people. I think we have to be very careful about that.

Ms. Jean Yip: Ms. Jeffrey or Ms. Huggins, do you have any comments that could perhaps reassure Chinese Canadian scientists?

Ms. Heather Jeffrey: I'd say that this is one of the reasons it's very important that any allegations or indices are tested through investigation by the appropriate security agencies and that evidence is collected through all of the means and tools at their disposal. In this instance, we had individuals who misrepresented themselves. Those who have not done so have nothing to fear from this process, and we need the talents of all of our scientists in Canada.

Hon. Mark Holland: Maybe I could add to that. This is one of the really dangerous things here, because what we don't want to have happen is for the national microbiology laboratory or anybody who's working in the area of virology, vaccines or therapies to start being afraid of collaborating. It is the lifeblood of scientific discovery. The threats we face from the potential of new pathogens are extraordinary. We need to, wherever possible, work with folks.

As to the part of the questions, looking back five years, about why we were collaborating and why we were working like that, it's because these people are earnestly trying to find solutions that save human beings. It is so sad that now these lines are having to be drawn and that we're losing international partners.

We can't allow further barriers to come to innocent Canadians, people who have done nothing wrong and who are leaders in their field. We can't have suspicion cast upon them, have people not collaborating with them and have their research not being listened to. In our fear of one thing, we can't create a shadow that does incredible damage in another area. We have to hold that in our minds as we debate these issues.

● (1920)

The Chair: Thank you, Ms. Yip. That's your time.

We'll now go to Monsieur Bergeron for two and a half minutes.

[*Translation*]

Mr. Stéphane Bergeron: Thank you, Mr. Chair.

I want to go back to what I was saying a few minutes ago. Despite the indications, we didn't seem to draw the conclusions we should have drawn over the past 20 years. In addition, it seems that the objective and tangible facts were not properly assessed.

For example, in the case of Xiangguo Qiu, the Government of Canada listed the research organizations with which she was affiliated. However, that list didn't include the Wuhan Institute of Virology and didn't mention that it applied to be part of the People's Republic of China's thousand talents plan.

How is it that this crucial information was not included with the list of organizations Ms. Qiu was associated with?

Hon. Mark Holland: In my opinion, the person you're talking about lied. Misinformation does happen, and it's terrible, unacceptable.

I simply don't understand why a Canadian citizen, a well-known scientist throughout North America, would misrepresent the facts like that.

Mr. Stéphane Bergeron: Mr. Minister, I'd like to ask you a question.

In a highly secure lab like the National Microbiology Laboratory in Winnipeg, when you make up the list of organizations a scientist is associated with, is it simply based on voluntary reporting or is there some sort of security screening?

Hon. Mark Holland: It's not voluntary; people are required to report all interactions and all the work they have done. It's mandatory.

Mr. Stéphane Bergeron: From what you're telling me, Mr. Minister, I understand that we rely on the person's word and that we don't call on our intelligence service to verify that.

Hon. Mark Holland: Yes. That's changing.

At the outset, especially in the case of an individual who is really well known, who has worked for the Government of Canada for a long time, it's their responsibility as a Canadian citizen to reaffirm their commitment, among other things. However, for new employees, the Royal Canadian Mounted Police and CSIS check personal data, security clearance, relationships and that sort of thing. That's done as well.

However, in that environment, and particularly at that time, it was possible to lie and create the conditions to spread misinformation. That's how things were. We're now working very hard to make sure we batten down all the hatches.

[*English*]

The Chair: Thank you, Mr. Bergeron.

We'll now go to Mr. Desjarlais for two and a half minutes.

Mr. Blake Desjarlais: Minister, I want to turn now to a question of opinion that is likely to form a question of policy in your mind as a minister. I think many Canadians want to understand what you think about particular issues as they relate to decisions of today. How important is security, communication and audit and evaluation work for your department?

Hon. Mark Holland: It was and is essential. I think every time a nefarious actor behaves in an unthinkable way, you learn. That certainly happened here. The behaviour of these two individuals created process improvements to ensure that similar actions couldn't be undertaken in a contemporary context.

Mr. Blake Desjarlais: You'd say that it's very important.

Hon. Mark Holland: It's essential.

Mr. Blake Desjarlais: It's essential, but your department plan as of February 29, 2024, indicates that you'll be cutting these three areas. As it relates to the Winnipeg incident, I think it's quite irresponsible to be making financial cuts in this area.

Can you describe why your department has tabled plans to make significant cuts to these three programs?

● (1925)

Hon. Mark Holland: I'm not aware of any cuts, so I—

Mr. Blake Desjarlais: It's in your departmental plans. Have you read your departmental plans you tabled on—

Hon. Mark Holland: Yes, I have, but I'm not aware of any cuts.

Madam Jeffrey.

Ms. Heather Jeffrey: We're not making any reductions to our security expenditures except for those related to the oversized nature of our pandemic response. Of course, our departmental estimates are coming down off that peak, but we in fact are making new investments in cybersecurity, IT restructuring and our security.

Mr. Blake Desjarlais: To clarify, you're saying that—

Hon. Mark Holland: To colour that, because it's important, I didn't understand—

Mr. Blake Desjarlais: Yes, please clarify.

Hon. Mark Holland: You could imagine that during the pandemic, the Public Health Agency was scaled up radically to meet the demands of the pandemic—

Mr. Blake Desjarlais: Do you mean for the areas of security, communication and audit evaluation?

Hon. Mark Holland: It was for every aspect, because you can imagine that the number of employees we had was vastly larger. For example, if you have to run security checks for a much larger workforce, there will be increased costs. If you have a smaller workforce, you'll have less need for security. Any reductions in security have nothing to do with a reduction in security; they have to do with a scaling back of the workforce, moving into a postpandemic period.

Mr. Blake Desjarlais: What level did you return it to, then?

Hon. Mark Holland: We're above prepandemic levels, 2019 levels, and we're making continued investments to go beyond that, some of which I look forward to talking about in the coming days. We're above where we were prior to the pandemic.

Mr. Blake Desjarlais: In terms of judging how you allocate resources particular to these areas, in light of the Winnipeg incident, how do you justify, or not, the increase?

Hon. Mark Holland: I think the investments have been appropriate, and they continue. There are, across the spectrum of health, unbelievable needs. Every moment you take from one area, you have to give to another, and there's a limit to what you can do fiscally.

I would say the increased investments we've made in security and in the protection of our facilities are extremely important, and we will continue to make the investments needed to—

Mr. Blake Desjarlais: The cuts were COVID-related, though, to summarize.

Hon. Mark Holland: Exactly, yes.

Mr. Blake Desjarlais: Thank you, Mr. Chair.

The Chair: Thank you, gentlemen.

Dr. Ellis, the final five minutes are yours.

Mr. Stephen Ellis (Cumberland—Colchester, CPC): Thank you very much, Chair, and thank you, Minister.

Back in 2017, Minister, the United States raised questions about the Chinese Ministry of Defence's Academy of Military Medical Sciences and its Institute of Microbiology and Epidemiology, saying that they were a risk of potential biological weapon capabilities. Doesn't that fly in the face of you saying that we had a great relationship with China then?

Hon. Mark Holland: I don't recall saying we had a great relationship. I said there were at that point in time emergent concerns around the way in which China was engaging internationally. There were some early warning signals that things were beginning to turn in a bad way. However, the management of risk—particularly when we're talking about deadly pathogens, trying to find answers and thinking that you would try to use information around therapies and vaccines for some sort of geopolitical military purpose—was a different dimension at that moment in time.

Mr. Stephen Ellis: Realistically, Minister, clearly the United States identified that they were talking about a small-scale offensive biological weapons program—

Hon. Mark Holland: At that moment in time—

Mr. Stephen Ellis: You've talked a lot about Ebola. When you think about it, wouldn't you use Ebola to do that? Wouldn't that be a great pathogen to do it with?

Hon. Mark Holland: No, actually. What I would say is that the international co-operation—

Mr. Stephen Ellis: No [*Inaudible—Editor*], is that what you're saying?

Hon. Mark Holland: You're not letting me finish my sentence. What I'm saying is—

Mr. Stephen Ellis: You're not answering the question.

Hon. Mark Holland: I'm attempting to answer it.

What I'm saying is that international collaboration at that moment in time was with respect to Ebola and any number of other pathogens happening on the international stage. China represents a billion people. It has an enormous wealth of knowledge and information—

Mr. Stephen Ellis: I don't need to know about China—

Hon. Mark Holland: No, but we wanted them to be part of that solution.

Mr. Stephen Ellis: Don't you think that this is dangerous?

Hon. Mark Holland: I think it's dangerous to give up on collaboration with a billion people. Unfortunately, we had to do that because the threat environment evolved.

Mr. Stephen Ellis: Even though we have scientists sending a potentially weaponized virus to a power that's going to make biological weapons, clearly you think that's okay.

Hon. Mark Holland: No. I think Ebola exists today as a deadly pathogen.

Mr. Stephen Ellis: Is that okay with you or is it not?

Hon. Mark Holland: Ebola exists and is easily found. There are outbreaks all over the world.

Mr. Stephen Ellis: No, that's not true, Minister, because do you know what?

Hon. Mark Holland: Well, there are outbreaks all over the world, and—

Mr. Stephen Ellis: They didn't have it.

Hon. Mark Holland: —China's objective was to—

Mr. Stephen Ellis: Excuse me.

Hon. Mark Holland: Look, I don't know if you want me to answer or not. I guess that's up to you.

Mr. Stephen Ellis: At the Wuhan Institute of Virology, they didn't have Ebola until the scientists at the national microbiology lab sent it to them. They did not have it.

Hon. Mark Holland: There have been regular outbreaks of Ebola over the last 20 years.

Mr. Stephen Ellis: Did they have it in Wuhan before it was sent from Canada or not? It's a simple question.

Hon. Mark Holland: What I would say is this. Ebola exists today. It has existed for decades as a deadly pathogen, and it doesn't need to be weaponized. It already is.

Mr. Stephen Ellis: Minister, I didn't ask you for a lecture on Ebola.

Mr. Yasir Naqvi: I have a point of order, Chair.

The Chair: Mr. Naqvi, go ahead.

Mr. Yasir Naqvi: I think this committee was going so well. Some very thoughtful back-and-forth took place among members from all parties, and all of a sudden I'm seeing a behaviour that I saw from Mr. Ellis at the HESA committee, which is highly inappropriate. I think it's undervaluing the work this committee is doing on this very important topic.

Pose a question, wait for the answer and get the answer. You may not like the answer, but at least give an opportunity to have a respectful discussion between the member and the speaker. I just—

● (1930)

Mr. Stephen Ellis: I didn't ask for a lecture on Ebola. Thanks.

Mr. Yasir Naqvi: Thank you for interrupting. Mr. Ellis just made my point by interrupting another member on a point of order.

Did you come here with a certain attitude, or are you here to make sure there is respectful conversation happening, as was being done by other members from your own party and other members of the committee?

The Chair: I think that—

Hon. Mark Holland: Perhaps I could have just 10 seconds, Mr. Chair, to respond. Can I have a 10-second runway to answer the question?

The Chair: Well, no. We've stopped the clock because I want Dr. Ellis to have his full five minutes.

Mr. Stephen Ellis: Thanks very much, Mr. Chair. I appreciate that.

The question—

The Chair: Dr. Ellis, if I could, please.... Again, this is just for the interest of our interpreters. When we talk over each other, it makes things very difficult for them, so I would ask, out of respect for them, that we keep things orderly.

Mr. Stephen Ellis: Yes, maybe if the minister would answer the question. We'll move on from there. I guess that's the question we'll leave.

Are there other thousand talents program scientists working in other Canadian labs run by the Canadian government?

Hon. Mark Holland: None that we are aware of, no, and I can say that there's no weaponization—

Mr. Stephen Ellis: Thank you, Minister. I appreciate that answer.

Hon. Mark Holland: To the other one, there's no evidence of weaponization—

Mr. Stephen Ellis: Chair, are we going to have this guy answer the question? Once he does, he doesn't need to keep talking. He answered the question. I'm quite satisfied with that.

Hon. Mark Holland: Well, I was attempting to answer the question. I didn't get a chance to answer before because you were interrupting me, so I don't—

Mr. Stephen Ellis: To move on from that, then, have you done an extensive investigation to understand if there are other thousand talents program scientists?

Hon. Mark Holland: That would not be conducted by me. I would refer you to intelligence officials for what actions they have taken.

Mr. Stephen Ellis: Is that investigation ongoing?

Hon. Mark Holland: My understanding is that those officials are going to be before this committee, and there will be an opportunity—

Mr. Stephen Ellis: Is the investigation ongoing now, at the current time, Minister?

Hon. Mark Holland: I'm not responsible for that investigation. It wouldn't be me or my department, but those—

Mr. Stephen Ellis: I didn't ask if you're responsible. I asked you if there was an investigation going on.

Mr. Peter Fragiskatos: I have a point of order, Chair.

Hon. Mark Holland: Those individuals will be appearing before this committee, and you can ask the questions of them.

The Chair: Mr. Fragiskatos, go ahead.

Hon. Mark Holland: If you want to listen to them or give them an opportunity to have an answer, then—

Mr. Stephen Ellis: No, I'm asking you a question.

The Chair: Dr. Ellis, I'm sorry, but we have a point of order.

Hon. Mark Holland: You're not really asking me a question here. You're badgering me, but that's okay.

Mr. Stephen Ellis: Oh, I'm sorry to hurt your feelings.

The Chair: Dr. Ellis, please—

Hon. Mark Holland: You're not hurting my feelings. You're just not letting me get a chance to answer.

Mr. Stephen Ellis: You're not answering the question. That's the biggest problem.

The Chair: Dr. Ellis, please.

Mr. Peter Fragiskatos: Chair, I echo what Mr. Naqvi said. The meeting was going well. These are important issues and no one's denying that, but if we're going to be serious about getting answers that allow for a genuine approach, one that prevents errors like this from happening in the future, then let's at least allow a civil dialogue to take place. That's all we're asking for.

We're going to have a number of meetings on this very issue, it looks like. I don't know whether Mr. Ellis is here as a permanent replacement or he's here temporarily, but I would just ask for the member to act as an adult. I don't know how else I can put it.

Mr. Stephen Ellis: Thanks for the lecture.

The Chair: All right. Listen, we've made our points. Let's keep things cut, neat and tidy, with short questions and answers, and get it done.

Dr. Ellis, you have just a tad over a minute left.

Mr. Stephen Ellis: Thanks very much, Chair.

Considering what we have learned so far, which is next to nothing, what prompted the SDG of the NML to ID Dr. Qiu and Dr. Cheng as potential security risks as far back as 2018?

Hon. Mark Holland: As Madam Jeffrey indicated, there was a process with an update from CSIS on the potential for employees to be approached in an attempt to get information from them, and reviews were undertaken. As part of the review that came out of that process in the fall of 2018, it was found that a patent had been—

Mr. Stephen Ellis: Excuse me, Minister, but that's not true because the patent issue, as we already established, came in October. This was in August 2018. The SDG said to CSIS there was a problem with two scientists. They named Qiu and Cheng. Why?

Hon. Mark Holland: Again, my understanding of the chronology—and Madam Jeffrey can correct me if I'm wrong—is that in August 2018, there was a CSIS briefing.

Mr. Stephen Ellis: Yes, but you're not answering the question, Minister.

The Chair: Excuse me—

Hon. Mark Holland: It was in September 2018 when the patent was discovered.

Mr. Stephen Ellis: That's not what I asked you, though, Minister.

The Chair: We're out of time. I'm sorry, Dr. Ellis.

Minister Holland, I appreciate your appearance here today.

Our hour has gone a bit over. We will now suspend for a few minutes while we line up for the next panel.

● (1930)

(Pause)

● (1935)

The Chair: Everybody, in the interest of time, shall we get back to work and introduce our second panel?

I would now like to welcome David Vigneault, director of the Canadian Security Intelligence Service, and the following officials: Adam Fisher, director general, litigation and disclosure, and Leonard Stern, deputy director general, security screening.

Mr. Vigneault, you have five minutes for some opening remarks.

● (1940)

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

[*Translation*]

Good evening, everyone.

Mr. Chair and members of the committee, it is an honour to join you this evening and to have the opportunity to contribute to your discussion on the matters revealed in the Winnipeg National Microbiology Laboratory documents and, more broadly, on the importance of protecting Canada's research from foreign interference.

My goal today is to provide some clarity on CSIS's role in protecting our research, through its screening mandate, intelligence collection and advice, and stakeholder engagement. I also welcome the opportunity to provide clarity on CSIS's disclosure processes, and how we are working to maximize transparency while protecting sensitive information.

[*English*]

As this committee is well aware, Canada's research sector is 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 whereby details about the source of funds can be obscured or misrepresented. Through deceptive partnerships and collaborations, vital research and novel intellectual property are stolen. The PRC is by far the greatest perpetrator of these activities.

Needless to say, as state actors become more sophisticated, these threats become harder to identify and counter. It is therefore imperative that Canadians work together. This effort begins with informed and transparent discussions among and within all levels and branches of government, as well as with communities, academia and businesses.

As a committed partner in this effort, CSIS continues to investigate, provide advice to the government and, when appropriate, take measures to reduce threats. This work includes close collaboration with other government departments. For example, CSIS leverages its unique tools and access to provide to requesting departments thorough security assessments on individuals who require access to classified Government of Canada information or sensitive sites. This is one of the tools used to protect Canada's research infrastructure against insider threats.

[*Translation*]

Other tools include stakeholder engagement, which, through education and knowledge dissemination, builds resilience against foreign interference, and thus ensures that government investments do not inadvertently advance the research of hostile states in sensitive areas.

While, as an intelligence service, CSIS needs to be able to protect its own intelligence in order to fulfil its mandate, CSIS has also actively been taking measures to increase transparency with Canadians through increased public engagement with communities and institutions on national security issues. CSIS has briefed more than 200 organizations and 1,000 individuals across Canada who are now well informed about possible threats, which has provided them with the tools to protect themselves, their research, and their employees.

CSIS also exercises transparency through regular proactive and responsive disclosures of information. In the case of the Winnipeg lab documents, CSIS worked collaboratively with the panel of arbiters to maximize transparency through sanitization, including by summarizing certain redactions to provide unclassified information. This resulted in the publication of a greater amount of national security information than previously released. The panel recognized that the release of the remaining redactions could be detrimental to Canada's national security.

[*English*]

What is considered injurious to national security is not static; rather, it evolves over time. With the passage of time, these assessments may change. This is why CSIS dedicates subject matter experts to review documents line by line, irrespective of their initial classification, to maximize transparency to Parliament and Canadians.

● (1945)

The PRC has been bold in its attempts to threaten Canada's security, prosperity and research through strategic espionage and foreign interference. To counter these threats, CSIS is continuously implementing lessons in how it responds to the constantly evolving threat environment. This includes increasing transparency with Canadians through an increased openness and willingness to release as much information as possible through processes such as this one.

Finally, I will note that in order to protect the safety and security of Canadians, I cannot publicly comment on operational matters and requirements. Nonetheless, I welcome this opportunity for frank and transparent discussions to the extent that's possible, and will be happy to answer your questions.

[*Translation*]

Thank you, Mr. Chair.

[*English*]

The Chair: Thank you, Director Vigneault.

I should note that we have been rejoined by Ms. Lantsman. It's good to have you there on the screen.

For our first round of questioning, we will go to Dr. Ellis for six minutes.

Mr. Stephen Ellis: Thank you very much, Chair.

Thank you, gentlemen, for being here.

Specifically related to the national microbiology lab, is it true that in August 2018, CSIS provided a briefing to national microbiology lab security officials?

Mr. David Vigneault: Absolutely. As part of its effort to make sure there's increased resilience against threats posed by a number of foreign actors, CSIS engaged in proactive discussions with the Public Health Agency, including the national microbiology lab, about threats and indicators of insider threats. That was a very important and very useful discussion in 2018.

Mr. Stephen Ellis: Mr. Vigneault, I'm not sure how much you may or may not want to comment on this, but is it not true that the SDG of the national microbiology lab brought the names of two Chinese scientists forward to CSIS at that time?

Mr. David Vigneault: My understanding is that these discussions took place a few weeks after that discussion, but they were generated by the initial discussion.

We received names of the two individuals in question, yes.

Mr. Stephen Ellis: I'm not entirely sure, Mr. Vigneault, if you're aware of the timelines, but I'll ask you this anyway.

That would then lead us all to believe that there were concerns about Dr. Qiu and Dr. Cheng before the discovery of the two patents in the PRC registered under Dr. Qiu's name. Is that true, sir?

Mr. David Vigneault: My understanding is that some initial concerns were brought forward by PHAC and the NML to CSIS. As a result, we started further investigations. It's as a result of those investigations that we discovered the information about the patent.

Mr. Stephen Ellis: Is there any more information about the nature of the exact concerns that officials brought to CSIS back in August 2018 with respect to Dr. Qiu and Dr. Cheng?

Mr. David Vigneault: I don't have any other details at this point.

Mr. Stephen Ellis: Is that something you can provide to the committee in writing?

Mr. David Vigneault: I will absolutely endeavour to see what we can do. Of course, there will be limitations over what has already been disclosed through the process. If there is more information we can share, we will do so.

Mr. Stephen Ellis: Mr. Vigneault, given that I realize there are security concerns around this, we asked the minister previously about other ongoing security assessments or investigations of the thousand talents program or like programs. I understand that there's a new name for that program potentially. It's for any scientists working at any government labs in Canada. Is there currently an investigation going on with respect to that?

Mr. David Vigneault: As I mentioned in my initial comments, there are limits to what I can disclose publicly.

If it's helpful, I can tell the member that the thousand talents program is something we're keenly aware of and quite concerned with. The different ways the PRC—or, for that matter, other countries—could try to use this type of program are something that CSIS investigates fairly thoroughly, and we work with our international partners to better understand those dynamics.

Unfortunately, I'm not at liberty to discuss more specific details.

● (1950)

Mr. Stephen Ellis: Mr. Vigneault, are you at liberty to say if CSIS is aware of any TTP-like scientists working in Canadian labs at the current time?

Mr. David Vigneault: Unfortunately, my previous comments would apply to this question as well.

Mr. Stephen Ellis: That's fair enough. I appreciate that.

One of the things we know—the minister talked a lot about this—is that due process is more important than national security. Obviously your lens is a little different than that of the minister. Do you share those comments?

Mr. David Vigneault: I did not have the opportunity to listen to all of the minister's previous comments, but what I can tell you is that as an intelligence service working in a democratic environment governed by the rule of law, we are, of course, keenly focused, as per our mandate, on investigating all threats to national security. We try to do that very thoroughly.

We are also mindful that Canadians are entitled to due process and different procedures. In the case of a security screening assessment, our role is very clear. We investigate and we provide advice to the requesting department, which is the owner of the decision at the end of the process.

Mr. Stephen Ellis: Sir, I might suggest things were a bit different. Things had evolved to the point that early in 2019, this scientist's computer was mirrored, in my understanding from the information we have in the briefing, yet the institution, the national microbiology lab, the scientist worked for allowed a very deadly pathogen—probably two pathogens, Ebola and Henipah virus—to be transferred to an existing level 4 lab in the PRC, the Wuhan Institute of Virology.

Sir, in your assessment of threat and security, does that make any sense?

Mr. David Vigneault: I think the specific dynamic of when, how and under what authority those samples were transferred has been looked at by this committee, and I would argue that the members of this committee have more specific knowledge than CSIS on that very aspect.

What I can tell you is that it is an area of great concern for CSIS when we see that directly or indirectly, covertly or not, the PRC is in any way able to potentially increase their threat activity against Canada and against other western nations and their neighbours. That's the prism through which we look at these issues at CSIS.

The Chair: Thank you, Dr. Ellis. That's your time.

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

Mr. Peter Fragiskatos: Thank you, Chair.

Thank you to all of you for being here tonight.

Mr. Vigneault, to what extent can we say that every democracy is dealing with these kinds of issues in some shape or form, with implications for national security when we look at issues of research and research collaboration?

Mr. David Vigneault: I will use a very specific example to illustrate that point. My colleagues and I, the heads of the Five Eyes intelligence services, took the unprecedented avenue of meeting together in public for the first time in our history in October of last year at Stanford University in the context of talking about innovation and the need to secure innovation for the well-being, prosperity and security of our countries in the future. We had a common assessment, the heads of Five Eyes, that specifically the work of the PRC against all of us, against essentially any organization that has information or know-how that the PRC is interested in, puts us at risk because there is an institutional approach through the thousand talents programs, through covert espionage activities and through open arrangements and investments to try to get information.

What is done in an overt way is not the problem. In the case of the PRC, there is a very specific set of conditions that apply, and the Chinese Communist Party has been very clear that their goal is to have, for example, the most advanced and modern military by 2049. In order to do so, the President of China, Xi Jinping, who is also the general secretary of the Communist Party, chairs a committee of military-civil fusion. In all of the information, know-how and data they acquire, there is an institutional approach to try to leverage it and turn it into a military advantage.

From that point of view, Mr. Fragiskatos, you're right to say that it's not just Canada under threat, but any other country that has something the PRC is interested in acquiring.

● (1955)

Mr. Peter Fragiskatos: What would you say is the message to post-secondary institutions? I represent London, Ontario—or help to represent London, Ontario—in the House of Commons. Western University is in London. We have universities throughout the country that look at medical research and research in general, and collaboration is key to that research in so many different cases.

What message is being relayed either through the Five Eyes or generally? What would you say here to universities that look at situations like this and wonder about security implications for research?

Mr. David Vigneault: This is one of the areas where we have to be very careful in how we engage in these discussions. Canada is a prosperous country because we have excellent know-how, universities and research. This is the basis for our prosperity. We have to be careful not to stifle that innovation, because we will not be where we need to be in 10, 15 or 20 years. That innovation needs to be protected. However, the world has changed, and the number of actors have also changed in the process. The way they are engaging in these activities has evolved to the point where some of these activities are indeed threats to our country.

One of the most important ways to specifically work with universities is to engage in open dialogue and share information with them. We have published unclassified documents that get at the core of this issue.

In the past year, we have engaged directly with universities. We visited 13 universities across the country. We work with the research universities in the country and with Universities Canada to share our information. We meet with academia, student bodies and academic administrators to essentially share with them what we know and the concerns we may have, and to work in collaboration to accomplish two objectives: great innovation in our universities and protecting our national security at the same time. Both need to be achieved.

Mr. Peter Fragiskatos: Beyond universities, you said there were around 200 organizations that CSIS has briefed. What kinds of organizations are we looking at here? What is the nature of those briefings? I ask that question because I wonder if there are particular sectors you're worried about that are more susceptible to threats.

Mr. David Vigneault: Indeed there are a number of specific sectors we're more concerned with, such as quantum technology, biopharma and aviation. We're looking at anything related to cyber. Our agriculture is an area of concern, because we're developing very innovative approaches in our country.

We're meeting with universities, as I mentioned. We're also meeting with industry associations. We're publishing unclassified documents and trying to make them as available as possible.

If it's of interest, I can say that we're also working.... We have been talking about foreign interference. Elements of the approach by the PRC are espionage and foreign interference. They are often two elements of the same strategy. We've been engaging very significantly with the diaspora in the country to make sure we are seen by the diaspora as part of the solution. We share our information, listen to their concerns and better interact with them regarding what would be relevant.

The work of this committee is also very important, because it's increasing the knowledge and know-how we have that we can share through you. It's through these different efforts that we'll increase the resilience of Canada and Canadians.

The Chair: Thank you, Director.

We'll now go to Mr. Bergeron. The next six minutes are yours.

[*Translation*]

Mr. Stéphane Bergeron: Thank you, Mr. Chair.

Good evening, gentlemen. Thank you for being here.

A few moments ago, I reported on an article published in the Journal de Montréal on January 29, 2024, in which we learned that, as early as 2010, you were warning the government of an increasingly aggressive attitude on the part of China, particularly regarding intelligence activities. What we've found is that the government has been slow to pick up the message, so much so that the minister was telling us a few moments ago that, until very recently, employees were essentially relied upon to self-declare in order to get a clear idea of the "pedigree" of the links they had with other institutions.

I don't mean to put you on the spot, but do you feel that the government should have put in place background check mechanisms sooner for people working in a high-level, tier 4 lab like Winnipeg?

● (2000)

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

Mr. Bergeron, your question is very interesting and touches on several important points. One of these matters to consider is China's evolution in recent years, especially since Xi Jinping came to power, the degree of aggression and disrespect for international law...

For example, China has refused to abide by the International Court of Arbitration's 2016 ruling on the South China Sea. Yet the ruling was very clear and unequivocal. This is one of the triggers. Since 2013, when Xi Jinping came to power, various examples like this one demonstrate an important trajectory for China.

At the same time, Chinese legislation and several programs have evolved. For example, the Thousand Talents Program has become much more institutionalized. In some ways, China is very open, but since 2017 and 2018, laws have been put in place to force people, companies and all Chinese people everywhere to collaborate with intelligence services.

I'd also like to mention the evolution and growth of the United Front Work Department. Its approach is to influence and control the Chinese diaspora and influence other countries in order to further Chinese interests.

The United Front Work Department, the Thousand Talents Program and the evolving threat posed by China are all elements that need to be taken into account. In fact, that's what our intelligence services, analysts and experts on China are doing. We need to take the information we have in 2024 and put it in the context of 2010. We have to take into account what we knew at that time, what was known and what measures could have been taken.

Finally, I'd like to add that, in working with my colleagues around the world on issues of Chinese spying and interference, I've been able to see that these behaviours have evolved everywhere over the past few years.

So Canada is also part of this evolution.

Mr. Stéphane Bergeron: When you testified before the committee in March 2021, you were talking about the relationship between your institution and universities. You mentioned that the Canadian Security Intelligence Service maintained "a close dialogue" with universities and that you wished "to be able to engage in dialogues" that were even more extensive.

In March 2024, the CBC reported that the University of Saskatchewan would ultimately host Canada's first level 4 non-governmental laboratory.

Given your institution's limitations on information sharing, how do you plan to collaborate with such a high-level laboratory outside the Canadian government?

Mr. David Vigneault: Once again, that is a very good question.

Mr. Bergeron mentioned the limitations of the Canadian Security Intelligence Service Act with regard to information sharing. The Minister of Public Safety, Mr. LeBlanc, has reported on consultations that have taken place in Canada and his willingness to table amendments to the act. We hope this will happen, as this is one of the existing gaps in our system.

With regard to the laboratory in Saskatchewan, I won't go into all the details, but I can say that we have had discussions, for a long time, with the organization in question to enable the exchange of information and to raise awareness properly.

While coping with the limits imposed by the law, we have been able to start a dialogue, and we hope that this dialogue will go even further.

That said, the dialogue is taking place.

● (2005)

Mr. Stéphane Bergeron: Thank you very much.

[*English*]

The Chair: Thank you very much, gentlemen.

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

Mr. Blake Desjarlais: Thank you very much, Mr. Chair.

I want to thank the witnesses for being present today, and of course for your immense work in keeping Canadians safe and all the work your staff does to ensure that our work to make them safer continues. That's why we're all here today.

The question I want to ask is similar to what Mr. Fragiskatos mentioned about the sectors that are under threat. Coming from Alberta, I know this has been a conversation we've had for a long time, particularly with the development of our oil sands.

In Alberta, as you may know, in 2012 and even previous to that, there was an economic policy by the Conservative Party to find ways to sell off assets, particularly our access to oil sands projects. CNRL, Canadian Natural Resources, was unfortunately sold to Nexen.... Sorry, Nexen was sold to companies controlled by China, and today that's the same.

How much of a threat is the People's Republic of China to our oil sands and to the production and development of research for petroleum products?

Mr. David Vigneault: The question is interesting because you're looking at two things. One is the control and ownership of a fixed asset. You also talked about the development of know-how and innovation. I would make a distinction between something you can control, which is the asset.... You cannot, in the middle of the night, come in covertly and take it over. Knowing and understanding the intent not just of the PRC but of other countries means having the right legislation to make sure that you're able to protect it through the Investment Canada Act, among other things.

A very important question as well is the development of the know-how and innovation. When you look at carbon capture, there are very innovative things happening in Alberta and other parts of the country. We know that if it's of interest to the PRC or some other countries, there will be an effort, either overtly, sometimes through direct engagement, or through other means, including covert espionage, to acquire this know-how and information. We have to be very mindful of that.

At CSIS, we try to look at very specific activities, but we also zoom out and try to understand the cumulative impact of some of these issues and see what the consequence is for Canada's national security not only now but also in the future. This is the advice we try to provide to the government.

Mr. Blake Desjarlais: That's a fantastic answer.

Just to frame that at the time these policies were in existence, I would assume they existed in 2012 when China took over Alberta's oil companies. Is that correct?

Mr. David Vigneault: As I mentioned, what we've seen is that, while some of these conditions already existed, from 2012 to 2024 there's been a very significant evolution and there have been a couple of pivotal moments. One of them has been the ascension to power of Xi Jinping, but a number of other steps have been taken, including the publication of very specific strategies, like “Made in China 2025” and their five-year goals, strategies that are sometimes very overt. They say where they want to be and want to dominate this and that sector.

I think in the evolution we've seen since 2013, some of these elements were there. Some of these dynamics were there in 2012, but we've seen a dramatic acceleration.

● (2010)

Mr. Blake Desjarlais: I see that. I hope you can see my curiosity and the very problematic connection that comes to mind when I think of the control of Alberta's oil asset, petroleum, which is an immense resource we have here in Canada, particularly in Alberta. I see your concern of the potentials, especially if we're looking at the PRC's mandate to have the strongest, most technologically advanced military by 2049, as I believe you said. Those two things in my mind present a credible risk. If they have control over physical resource assets like petroleum, an incredibly important asset for war and the military, they would also have access to the information that supplies it.

Do you believe the ownership of these companies should be challenged, especially now in light of what we're seeing with very aggressive modes of information and hostile actions?

Mr. David Vigneault: That's a question I honestly would have to reflect upon. In the last number of years, the specific ownership of those resources has not been as much at the top of our agenda.

I will reflect on this, Mr. Desjarlais, and may bring back something more intelligent to share with you.

Mr. Blake Desjarlais: I would appreciate that and look forward to hearing from you. Maybe you can supply that in writing at a certain time to this committee, when it's appropriate for you to review that information and supply an opinion or response.

Mr. David Vigneault: Yes.

Mr. Blake Desjarlais: I understand I have 30 seconds, but I want to ask a question that I asked the minister about impacts of this study and other studies related to the Winnipeg lab. It's on our relationship with our partners across the globe, particularly the Five Eyes and NATO. Did that serious breach of information present a credible risk to our partners, and did they present that risk to you as a question or recommend ways to reduce that risk?

Mr. David Vigneault: As I mentioned, we are working extremely closely with not just our Five Eyes partners, but a number of other extremely sophisticated intelligence services around the world. CSIS has over 300 relationships around the world with intelligence services, and this is one of the very significant issues we're talking about.

Each country has challenges when it comes to the penetration of institutions and espionage activities. That is one of the reasons we share so much together at the classified level. It is to collectively be more resilient and learn from each other. You can be sure that in a case like this, the lessons we learn as an intelligence service are shared with our partners to make sure, again, that we raise the bar and make it harder for hostile actors to threaten our well-being.

Mr. Blake Desjarlais: Thank you, Director.

The Chair: Thank you, Director Vigneault.

We'll now go to Mr. Chong for five minutes.

Hon. Michael Chong: Thank you, Mr. Chair.

CSIS has assessed that foreign interference from the PRC is a serious threat to Canada. I want to quote what CSIS has assessed: “Foreign interference is a complex national security threat. It poses a significant threat to the integrity of our political systems, democratic processes, social cohesion, academic freedom, economic prosperity and challenges Canadians’ rights and freedoms.”

You mentioned earlier in your testimony that espionage is not exactly the same thing as foreign interference, but it's very closely related. How do you assess the PRC's espionage activities in Canada in terms of threat?

Mr. David Vigneault: Because of the organized systematic approach and capabilities of the PRC, we assess that the PRC is the most significant espionage threat against our country.

Mr. Chong will know that the dynamic is somewhat similar to foreign interference in the sense that you have a continuum of activities. The intent is very clear. One of them, for example, is to have the most sophisticated modern military in 2049, and, through the five-year programs, to dominate certain aspects of the economy in the future. The means can vary from the overt to the very much covert, and in the dynamic we see in foreign interference, we see the same thing. We see legitimate means of engaging in our economy that are absolutely appropriate. I've talked to different companies that are essentially telling us they know, when they get into some deals, that they will lose intellectual property.

It's very sophisticated, up to and including very covert espionage.

● (2015)

Hon. Michael Chong: Thank you for that answer.

You mentioned earlier in your testimony that CSIS is concerned with the thousand talents program. How do you assess the thousand talents program with respect to government scientists? In other words, do you think it is appropriate for Government of Canada scientists to participate in the thousand talents program or any of the 200 or so other recruitment programs of the People's Republic of China?

Mr. David Vigneault: I will reiterate what I said earlier in the sense that in these types of cases, we do an assessment of the generic nature of those talent programs. That's one thing. Then at the request of the agency, we do the screening of very specific individuals and provide that assessment, that advice, to the host agency for them to make determinations.

The reason I reiterate this point, Mr. Chong, is that there might be some circumstances in which it is totally transparent and it is an activity that would benefit Canada and, in this case, China. There might be some cases like that, so I would not want to be categorical and say one hundred per cent no—

Hon. Michael Chong: It could be appropriate in some cases and not in others.

Mr. David Vigneault: They have to be very transparent. That is one of the key issues at play here.

Hon. Michael Chong: That's understood.

We know that Dr. Qiu clandestinely and corruptly co-operated and collaborated with the government and the military of the People's Republic of China. She also received payment for travel within the People's Republic of China from both of those entities and did not declare it with the Government of Canada.

One of the entities she clandestinely collaborated with was the Wuhan Institute of Virology. The Wuhan Institute of Virology is not on the list of named research organizations of the Government of Canada, so it is technically possible for a government entity to collaborate with that organization.

Do you assess that to be an acceptable security risk, particularly in light of the fact that according to publicly sourced reports, Dr. Qiu is working at the Wuhan Institute of Virology—or working with scientists there—as we presently speak?

Mr. David Vigneault: I would say that having entities listed by the government as problematic is a very welcome approach. It speaks to Mr. Fragiskatos' question earlier about how we work with people. Giving them more information about what might be appropriate or not is very important. In this case, listing these organizations and telling them why there might be a problem help people make their own decisions. We at CSIS have provided advice to ISED and Public Safety, which came up with that list.

In the specific case of the Wuhan institute, again, there might be legitimate reasons why, for the benefit of Canada, it would be appropriate to work with them. I think it would be useful in this case, if there were to be any such arrangement, to ask specifically what kind of due diligence has been done on these—

Hon. Michael Chong: I have just a very quick, final—

The Chair: I'm sorry, sir. You are out of time.

We'll have to go now to Mr. Erskine-Smith for five minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much, Chair.

As the director of CSIS, you are one of the people in this country who thinks about national security more than most. When you reflect on the timeline here, there have been accusations of delay and inappropriate due diligence.

As of August, a lab employee identifies two colleagues who might be targeted by the PRC. In September 2018, PHAC, through some due diligence, becomes aware of a patent filed by Dr. Qiu. Later that year, in December 2018, a security consultant is engaging in fact-finding and ultimately reports to PHAC in March 2019. The RCMP escorts the individuals out of the lab in July 2019.

When you reflect on that timeline, do you think PHAC acted with appropriate due diligence?

Mr. David Vigneault: I think this chronology is very instructive because now, with what we know in 2024, it's easy to look back at the events of the day and try, with the knowledge we have....

I was talking earlier today to my colleagues who are responsible for the screening branch, looking at those dates and so on. My experts were telling me that as far as cases go, this one was very quick to come to fruition.

I know there were some questions about due diligence and due process, but one thing that is important is how to start to mitigate the threat significantly. These individuals were walked out and not given access to their information in the lab itself. This is one way to mitigate the threat while the rest of the investigation takes place.

I will reiterate, Mr. Erskine-Smith, that my expert colleagues have told me that they thought it was a fairly expeditious process.

● (2020)

Mr. Nathaniel Erskine-Smith: I appreciate that.

In your view, from a security vantage point, what more could PHAC have done? These individuals we're talking about are employees from the early 2000s. This is not an infiltration operation. This is an operation where they were ultimately co-opted down the road of their careers, which strikes me as a more challenging thing to screen, all things considered.

I wonder what your view is as the director of CSIS. What more could and should PHAC have done in the circumstances to mitigate the risks that ultimately were realized?

Mr. David Vigneault: The way I'll try to answer this question is to say that of course, as Mr. Erskine-Smith mentioned, we look at the issues through a national security prism. We make an effort to share our knowledge, our expertise and our concerns with our colleagues to make sure that one of the filters through which they look at issues within their organization is a national security aspect. Increasing the security culture of these organizations is one thing we're very keen to do.

It is more of a generic comment, as opposed to a specific one, looking back at times.... Anytime we can work more closely with organizations to increase what I would refer to as a connective tissue between national security and their business, it makes Canada and these organizations more resilient.

Mr. Nathaniel Erskine-Smith: That's a very good answer.

I was amazed by this, actually. I read the April 2020 security assessment, the first security assessment, and it's pretty thin. There was an interview, and Dr. Qiu lies straight up to your officials. Then mere months later, on June 30, there is a second security assessment, and it's incredible what your agency was able to glean and document in a mere matter of months, especially with a level 4 lab. That close relationship between CSIS and a level 4 lab is essential, is it not?

Mr. David Vigneault: Yes, absolutely.

As I mentioned, the evolution of the threat activity of the PRC and other countries against Canada has been such that we had to change our approach at CSIS. We have to collect, very covertly, intelligence and secrets, which the government—Parliament, essentially—through the CSIS Act, is asking us to do. At the same time, we need to increase our transparency, because the ecosystem in Canada has changed because of those threat actors.

When you look, Mr. Erskine-Smith, at the dynamic in the lab at the time and the dynamic with the organization, I think what you see is the realization of that threat, but also a number of people who started turning to security issues much more significantly. Again, I commend the work of this committee, because I think through this work, more Canadians will be thinking about these issues. This is only way to more transparency, which will increase our resiliency. I would say that—

Mr. Nathaniel Erskine-Smith: I'm out of time, but I have two questions—

The Chair: I'm sorry, gentlemen, but you are out of time. It goes by very quickly.

Mr. Nathaniel Erskine-Smith: All right. Thanks a lot.

The Chair: Mr. Bergeron, we have two and a half minutes for you.

[*Translation*]

Mr. Stéphane Bergeron: I'd like to ask two quick questions, Mr. Chair.

First, if CSIS gets wind of the fact that a top researcher in Canada is part of the Thousand Talents Program, does it intervene?

Secondly, the Laboratories Canada strategy, adopted in 2018, which includes state-of-the-art work environments protected against cybersecurity threats, will extend over a 25-year period. Do you think we need to act faster?

Mr. David Vigneault: I don't know the details of the strategy, which is spread over a 25-year period. However, I do know that government strategies of this nature are implemented over several years. However, we always try to manage the most important threats as quickly as possible.

What was your first question, Mr. Bergeron?

Mr. Stéphane Bergeron: My first question was about the top researchers who are part of the Thousand Talents Program.

Mr. David Vigneault: Absolutely, yes. If our security screening work or our intelligence gathering work tells us that any individual in Canada is involved in a program being run by China or another country, we will intervene.

Mr. Stéphane Bergeron: Thank you very much.

● (2025)

[*English*]

The Chair: Mr. Bergeron, I still have you down for a minute.

[*Translation*]

Mr. Stéphane Bergeron: Do I have a minute left? My goodness, that is a luxury.

[*English*]

The Chair: Your questions were short for a change. You fooled yourself.

[*Translation*]

Mr. Stéphane Bergeron: We've learned that, among the charges levelled against the two researchers, one was the fact that people were allowed to work unescorted inside the laboratories.

How could such a thing happen? In your opinion, is this the kind of practice that can still go on, or has it been tightened up since then?

Mr. David Vigneault: As far as I know, we've learned from our mistakes.

Our colleagues at the Public Health Agency of Canada have been very rigorous in implementing these lessons to plug some of the safety loopholes that existed. To the best of my knowledge, these practices no longer exist.

On the other hand, the very nature of espionage and counter-espionage work means that the more useful and effective our tactics and techniques for understanding and gathering intelligence become, the more our adversary changes techniques to make our task even more difficult. So it really is a game of cat and mouse. We can't sleep soundly thinking it's all settled. That's why I always talk about partnership and dialogue between national security experts, like those at CSIS, and the organizations, because the situation, techniques and methods of espionage are evolving.

So we have to evolve at the same time.

Mr. Stéphane Bergeron: Thank you.

[*English*]

The Chair: Mr. Desjarlais, it's two and a half minutes for you.

Mr. Blake Desjarlais: Thank you very much, Mr. Chair.

I now want to turn to what I believe to be an overarching concern related to China, which is the potential of China organizing global allies toward their own ends. I know the mandate of this committee is more narrowly specific to China, but my concern is largely how China could be leveraging its state supporters to meet the ends that you described at the very outset of our meeting today.

The greatest potential and greatest risk that I perceive from your comments in today's meeting is the plan towards a larger military, which from the New Democrat perspective is bad for peace. Of course, when you have larger and larger militaries continuing to gather, it makes an inevitable situation likely. I think it's a major concern for not just Canadians but the globe writ large.

How concerning is China's relationship with other state actors toward what could potentially be a really serious collision course with NATO and our allies?

Mr. David Vigneault: One of the significant by-products, if you will, of Russia's invasion of Ukraine has been a rapprochement between the People's Republic of China and Russia. We're talking about two dictatorships. We're talking about two authoritarian systems that collaborate because they see an interest in doing so for each one of them. The dynamic of an increased military collaboration between the PRC and Russia is of concern. We see also a rapprochement with North Korea. When you start to look at the security dynamics in that part of the world, you start to see a number of indicators going in the wrong direction.

For Canada specifically, we see that the PRC has invented a new concept and declared themselves a near-Arctic state. That did not exist before, but now it exists, at least in their nomenclature. It's for the specific purpose of trying to increase their capabilities for operating in the north, including in the Canadian Arctic. They see economic potential with climate change and the opening of sea routes in the north, but there's also a military component to this. From a Canadian point of view, we are concerned about, specifically using this example, what is a potential direct impact on Canada's security now and in the future.

Also, as you mentioned, Mr. Desjarlais, there's the question of the global instability that is created by military arrangements, the sharing of military know-how and the sharing of equipment in that part of the world. This is of significant concern now but also in the future.

● (2030)

Mr. Blake Desjarlais: Thank you, Chair.

The Chair: Thank you to you both.

To take care of our final two five-minute periods, we will go to Mr. Chong and then Mr. Naqvi, who will wrap this up.

Mr. Chong.

Hon. Michael Chong: Thank you, Mr. Chair.

The Government of Canada outsources to and contracts with a lot of outside individuals and companies. ArriveCAN has obviously been in the news recently, but one thing that surprised me in reading the documents we received was that a private company did some parts of the investigation.

Why is a private company, in this case Presidia Security Consulting, doing security investigations for the Government of Canada? What is your view of that? Secondly, what is the relationship between CSIS and this private company in respect of these investigations?

Mr. David Vigneault: I think it's an interesting point in the sense that some organizations may have more in-house capabilities to do some of these sophisticated investigations.

In this case, Mr. Chong, I don't know if you've had the chance to ask PHAC a question on why they did that. In my experience, one of the issues is that people do not have enough expertise in some specific areas. I'm speaking in a general manner. I don't know. There is no relationship between CSIS and such an organization for the simple purpose that there is nothing we can share with them. We would not be sharing our techniques and methods and our information with them.

I would say again, at a general level, that there might be scenarios in which it could be useful. Some private companies have a lot of very good expertise in niche areas of investigations, so that might be useful, but that of course needs to be complemented, especially if you're talking about government assets and government information, with a government investigation. This is where CSIS would have to come into play. Of course, in the context of potential criminality, our colleagues at the RCMP need to be engaged.

Hon. Michael Chong: In other words, the department and the agency are responsible for carrying out the investigation with their own resources, and if they don't have them, they contract a private company to do that. I would have thought that if there was a security concern within PHAC, they would have contacted Government of Canada authorities such as CSIS or the RCMP to conduct the investigation rather than hiring a private contractor to do the work and gather the information.

Mr. David Vigneault: Our mandate at CSIS is fairly clear in this circumstance. We would investigate the national security threat and do the security screening aspect, but everything between those arcs, the administrative portion, we would not be equipped to do. It would not be appropriate.

I want to reiterate that I was making a general comment when I said that—

Hon. Michael Chong: Yes, I understand.

Mr. David Vigneault: —so I don't know the rationale for PHAC.

Hon. Michael Chong: I have a related question.

CSIS does intelligence assessments, so if an individual wants to get clearance to go into the Winnipeg lab, CSIS will do the assessment on that individual and provide advice to the department or agency. Within the machinery of the Government of Canada, who is normally responsible for granting that security clearance? Is it the deputy minister or head of the agency, such as the president of PHAC? Who is it normally, and can those authorities be delegated?

Mr. David Vigneault: According to the government security screening policy, the authority rests with the deputy head of each organization.

Hon. Michael Chong: It's the deputy head.

Mr. David Vigneault: Yes.

In terms of the delegation of authority, I believe it is possible—

● (2035)

Hon. Michael Chong: In the case of PHAC, would the authority responsible for the NML and for granting the security clearance be the president?

Mr. David Vigneault: Yes, the authority is indeed through the president or the deputy head. It's the same for revocation.

Hon. Michael Chong: I understand. Thank you.

My last question concerns a report. There's basically one level 4 lab in Canada and it's in Winnipeg. There are two parts to it, the animal side and the human side, one side run by CFIA and the other run by PHAC. It was reported last month that the University of Saskatchewan is interested in setting up a level 4 lab. Do we have the state capacity in Canada to have another level 4 lab, particularly at a non-governmental institution, in light of the massive security breaches we saw at the government's lab in Winnipeg?

Mr. David Vigneault: I'll be very transparent with the member: This is not an issue we at CSIS have looked at.

I have not personally looked at the capacity the way you referred to it, Mr. Chong.

In answering Mr. Bergeron's question, I mentioned we have already connected and engaged with the Saskatchewan entity that is looking to establish that lab. Again, if there's one thing that will come out of the work of this committee, I think it's that everybody will be even more aware of, concerned with and, I would expect, diligent in the setting up and security aspect of any such lab.

Hon. Michael Chong: Thank you.

The Chair: We'll go to Mr. Naqvi for five minutes.

Mr. Yasir Naqvi: Thank you, Chair.

Thank you for being here, Director Vigneault, Mr. Stern and Mr. Fisher.

Director, you spoke about the processes in 2018 and 2019, and it's your testimony that, looking back, you felt the matter was dealt with in a fairly expeditious manner.

I want to ask you a forward-looking question. Having seen this process and the changing climate around safety and security as it relates to the PRC, what do you think needs to happen to improve processes around a level 4 lab and other government apparatuses that may deal with foreign countries?

Mr. David Vigneault: I think what we realized is that the dynamics in our countries have been changing for some time. There are a number of threat actors, unfortunately, who are after what we have. They want what we have here: our know-how, expertise and intellectual property.

As I mentioned before, there are a number of different elements.

One, you need to talk about these issues. It cannot just be in the confines of CSIS where these issues are of concern. It should be part of a societal discussion. Unfortunately, there are threats to our national security and we need to talk about these. That's one aspect.

The second aspect is to make sure you create the right connective tissue, to use the expression I used before, between different organizations. People need to know each other a bit. People need to have confidence. If I have a concern, where do I go and how do I engage in these discussions?

We definitely do not have all the answers at CSIS; we do not know everything. I would like to think we know a few things, but at the same time, what we need, not just with many other federal government entities but also with provincial, municipal and academic institutions and research laboratories, is to have areas where people will talk to each other. In the last number of years, I have seen an increase in the number of organized venues, formal and informal, for information exchange.

The last thing I would say, as we say in French, is this:

[*Translation*]

I'm going to preach for my parish.

[*English*]

It's important to make sure you know that the organizations dedicated to protecting national security have adequate capacity to do that, including through legislation.

Mr. Yasir Naqvi: My last question for you encapsulates the general themes you just spoke about that should be kept in mind moving forward.

Are there specific recommendations on improvements to rules and processes that you can provide, as CSIS, to this committee in writing that can help us in our report writing given what we saw? How can we improve things moving forward?

● (2040)

Mr. David Vigneault: I welcome the opportunity. I will work with my colleagues and endeavour to provide some of our thoughts and potentially even bold advice to the committee.

Mr. Yasir Naqvi: Thank you for your time, sir.

The Chair: Thank you, Mr. Naqvi.

That brings us to the end. We appreciate all the questions and certainly our witnesses Mr. Stern, Mr. Vigneault and Mr. Fisher.

I want to thank the clerk, the analysts, our interpreters, the staff and the service staff.

Hon. Michael Chong: I have a quick point of order.

I noticed we're meeting on Friday afternoon.

The Chair: Yes, we are.

Hon. Michael Chong: I was told today that the only Wednesday slot available is 7:30 p.m. to 9:30 p.m.

Could we quickly canvass members of the committee on whether they want to meet on Friday afternoon or Wednesday evening? I'm agnostic. I realize it's quite a late Wednesday slot. I thought it was earlier in the day.

The Chair: Can we have the clerk follow up with everybody and get everybody's thoughts and feelings on that?

Hon. Michael Chong: Sure.

The Chair: We will certainly go with Friday this week.

Hon. Michael Chong: Okay. We'll see about next week.

The Chair: We will see about the wishes of the committee, even though Wednesday evening would be a horrible imposition on your chair. I don't want to play the big victim here, but we will leave that to your conscience, sir.

Hon. Michael Chong: Thank you, Mr. Chair.

The Chair: With that, the meeting is adjourned.