HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

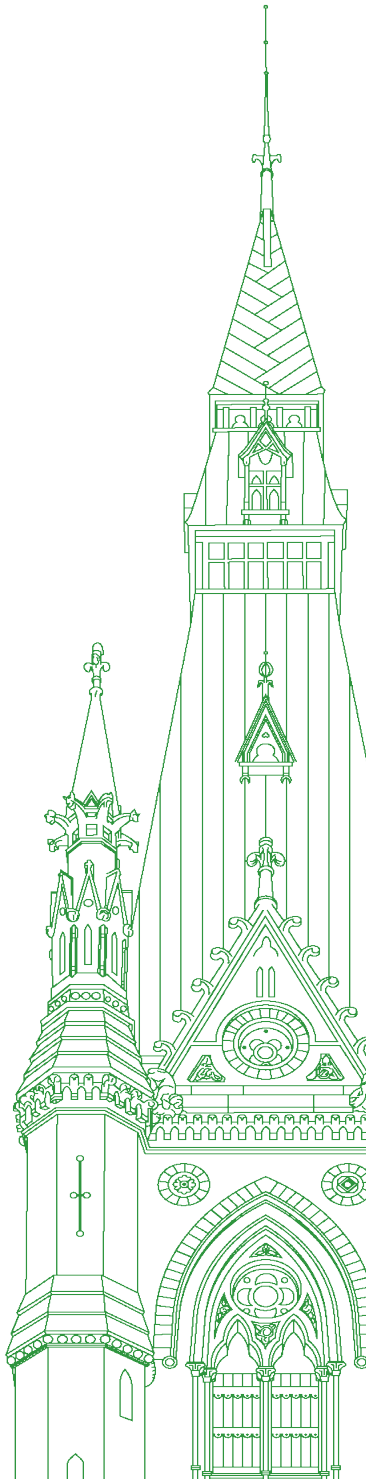
43rd PARLIAMENT, 2nd SESSION

Special Committee on Canada-China Relations

EVIDENCE

NUMBER 020

Monday, March 22, 2021



Chair: The Honourable Geoff Regan

Special Committee on Canada-China Relations

Monday, March 22, 2021

● (1835)

[*English*]

The Chair (Hon. Geoff Regan (Halifax West, Lib.)): I call this meeting to order. Welcome to meeting number 20 of the Special Committee on Canada-China Relations. Pursuant to the order of reference of Wednesday, September 23, 2020, the committee is meeting on its study of Canada-China relations.

[*Translation*]

This meeting is in hybrid format, pursuant to the motion adopted by the House on January 25, 2021.

[*English*]

I would now like to welcome the witnesses for our first panel.

From the Public Health Agency of Canada, we have Mr. Iain Stewart, president, as well as Dr. Guillaume Poliquin, acting scientific director general, National Microbiology Laboratory.

Thank you so much for being here tonight. I will now turn the floor over to Mr. Stewart for the opening remarks.

Please proceed. You have five minutes.

Mr. Iain Stewart (President, Public Health Agency of Canada): Thank you, Mr. Chair.

Thanks for the invitation to the discuss the Public Health Agency of Canada's relationship with China. A key focus of PHAC's current relationship is of course in the context of the response to COVID-19.

In the case of COVID-19, the Public Health Agency became aware on December 30 at 10:30 p.m. that something was happening in Wuhan, via GPHIN, the global public health intelligence network that we run. For us, it was a big thing. This detection of an outbreak of pneumonia in Wuhan was distributed in our daily report the next morning, December 31, and supplementary monitoring started right away.

The Chair: Pardon me, Mr. Stewart. I'm very sorry to interrupt you, but are you able to turn your camera on or is there a problem? We can't see you. I don't know if you know that.

Mr. Iain Stewart: No, I didn't know that.

The Chair: Please proceed.

Mr. Iain Stewart: Okay. Thanks, and thanks for the tip. I'm sorry about that, members.

Mr. Chair, as I was saying, we detected something in Wuhan on December 30 in the late evening. The next day, we sent out through the daily notification that in fact an infection event was occurring in Wuhan. The next day, Dr. Tam notified the Council of Chief Medical Officers of Health and we alerted the federal/provincial Public Health Network Communications Group and the Canadian Public Health Laboratory Network. For us, it started abruptly at the end of December and the very beginning of January.

With the world in the midst of the unprecedented global event that this resulted in, learning more about the zoonotic source of the virus has become crucial to better understand the situation and to help prevent future pandemics. That's why in May 2020 Canada co-sponsored the World Health Assembly resolution 73.1, which called for an "impartial, independent and comprehensive" review of the WHO-coordinated international health response to COVID-19 and scientific and collaborative field research missions, which laid the groundwork for the joint WHO-China mission on the origins of the SARS-CoV-2 virus.

In January 2021, a team of WHO-convened international experts travelled to China to work with Chinese counterparts to advance these efforts. Their reports are expected in the coming weeks. Canada has committed to supporting the WHO and its scientific work, and Canadian officials have reiterated the need for China to be open and transparent as part of this process.

Canada and China share a long-standing relationship in health, dating back to an MOU signed in 1995 calling for regular dialogue on health-related issues. The Canada-China policy dialogue on health has been the main vehicle for our formal bilateral engagement, including, at the ministerial level, four dialogues between 2009 and 2014. Since 2014, engagement with China has primarily been in health-related multilateral fora, such as the WHO and the Asia-Pacific Economic Cooperation health working group.

China has a growing capacity for basic and applied research, and there's a mutual benefit from academic exchanges. Reflecting on this, in January 2007, Canada and China signed a science and technology co-operation agreement. The agreement launched a sustained effort to boost collaborative research and development in fields like life sciences to promote collaboration in research and development between Chinese and Canadian academics and both private and public sector researchers and innovators. The initial areas of focus in life sciences included vaccines.

As with all collaborations, care is required to make sure that both parties have a clear understanding of the uses of the information being exchanged and, of course, the intellectual property that underlies the research teams. In our work, we've taken important steps to protect against security threats and intellectual property concerns. The Minister of Health, the Minister of Innovation, Science and Economic Development, and the Minister of Public Safety jointly issued a policy statement on research security and COVID-19 in September 2020, encouraging members of the research community to take precautions to protect the security of COVID-19-related research, intellectual property and knowledge development.

Challenges persist in any relationship, but there are benefits in exchanging information and research, and there are meaningful opportunities to do so through the relationships that I've just described. The global pandemic underscores the importance of international engagement and coordination, and international coordination will remain important to managing the pandemic going forward.

Thank you very much, Mr. Chair, for the opportunity to make remarks.

The Chair: Thank you very much, Mr. Stewart.

We'll now go to the first round of questions. We'll start with Mr. Chong.

You have six minutes, Mr. Chong.

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

Thank you, Mr. Stewart, for appearing in front of us.

In July 2019, one of the researchers at the lab in Winnipeg and her husband had their security clearances revoked and were escorted out of the lab. Can you tell us why?

Mr. Iain Stewart: That matter was the subject of an investigation. It was a security investigation. I'm not going to be able to talk about the details of that investigation.

Hon. Michael Chong: Did you co-operate with the RCMP investigation?

Mr. Iain Stewart: Do I co-operate with the RCMP investigation...?

Hon. Michael Chong: No, did you and the employees of the lab co-operate with the RCMP investigation?

Mr. Iain Stewart: There is an RCMP investigation under way at this time. If the RCMP need anything from us, they will have our co-operation, for sure.

Hon. Michael Chong: A CBC report indicated that staff members at the lab, who spoke on background to CBC, have indicated that senior management had not made them accessible to police or allowed staff to contact the RCMP with relevant information. Are you aware of that CBC report?

● (1840)

Mr. Iain Stewart: I'm not aware of that CBC report. However, I would say that if the RCMP wants anything from us, we will of course support them in that investigation.

Hon. Michael Chong: Are you indicating to employees that they're free to contact the RCMP with any relevant information they might have?

Mr. Iain Stewart: I'm surprised that this is an issue. The RCMP has been doing an extensive investigation, and we will of course support them in any way required.

Hon. Michael Chong: Okay. I'll take that as a yes—that employees of the lab are free to contact the RCMP with any relevant information they might have, because the RCMP has indicated they're interested in any information that people might have. I note that these scientists were just terminated from their employment at the lab six weeks ago or five weeks ago.

Can you tell us what happened, exactly, with the shipment that took place from the lab in March 2019 to China? This is not a personnel matter. This concerns a shipment of live Ebola and henipavirus to Beijing, on an Air Canada flight on March 31, 2019, which raised concerns.

Mr. Iain Stewart: In what sense?

Hon. Michael Chong: In what sense? There was a CBC News report, dated August 2019, that said the shipment of these live viruses to China “raises questions” and that the shipment may not have been done according to “the lab's operating procedures”.

Mr. Iain Stewart: I see.

Hon. Michael Chong: Is that news story correct?

Mr. Iain Stewart: All that we do, we do in conformity with the Human Pathogens and Toxins Act, the Transportation of Dangerous Goods Act and the Canadian biosafety standards. I don't think I'm able to comment on that specific allegation. I just know that from a policy level at this time, those are the policies we're guided by, sir.

Hon. Michael Chong: The shipment that took place on March 31, then, was done in accordance with the requirements under the Human Pathogens and Toxins Act and in accordance with the Transportation of Dangerous Goods Act, the Canadian biosafety standard, and the lab's own standard operating procedures. Is that correct?

In other words, what you're telling this committee is that there was nothing concerning about the shipment of those viruses, those live viruses, to China in March 2019, and everything was done properly, according to law, according to regulation, and according to standard operating procedure. Is that correct?

Mr. Iain Stewart: What I said was that those are what we're guided by.

If you'll allow me, I'll turn to my colleague. He runs the lab and was around at the time you're referring to.

Mr. Michael Chong: Sure.

Mr. Iain Stewart: I started this job after the date being discussed.

Dr. Poliquin.

Hon. Michael Chong: Please go ahead. Time is limited here.

Dr. Guillaume Poliquin (Acting Vice-President, National Microbiology Laboratory, Public Health Agency of Canada): The specific shipment that was being referenced, Mr. Chair, was done in accordance with the lab's standard operating procedures in compliance with the HPTA and the Transportation of Dangerous Goods Act, as well as with the Canadian fire safety standards.

Hon. Michael Chong: Thank you.

Can you understand why Canadians are concerned about the termination of the employment of these two scientists at the lab and why it's concerning that no further information is being released, even to a parliamentary committee? It creates a lot of suspicion and questions, the termination of these two scientists. I'm asking if you would be forthcoming and let us know why they were terminated.

You're protected here in front of a parliamentary committee. You have privilege as a witness. In other words, your testimony here cannot be used against you outside of this committee. The Canadian public would like to know why these two scientists were terminated.

The Chair: Mr. Chong, regrettably the time, of course, as you said is limited and the time is not protected. In that sense, I'm afraid yours has concluded. It may be that someone else can raise the same question again, and then we'll have a chance for one of the witnesses, or perhaps both, to answer that question.

Now I have to go on.

● (1845)

[*Translation*]

I'll now give the floor to Mr. Dubourg for six minutes.

Mr. Emmanuel Dubourg (Bourassa, Lib.): Thank you, Mr. Chair. I'm going to share my time with my colleague Mr. Fragiskatos.

First of all, allow me to acknowledge the witnesses, Mr. Stewart and Dr. Poliquin. We are pleased to hear them talk about Canada-China relations.

Mr. Stewart, you said in your opening remarks that you have had discussions with China on science, technology and intellectual property. Could you elaborate a little more on the nature of those discussions?

[*English*]

Mr. Iain Stewart: Thank you, Mr. Chair.

I was referring, sir, to a series of agreements that the Government of Canada and China have reached around collaboration in research, as you note. Those go back for many years. In the case of science and technology in particular, they go back to a 2007 arrangement focused on life sciences and, as I mentioned, areas such as vaccines.

[*Translation*]

Mr. Emmanuel Dubourg: How would you characterize the discussions you have had since last March with the Chinese authorities or your counterparts in China on vaccines and citizen assistance processes?

[*English*]

Mr. Iain Stewart: These are normally done as missions of scientists and government officials. Usually there are events. We go over, and there are specific topics of concern, areas of research in which presentations are made, so it's of that nature.

[*Translation*]

Mr. Emmanuel Dubourg: Okay.

During the pandemic, have you put in place additional security measures for the research done by Health Canada?

[*English*]

Mr. Iain Stewart: Do you mean at the Public Health Agency?

[*Translation*]

Mr. Emmanuel Dubourg: Yes, I'm sorry; I'm talking about the Public Health Agency of Canada's measures to counter cyber-attacks and prevent our research from being compromised.

[*English*]

Mr. Iain Stewart: This has been an area of concern for the government. I believe CSIS and perhaps CSE, which would be known to this committee, put out guidance and in fact warnings about persistent threat actors and activity around research related to the COVID situation. It's not for me to speak about their activities with respect to cybersecurity and so on, but yes, you're absolutely right, sir, that it has been an area of concern.

[*Translation*]

Mr. Emmanuel Dubourg: Okay, thank you.

You said that this is the mandate of CSIS, and I understand that, but have these organizations contacted you at any point to tell you to watch out for this or that type of process in your agency?

[*English*]

Mr. Iain Stewart: The people who are responsible for digital security and cybersecurity have been doing a fair amount of outreach, as you're suggesting, to government labs like ourselves, as well as to the private sector and others. Again, I'm not necessarily in the best position to speak about what they're doing, but with respect to ourselves, we take cybersecurity very seriously, particularly around our labs and the research that we're doing related to COVID. It has been an area where, in fact, we have been paying particular attention, sir.

[*Translation*]

Mr. Emmanuel Dubourg: Thank you.

I have one last question for you, Mr. Stewart.

We had a chance to meet with Dr. Scott Halperin, the director of the Canadian Center for Vaccinology at Dalhousie University. We know that he has been to China a few times and has met with representatives of the security agencies.

Were you in contact with Dr. Halperin or with Dalhousie University regarding vaccination, for example?

● (1850)

[*English*]

Mr. Iain Stewart: Yes. Actually, in my career I had an opportunity to work at Dalhousie University, and I know Dr. Halperin from that period some time ago. More recently, in my time at the National Research Council, we had discussions related to his work at the Canadian vaccination centre—he is, in fact, a pivotal part of the Canadian research community in that way—so, yes, I do know and I have spoken with Dr. Halperin.

[*Translation*]

Mr. Emmanuel Dubourg: Following his return from China, did you have similar discussions to talk about his discoveries or research?

[*English*]

Mr. Iain Stewart: I've actually never spoken to Dr. Halperin about his trips to China, nor about his actual personal research in the context that I'm discussing now. I've been talking to him in the context of his leadership through the Canadian vaccination centre at Dalhousie. That was around projects that he does for that institution.

Mr. Emmanuel Dubourg: Thank you so much, Mr. Stewart.

[*Translation*]

The Chair: Thank you very much.

Mr. Bergeron, you have six minutes.

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

I'd like to thank the witnesses.

Mr. Poliquin, I must admit that I was somewhat surprised by the brevity—to say the least—of your remarks earlier.

Anyway, I would like to follow up on what Mr. Chong was talking about. He talked about this pair of Chinese researchers who went to China a few times, including once in July 2019. In fact, they were kicked out of the lab after going to China with live samples of Ebola and Nipah. Yet it appears from the evidence that everything was done by the book.

Why were they kicked out of the lab, then? Why did they wait several months before firing them outright?

[*English*]

Mr. Iain Stewart: They are no longer with the agency. We undertook an investigation, and I'm not really at liberty to talk more about that, sir.

[*Translation*]

Mr. Stéphane Bergeron: What do you mean when you say you're not at liberty to talk about it? You are before a parliamentary committee, so you normally have to answer questions from parliamentarians. The question is simple: if everything was done properly, why were they kicked out and fired a few months later?

The question is simple; the answer should be, too.

[*English*]

Mr. Iain Stewart: An investigation was undertaken, and they no longer work with the agency.

[*Translation*]

Mr. Stéphane Bergeron: In this case, since it was deemed appropriate, after an investigation, to kick them out and then dismiss them, there is reason to believe that everything wasn't done properly.

What were they accused of?

[*English*]

Mr. Iain Stewart: There was an investigation, and they're no longer with the agency.

[*Translation*]

Mr. Stéphane Bergeron: We understand that. What we want to know is what they were accused of. Why are they no longer employed by the agency?

[*English*]

Mr. Iain Stewart: I am not at liberty to discuss the details of that investigation, sir.

[*Translation*]

Mr. Stéphane Bergeron: I'm sorry, Mr. Stewart, but you're putting yourself in a position where you could be charged with contempt of Parliament. You're not answering the questions you're being asked. It's a simple question.

You told us a few moments ago that everything had been done properly, but that following an investigation, you had dismissed them and fired them. If everything was done according to the rules, what happened to get them to be dismissed?

Your answer raises many questions, not only for us parliamentarians, but also for the general public. Indeed, we have every reason to believe that a mistake was made and that information was passed on to the Chinese authorities.

● (1855)

[*English*]

Mr. Iain Stewart: I'm sorry, sir. What's the question you'd like me to answer?

[*Translation*]

Mr. Stéphane Bergeron: The question is simple: why were they dismissed?

[*English*]

Mr. Iain Stewart: They were investigated, and the investigation was completed. They are no longer a part of the agency.

[*Translation*]

Mr. Stéphane Bergeron: We understand that. What we don't understand is why they were dismissed, if everything was done by the book. What mistake did they make?

[*English*]

Mr. Iain Stewart: Sir, you've asked me the question. I can repeat the answer. An investigation was undertaken. They're no longer part of the agency.

[*Translation*]

Mr. Stéphane Bergeron: We understand that. It's very clear.

[*English*]

Mr. Iain Stewart: I'm not at liberty to discuss this further.

[*Translation*]

Mr. Stéphane Bergeron: What we don't understand is why they were dismissed. We understand that there was an investigation and that they're no longer with the agency. But what we don't understand is why they were dismissed if everything was done properly. It suggests that not everything was done properly and that a mistake was made and we don't know what it was. There is every reason to believe that this mistake was serious enough, in terms of transmitting information to the Chinese authorities, that you felt it was appropriate to eject them and subsequently dismiss them.

What mistake did they make?

[*English*]

Mr. Iain Stewart: I'm not at liberty to discuss the details of that investigation, sir.

[*Translation*]

Mr. Stéphane Bergeron: A point of order, Mr. Chair.

Doesn't the witness have an obligation to answer questions that parliamentarians ask him?

The Chair: Thank you, Mr. Bergeron.

My impression is that witnesses have the right to respond as they wish. If the committee wants to make a decision on that, it can discuss it.

Mr. Stéphane Bergeron: So I would like to tell the witness that we will certainly be looking at the refusal to answer that we've seen in the last few minutes. In terms of transparency and accountability, it is extremely distressing for Canadians and Quebecers.

It's also very concerning, because there was obviously a security breach. We know that live viruses were carried on an Air Canada flight. Is that a common practice?

We also know that there have already been breaches and leaks, as far as vaccines are concerned, at the Wuhan lab—

The Chair: Mr. Bergeron, your six minutes are up.

I have to give the floor to Mr. Harris now.

[*English*]

Mr. Harris, you have six minutes.

Mr. Jack Harris (St. John's East, NDP): Thank you, Chair.

Mr. Stewart, the individuals we're talking about here.... I know you haven't answered Mr. Bergeron's question, but I'll ask one more. Were these individuals charged with any offence?

Mr. Iain Stewart: They would not be charged with an offence by us, sir. That is something that would come, of course, from police officers or an investigative body of some kind—

Mr. Jack Harris: Would you know that?

Mr. Iain Stewart: At this time, I'm not aware of them being charged with any offence. What I can say is that an investigation was done, and they're no longer with the Public Health Agency.

Mr. Jack Harris: So you've never done any follow-up to find out what happened to them: whether they were charged, whether they weren't, what the results of the investigation were.

Mr. Iain Stewart: To my knowledge, they have not been charged, but that's a matter you would want to pose to the RCMP. That's not an area we're involved in.

Mr. Jack Harris: You said there was an investigation, but you have no idea of the results of the investigation and you weren't involved in that.

Mr. Iain Stewart: The RCMP investigation is not a matter that we're directly involved in. We're happy to support them in any way.

Mr. Jack Harris: Wouldn't they report back to you? These people were just investigated, and that was it. They're no longer there.

How did they leave?

● (1900)

Mr. Iain Stewart: They've left the agency.

Mr. Jack Harris: Did they leave on their own?

Mr. Iain Stewart: The two scientists are no longer employed by the Public Health Agency of Canada.

Mr. Jack Harris: We understand that, but people leave in various ways. Some people retire; some resign; some get another job. They were under investigation, and they left. You're saying you have no idea why they left, or how they left, or what the results of the investigations were.

Mr. Iain Stewart: No, actually, I did not say that we had no idea why they left. I said they no longer work at the Public Health Agency. We can't disclose additional information on this matter.

Mr. Jack Harris: Let's see what you can disclose about something else.

You talked about GPHIN, a very well-regarded agency that has operated inside of the Public Health Agency for a very long time. It was recognized worldwide as having a global alert system that was well respected and needed, and in fact looked to around the world for alerts on things like the COVID-19 situation happening.

You said that you got information from them on December 31 that there was something going on in Wuhan. Is that correct?

Mr. Iain Stewart: At 10:30 p.m. on December 30, GPHIN gave us an indication that there was something of interest in Wuhan.

Mr. Jack Harris: You followed up on that, I presume. You were glad that they were able to give you that information and, presumably, you got further reports from them. Is that correct?

Mr. Iain Stewart: Yes, sir.

Mr. Jack Harris: We have a very thorough investigative report published by The Globe and Mail in July of last year, outlining a whole series of problems after that among the people who were involved in that alert system, providing information that was not getting to the right place.

Can you tell us about that?

Mr. Iain Stewart: I can, sir. Thank you for the question.

First of all, GPHIN is a platform. It's a technology for gathering open-source information. Second, it's a group of experts who interpret and provide...broadcast notifications out. They do a daily report, and they do an alert report. The daily report was what came out the next day, indicating there had been an indication of interest in Wuhan.

Mr. Jack Harris: These daily reports that were being filed internally.... It's reported that they began to face push-back from within the department. They were told to focus their efforts on official statements, such as data from the Chinese government and WHO. They were told that other sources of information were just rumours. They just wanted the reports restricted to only official information.

Can you confirm that?

Mr. Iain Stewart: I haven't seen any guidance that they should focus their attention on information sourced from the Government of China and the WHO.

Mr. Jack Harris: There was no official written guidance. When someone says they were told that, you're saying there was no official guidance.

They were also criticized at one point, a few weeks after the outbreak. The public health director was asked why GPHIN's internal reports had missed crucial developments being widely reported in the news around the world, that human-to-human transmission had been detected. The response was, from the analysts, that the information had, in fact, been discussed in earlier reports, before the documents went up the chain, but somehow the information was taken out of that.

Can you tell us about that?

Mr. Iain Stewart: In my introductory remarks, I mentioned that a special report was issued at 9:00 a.m. on January 1. The special report included that there was this event of interest occurring in Wuhan, and Dr. Tam used that the following day to talk to the Council of Chief Medical Officers of Health.

Mr. Jack Harris: I understand that there were some issues, but at the same time, the information they were aware of regarding human-to-human transmission never made it up the chain. In fact, this was something that was not known by these senior people.

The Chair: Mr. Harris, thank you very much. Sorry for interrupting, but your six minutes have concluded.

We'll now go to the second round. We'll begin with Mr. Genuis for five minutes.

Go ahead, Mr. Genuis, please.

Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC): Mr. Stewart, has there ever been a case where any government lab has fired scientists as a result of security breaches or the improper transfer of viruses?

● (1905)

Mr. Iain Stewart: That's a very difficult question to answer.

Mr. Garnett Genuis: Well, I'm glad you have a bloody senior office in this country where you're supposed to account to parliamentarians and the Canadian people. Now answer the damn question.

Mr. Peter Fragiskatos (London North Centre, Lib.): Point of order, Mr. Chair.

The Chair: I just want to ask members to conduct themselves, of course, in a parliamentary fashion.

Mr. Garnett Genuis: I would like to ask the witness—

The Chair: I do appreciate that the member is entitled to ask the question. I just ask him to be parliamentary and try to remain calm. I understand.

Mr. Genuis.

Mr. Garnett Genuis: Mr. Stewart, this is a critical issue of national security. Has any lab in this country ever fired a scientist as a result of a security breach or the improper transfer of viruses? You're a public servant. People deserve an answer.

Mr. Iain Stewart: I am not able to answer the question as it was structured.

Mr. Garnett Genuis: Were there cases of people being fired for policy breaches?

Mr. Iain Stewart: In fact, you're asking a question that gets back at the two individuals of concern, and I have indicated—

Mr. Garnett Genuis: No, I'm not, sir. I'm asking a general question. Have there been cases of individuals fired as a result of policy breaches at any lab in Canada?

Mr. Iain Stewart: I'm only aware of the labs for which I have been responsible, and I can't answer the question as it's currently structured.

Thank you, sir.

Mr. Garnett Genuis: If someone had been fired for a policy breach, what would be meant by the term “policy breach”?

Mr. Iain Stewart: A policy breach, I don't know. It would be an administrative policy perhaps. It would be a safety policy perhaps. It would be a security policy perhaps. There could be different constructions.

Mr. Garnett Genuis: This is such an utter disgrace, but I think I have to move on.

Does Canada fund or permit—

Mr. Peter Fragiskatos: Point of order, Mr. Chair.

Mr. Garnett Genuis: —so-called gain-of-function experiments?

The Chair: On a point of order, go ahead, Mr. Fragiskatos.

Let's stop the time.

Mr. Peter Fragiskatos: I raised a point of order earlier, but you spoke about how we conduct ourselves as parliamentarians.

The member, our colleague, is free to ask questions as he wishes, but it's a bit unbecoming when the witness here continues to be badgered like this. Let the questions be asked, of course, but there's a way.... There's a decorum between colleagues that needs to be maintained. I would just advise my colleague of that. We need to be professional here.

Mr. Garnett Genuis: Mr. Chair, on the same point of order—

The Chair: Mr. Genuis, go ahead on the same point of order.

Mr. Garnett Genuis: I would submit that this is not a point of order. I would submit that pointing out something as a disgrace is perfectly legitimate and that if Mr. Fragiskatos wishes to interrupt the line of questioning in order to offer some cover to a senior public official refusing to answer important public security questions, that's on him. I'm happy for the public to observe his approach to this hearing and mine, and judge accordingly.

Mr. Peter Fragiskatos: Point of order, Mr. Chair, very quickly.

Mr. Garnett Genuis: It's not a matter of order, Mr. Fragiskatos.

Can I proceed with my questions, Mr. Chair?

Mr. John Williamson (New Brunswick Southwest, CPC): I think we lost the chair.

The Vice-Chair (Mr. Garnett Genuis): Okay, in that case, I'll assume the chair as vice-chair and continue with my round of questions.

Mr. Peter Fragiskatos: In that case, I have to raise a point of order.

The Vice-Chair (Mr. Garnett Genuis): You're out of order, Mr. Fragiskatos.

Does Canada fund or permit so-called gain-of-function experiments—

Mr. Peter Fragiskatos: You can't do that. I have a point of order.

The Vice-Chair (Mr. Garnett Genuis): —whereby researchers intentionally make viruses more deadly—

Mr. Peter Fragiskatos: Point of order.

The Vice-Chair (Mr. Garnett Genuis): —or more contagious for research purposes?

Mr. Emmanuel Dubourg: Point of order, Mr. Genuis.

The Vice-Chair (Mr. Garnett Genuis): Yes, Mr. Dubourg, I'll take your point of order.

Mr. Emmanuel Dubourg: Mr. Genuis, listen, [*Technical difficulty—Editor*] problem. Can we please take a break and make sure the clerk and the technician get back the chair?

The Vice-Chair (Mr. Garnett Genuis): Thank you, Mr. Dubourg.

No, we're not going to suspend the meeting. We have limited time. I'm going to continue with my line of questions for the remaining three minutes that I have, and then I will hand it over to the next person. That's—

Ms. Lenore Zann (Cumberland—Colchester, Lib.): Could you please try not to swear this time, though, Mr. Genuis?

Thank you.

The Vice-Chair (Mr. Garnett Genuis): Order, Ms. Zann, please.

Ms. Lenore Zann: Please try to not swear.

Thank you.

The Vice-Chair (Mr. Garnett Genuis): Does Canada fund or permit so-called gain-of-function experiments, whereby researchers intentionally make viruses more deadly or contagious for research purposes?

Mr. Iain Stewart: Thank you, Mr. Vice-Chair.

To my knowledge, the Public Health Agency of Canada does not fund research of the nature you're describing.

I'll ask Dr. Poliquin, who runs our lab, to confirm that.

Dr. Guillaume Poliquin: Thank you, Mr. Stewart.

When experiments are proposed that have the potential for gain-of-function applications, they are automatically referred to the institutional biosafety committee to ensure that no such experiments move forward and that any risks associated with them are mitigated.

● (1910)

The Vice-Chair (Mr. Garnett Genuis): Does the Government of Canada allow the transfer of viruses—

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

Madam Clerk, tell me the procedure here. Because Mr. Genuis has assumed the chair, is he still able to ask questions? Again, he can ask any question he wishes; I'm not trying to get in the way of him asking questions. I just wonder if it makes sense to briefly pause the meeting for the chair—who I understand is having tech issues—to come back online.

It's just a bit odd that the vice-chair would also be asking questions. I've never seen that happen before. I think there could be a breach in the protocol of the meeting.

The Vice-Chair (Mr. Garnett Genuis): Thank you, Mr. Fragiskatos.

Mr. Jack Harris: To that point of order, Chair, when someone takes the chair in the place of the original chair, then that person has to act as chair. If he wants to speak, he has to step down from the chair and pass the chair over to somebody else.

I don't think you can be the chair and deal with points of order, particularly ones that are dealing with your right or ability to ask questions at any given time. You would have to cede the chair to somebody else and step aside from the chair while you're asking questions.

Seeing as you're trying to perform both functions at once, I think it's out of order.

The Vice-Chair (Mr. Garnett Genuis): Thank you, Mr. Harris.

I want to make this as uncontroversial as possible. I'll happily cede the chair to Mr. Bergeron, who I think knows that I have three minutes left. I'll defer to him to allow me to proceed as he wishes.

[*Translation*]

The Vice-Chair (Mr. Stéphane Bergeron): Mr. Genuis, you may continue.

Mr. Garnett Genuis: Thank you, Mr. Chair.

[*English*]

Does Canada have a policy of prohibiting the transfer of viruses to other institutions for the purposes of gain-of-function experiments?

Mr. Iain Stewart: Dr. Poliquin, would you like to respond to that, please?

Dr. Guillaume Poliquin: The transfer of materials is governed by the Human Pathogens and Toxins Act, the Transportation of Dangerous Goods Act, and the Canadian biosafety standards. They apply to the export of materials from Canada.

Mr. Garnett Genuis: I understand that, but it's fairly—

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

[*Translation*]

The Vice-Chair (Mr. Stéphane Bergeron): Mr. Fragiskatos, you have the floor.

[*English*]

Mr. Peter Fragiskatos: I do remember that when Mr. Regan turned it over to Mr. Genuis he said five minutes. I believe he's gone well over five minutes at this point.

Mr. Garnett Genuis: Yes, that's because it's been you talking the whole time.

Mr. Peter Fragiskatos: That is not the case at all.

[*Translation*]

The Vice-Chair (Mr. Stéphane Bergeron): Madam Clerk, could you shed some light on this issue?

The Clerk of the Committee (Ms. Marie-France Lafleur): If the clock was indeed stopped earlier, Mr. Genuis has about two minutes left.

The Vice-Chair (Mr. Stéphane Bergeron): Mr. Genuis, you may continue.

[*English*]

Mr. Garnett Genuis: Thank you very much, Mr. Chair and Madam Clerk.

My question was specific to the transfer to institutions and gain-of-function experiments. Does the Wuhan Institute of Virology engage in gain-of-function experiments related to coronaviruses?

Dr. Guillaume Poliquin: Mr. Chair, I apologize. I'm not able to answer that particular question.

Mr. Garnett Genuis: If viruses were to be transferred to the Wuhan Institute of Virology, would you, as the head of the lab, be responsible for approving those transfers?

Dr. Guillaume Poliquin: [*Technical difficulty—Editor*] must be approved by senior management at the National Microbiology Laboratory.

Mr. Garnett Genuis: You are responsible for approving them—

The Chair: Mr. Genuis and colleagues, I'm happy to say that I'm back. I'm sorry for my absence, but my computer shut down on me.

I would just like to ask the clerk how long Mr. Genuis has had. If he's had five minutes, he has a minute left.

The Clerk: I can confirm that he has about a minute left.

The Chair: Thank you very much.

Mr. Genuis, please carry on.

Mr. Garnett Genuis: Thank you.

Mr. Poliquin, you're responsible for approving transfers, but you are unaware whether the Wuhan Institute for Virology engages in gain-of-function experiments related to coronaviruses.

How would you make determinations about the appropriateness of transfers to that institution, if you are unaware of such an important aspect of how transferred materials might be used?

● (1915)

Dr. Guillaume Poliquin: Mr. Chair, every transfer of material is assessed on a case-by-case basis. We have never transferred coronaviruses to the Wuhan Institute of Virology; therefore, we have not assessed the question as structured.

Mr. Garnett Genuis: Have you assessed whether they conduct gain-of-function experiments related to the viruses that were transferred?

Dr. Guillaume Poliquin: Mr. Chair, prior to the transfer, one of the essential aspects of the transfer process is receiving a letter from the receiving institute with respect to their intent.

Mr. Garnett Genuis: Are you satisfied with the security protocols at the Wuhan Institute of Virology?

The Chair: Mr. Genuis, we'll have to wait for that answer. Your time has concluded.

We're now on to Mr. Fragiskatos for five minutes.

Mr. Fragiskatos, go ahead, please.

Mr. Peter Fragiskatos: Thank you, Mr. Chair. You may be aware of this already, but you missed some theatrics while you were gone.

Just to let colleagues know—in particular Mr. Genuis—when I raised points of order, they were not to prevent certain questions from being asked. Members have that privilege; they are members of Parliament. My points of order related, as I said, to parliamentary decorum, allowing a witness to finish an answer and not badgering that witness.

It's good to ask hard questions. There's nothing wrong with it. There is, however.... It's not even a fine line. There is a difference between asking a question in a meaningful way and making a mockery of a parliamentary committee, which I'm afraid my friend Mr. Genuis has done yet again.

But I'll leave that aside, Mr. Chair. My question is for Mr. Stewart.

Mr. Stewart, MPs here have asked difficult questions about an ongoing investigation, and they have accused you of being evasive. Is it fair to say that you can't answer the question because there is an ongoing investigation?

Mr. Iain Stewart: There are three aspects. There's privacy with respect to individuals. There is security with respect to the nature of the investigation. Third, I can't speak on behalf of the RCMP in their investigations.

Those are the reasons why I've been unable to answer the questions as posed, sir. I'm sorry it's causing stress and unhappiness. It's just the legal advice I was provided in preparation for this session.

Mr. Peter Fragiskatos: Thank you very much.

I want to ask you a question about the Global Public Health Intelligence Network, a widely respected tool. In fact, as we know, it is used in a very significant way by the World Health Organization when it comes to the monitoring of pandemic data and threats to international public health more generally, beyond pandemics. You know this much better than I do; I'm just saying it for context.

There was an audit carried out recently, and this matter has come up here tonight, but I want to ask you specifically about it and get your response. I'm quoting here from a Canadian Press report that itself quotes the audit, so I'll put it on record.

It says:

> The interim report concluded that the news monitoring system did identify the outbreak of the pneumonia that would [become] COVID-19 on the night of Dec. 30, 2019—

This is the point you referred to earlier, Mr. Stewart. It continues:

> —and included this information from Wuhan, China, in a special report to Canadian public health officials the next day.
>
> But the report noted that without [sending up] a formal alert, international partners relying on Canada's information were left to rely on other sources.

I'll also quote here, as the piece does, directly from the audit:

> "That [the system] identified early open-source signals of what would become COVID-19 and promptly alerted senior management does not mean that the system is operating as smoothly or as clearly as it could and should," the report concluded.

I just want to put that question to you to get your response as the president of the Public Health Agency of Canada. I think it's a relevant question, because this is something that Canadians are asking right now, and I think it deserves an answer.

Mr. Iain Stewart: Through the chair, thank you.

I would like to agree with you. It is a valued asset. GPHIN is important, and it needs to play an important role. The Public Health Agency made changes that I think diminished the value of the asset and its ability to help the health community prepare.

In my opening remarks, what I was trying to underline and note was that it actually did do its job and it did result in internal action. However, your question is underlining that it did not do the external, international role it used to play, through not transmitting an alert. We see value in those alerts, and we have corrected and restored that function.

Going forward, in terms of the report you're referring to, which is an arm's-length review that Minister Hajdu requested, there will be consideration of how we can do a better job in identifying developments of concern and responding more quickly, and to be frank, I look forward to that advice.

● (1920)

Mr. Peter Fragiskatos: Thank you very much.

Mr. Stewart, I have a few seconds, but if at some point you can't conclude the answer here because of limited time.... In terms of actions taken by PHAC to combat misinformation relating to the pandemic, the conspiracy theories that continue to circulate, I would love to hear more about what PHAC is doing on that front.

The Chair: Okay, I'm afraid we'll have to [*Technical difficulty—Editor*].

[*Translation*]

Mr. Bergeron, you have the floor for two and a half minutes.

Mr. Stéphane Bergeron: Mr. Chair, a few moments ago, Mr. Stewart revealed something to us that demonstrates an unfortunately all-too-common practice in the government apparatus: senior officials are advised to tell parliamentarians as little as possible.

I do not have the reference in front of me, Mr. Chair, but as a former Speaker of the House, you will most certainly be able to enlighten me on the matter. I know that an important ruling by Speaker Milliken mentioned that the state apparatus has an obligation to deliver information requested by parliamentarians.

I can understand that security or confidentiality considerations would cause the witness to be somewhat circumspect. However, I invite the Public Health Agency of Canada to provide parliamentarians with the answers to the questions that have been asked, on a confidential basis. Witnesses, especially when they are senior public servants, have a constitutional obligation to answer questions from parliamentarians in the interests of transparency and accountability.

I understand that not everything can be said publicly, but I am offering Mr. Stewart the opportunity to send us a written response, in confidence, to the questions that have been asked. Otherwise, I am telling you, Mr. Chair, we will have to take action. We cannot tolerate such an attitude from senior officials to the parliamentarians who represent the people and who are entitled to answers from those officials.

As Mr. Fragiskatos did, I am using my time to make this point. I understand that some information cannot be released publicly, but it's imperative that it be provided to parliamentarians, however it is done.

Once again, I offer Mr. Stewart the opportunity to provide a response to committee members on a confidential basis.

Thank you, Mr. Chair.

The Chair: Thank you very much, Mr. Bergeron. Your time is up.

With respect to the question you raised in your point of order, I can indicate that, when a witness says they cannot provide an answer for legal reasons, it is an answer that the committee will normally accept. Nevertheless, the committee may decide to report the situation to the House, as I mentioned.

[*English*]

Now we'll go to Mr. Harris, for two and a half minutes, please.

Mr. Jack Harris: Thank you, Chair. I think you are referring to me, but I can't hear you. That's not unusual, it seems.

I would like to ask Mr. Stewart a couple more questions about the operation of the Global Public Health Intelligence Network.

During the January and February period, they gathered continuous information that didn't seem to make it to the high levels in your department. Even up until the end of February, the chief public health officer told the House of Commons health committee that the situation was under control. We had controlled the virus. There were just a dozen cases in Canada. But that really wasn't the case, was it, Mr. Stewart? It wasn't under control. In fact, two weeks later, there was a public health emergency declared. We were all under a lockdown.

Why was the information that was being garnered by this public health agency, GPHIN, being ignored? Why was that not taken into consideration in making international alerts, for one, but also for Canada taking stronger action more quickly?

● (1925)

Mr. Iain Stewart: Thank you for the question, sir.

GPHIN is a notification system. It tells you when an event is occurring. As I mentioned in my opening remarks and in response to the other questions, the notice was provided, and it was responded to. Dr. Tam herself actually answered to that request—

Mr. Jack Harris: Excuse me, if I could interrupt you for one second.

They were also giving other information based on what was observed in China and what was happening there. These notifications were based on information that was gathered, which they had done for years, for more than a decade. They hadn't issued any alerts for the previous 12 months, because they weren't allowed to. That information could have provided—and did provide, if you had listened to it—the ability to detect what was going on.

You didn't do that, and it wasn't passed on to the Canadian public or to the world.

Mr. Iain Stewart: Mr. Chair, as I mentioned earlier, there are actually different streams of information that come out of GPHIN. Some, which are internal to the organization, like the daily reports, continued—and continue to this day. Some, like alerts, as the members have been noting, stopped being sent internationally—to international partners, for instance.

The Chair: Thank you very much. Thank you, Mr. Harris.

We now go on to Mr. Williamson for five minutes, please.

Mr. John Williamson: Thank you, Mr. Chair.

I have a number of questions. I'm going to return to Mr. Stewart.

My question is, why were the two employees of the National Microbiology Laboratory terminated?

Mr. Chair, I would move that the question be put to Mr. Stewart so we may receive a proper answer.

Mr. Iain Stewart: Mr. Chair, in response to this question from one of the members, I was led to believe that it's possible for me to seek to provide confidential and secure advice to you under certain conditions. That was what one of the members just said previously. If that's a venue that's open to me.... You have to understand that I don't normally work in security areas. I'm not familiar with this committee or its practices. There might be ways of responding to the question that you have that I'm not aware of.

I would like to have the opportunity to explore what is the appropriate legal way to respond to this request. Clearly, I am not able to orally answer the question in this public telecast venue at this time.

Hon. Michael Chong: Mr. Chair.

The Chair: Mr. Chong, do you have a point of order?

Hon. Michael Chong: Yes, it's a point of order.

According to *House of Commons Procedure and Practice*, when a question is put to a witness, the witness is obligated to reply. Testimony in front of this committee is privileged. That testimony cannot be used against the witness outside of this committee in a court of law. It cannot be used in police investigations. It cannot be used against the witness by the Government of Canada, or by anyone else. It's privileged testimony. Mr. Williamson asked that the question be put. The witness has an obligation to answer the question.

Thank you, Mr. Chair.

The Chair: Thank you very much, Mr. Chong. If you're asking me to examine the argument you've raised, I would need time to do that and consider the authorities, as you can imagine.

Hon. Michael Chong: Mr. Chair, the question was asked to be put to the witness. The witness has an obligation to answer the question. You're the chair, so I ask you to rule on that, please.

The Chair: Mr. Chong, what you read from the procedure book for the House of Commons suggests that the witness must answer. It does not talk about how a witness should answer. The witness has provided answers.

As I indicated earlier, and as the clerk will affirm to you, committees generally accept legal matters as a reason for not answering. The witness has given the reason that he is getting legal advice and there are legal reasons—an investigation is going on and so forth—for not answering the questions.

As I indicated, the committee has the power, if it should so decide, to report the matter, or some other matter, to the House of Commons.

Mr. Williamson, go ahead.

● (1930)

Mr. John Williamson: Thank you, Chair.

Mr. Stewart, am I to take it that you are committing to provide that information to this committee on a confidential basis and that a response will be forthcoming to the chair?

Mr. Iain Stewart: Mr. Chair, I will commit to explore with legal counsel and the appropriate people who understand the orders of procedure that you are following what is the venue to respond to your question. That's what I commit to, sir, to see what I'm able to do.

Mr. John Williamson: All right. You gave us three rationales for not answering. There's a fourth one, and that is just bureaucratic butt-covering, incompetence, malfeasance in the department. The reasons you gave us are far from exhaustive. In fact, you're treating this committee as if we are members of the press who are looking for answers but don't have rights to these answers.

We look forward to your response. I'm not going to dwell on it, because our time here is limited, but I do hope that information is forthcoming. I think you'll see there's a consensus, at least among the opposition parties here, that answers are needed.

I will now turn to Dr. Poliquin. Your last answer to my colleague on assessing the letter from a Chinese entity.... You didn't provide an answer, because we ran out of time. Do you take these letters from China as the truth and nothing but the truth? What investigations do you do to ensure that the letter will be honoured?

Dr. Guillaume Poliquin: Mr. Chair, to complete the answer, when we received the letter from the director of the Wuhan Institute of Virology with respect to the intended use of the viruses, it stated they were to be used for understanding the pathophysiology—the nature of infection—as well as the development of antivirals.

Neither Canada nor the National Microbiology Laboratory has the standing to investigate or audit laboratories, but the request for an assessment is what is required under the HPTA and the TDGA.

Mr. John Williamson: That's an astonishing admission. You're taking a request from a nation that has a history of theft and lies, and accepting that because it's what the law in this country says, that this is sufficient, at a time when our national security institutes are warning academia in general to be very careful. That's a remarkable testimony.

Is that what you're telling us here, that this letter goes into a file, the box is ticked and data is transferred based on the word of a government that is known to lie, not only to its people but to the world community?

Dr. Guillaume Poliquin: Mr. Chair, should I answer?

The Chair: Dr. Poliquin, please go ahead. I'll give you a few seconds.

Dr. Guillaume Poliquin: Mr. Chair, there is an extensive approach that is undertaken prior to the transfer of materials, and the Wuhan Institute of Virology is an organization dedicated to public health.

The Chair: Thank you, Mr. Williamson.

Now we'll move to Ms. Yip for the last five minutes in this hour.

Ms. Jean Yip (Scarborough—Agincourt, Lib.): Dr. Poliquin, scientists and governments around the world have been working together to combat COVID-19, and Canada has been an active partner in the global fight.

Can you tell us more about Canada's collaboration with the international community and any work that PHAC and NML are doing with international partners?

● (1935)

Dr. Guillaume Poliquin: The global community has collaborated extensively in the response to COVID-19, including through the convening power of the World Health Organization. The sharing of sequence data from China on the weekend of January 10 was what made the NML able to develop our first generation test for COVID-19 in five days, following the publication of that sequence. I think this illustrates the essential nature of international collaboration as we continue to fight the pandemic.

The National Microbiology Laboratory continues to be engaged, both domestically and internationally, on a number of efforts, including through the global health security lab network, which has been an essential forum for the sharing of information, science and learning with respect to SARS-CoV-2. It continues to be a source of ongoing support.

Ms. Jean Yip: Does this international collaboration also extend to PHAC's policy on participation with the foreign talent recruitment program?

Dr. Guillaume Poliquin: My apologies, Mr. Chair, but I am....

Ms. Jean Yip: Let me just restate this, to make it clearer.

What is PHAC's policy on participation in foreign talent recruitment programs?

Mr. Iain Stewart: On participation in foreign talent programs, are you referring to a specific program, like, for instance, the thousand talents program, or do you mean just talent development programs generically? Please excuse me for the clarification.

Ms. Jean Yip: I meant the ones offered by China.

Mr. Iain Stewart: Do you mean things like the thousand talents program?

Ms. Jean Yip: That's right.

Mr. Iain Stewart: We tend to see programs of that nature as a conflict of interest. If you're an employee of the Government of Canada, we expect that you would not also be involved in another government's programs in that way.

Ms. Jean Yip: Are there any Chinese nationals visiting or working at the NML right now?

Dr. Guillaume Poliquin: With respect to how visiting officials are handled when working at the National Microbiology Laboratory, following the development of the working officials policy, which is in the final status of its current review, a working official agreement is required prior to working at the NML. That includes an agreement that covers things such as IP rights and access to facilities. It also requires a valid secret level security clearance, to be obtained prior to work commencing at the National Microbiology Laboratory.

Ms. Jean Yip: Is there currently a security policy, or is what you just stated in the works?

Dr. Guillaume Poliquin: There is an existing security policy. The National Microbiology Laboratory requires a secret clearance and a number of other supportive documents prior to commencing work at the NML, but we are an organization of continual improvement and the latest iteration of the working official policy is under [*Technical difficulty—Editor*].

Ms. Jean Yip: I only have a bit of time left. What is the major improvement in the new working policy?

Dr. Guillaume Poliquin: Mr. Chair, it's not necessarily a significant change. It is just an ongoing review of these policies and of the development of streamlined processes.

Ms. Jean Yip: Thank you.

The Chair: Thank you very much. Thank you, Ms. Yip.

This concludes the first panel, and I will now excuse and thank the witnesses. We'll take a very short pause, I think, as we go to the next panel.

● (1940)

Mr. Garnett Genuis: I have a point of order, Mr. Chair.

The Chair: Mr. Genuis.

Mr. Garnett Genuis: Mr. Chair, just before the witness is excused, I want you to clarify your intention with respect to following up with the witness on the follow-up information that was requested. Mr. Williamson had put forward a motion that the question be responded to. Mr. Stewart noted he would seek advice on how to respond.

This is a simple piece of information that I think the committee could receive on a fairly time-sensitive basis. I'm just trying to understand from a perspective of procedure what your intention is, Mr. Chair, on following up and distributing this information.

The Chair: It's certainly my intention to await.... I anticipate a response from Mr. Stewart—I presume a written response—in terms of how he proposes to deal with what's been raised this evening, which I would then, of course, share with the committee.

The committee, of course, could choose, for example, to pass a motion giving a time limit and indicating that it wants and is expecting a response. Then it would proceed from there in whatever manner it wishes.

If you wish, we could ask Mr. Stewart if he has a timeline in mind. What is the preference of the committee?

Mr. Garnett Genuis: Mr. Chair, I believe that if you seek it, you will find unanimous consent from the committee to ask Mr. Stewart to provide a response by the end of the week.

The Chair: Thank you very much.

Are there any members who are opposed to that motion? Seeing none—

Mr. Fragiskatos.

Mr. Peter Fragiskatos: Mr. Chair, I'm sorry. There was an audio issue on my end. Could you have Mr. Genuis repeat what his motion is?

The Chair: Mr. Genuis, would you please repeat?

Mr. Garnett Genuis: Mr. Chair, what I said is that I believe you would find unanimous consent that Mr. Stewart be asked to provide a response to the committee with respect to the questions that weren't answered by the end of the week.

Mr. Peter Fragiskatos: If I could, Mr. Chair....

The Chair: Mr. Fragiskatos.

Mr. Peter Fragiskatos: Thank you.

My only issue with that is that there's an ongoing investigation, and I don't know if it will conclude by the end of the week. I agree that a follow-up ought to happen. I believe information further to what's been brought forward today could be provided to the committee. That's not in question. However, putting a timeline on it by the end of this week seems a bit strange.

Mr. Garnett Genuis: Mr. Chair, could I just clarify, and hopefully it will address the concerns of Mr. Fragiskatos?

The Chair: Mr. Genuis.

Mr. Garnett Genuis: We would be clear that the committee is expecting a response to these issues by the end of the week. Mr. Stewart can provide a response before the end of the week and then we can determine, following receipt of that response, whether we want to take further steps.

It's up to him to respond, and he can do so in private in the way he thinks fit, by the end of the week. But we are clearly seeking additional information.

The Chair: Thank you very much.

Mr. Genuis has asked for unanimous consent for this motion. Does any member object to this motion?

(Motion agreed to)

Madam Clerk.

The Clerk: Just to clarify, by the end of the week.... Are we saying Friday at five o'clock?

The Chair: Does anyone object to Friday at five o'clock? That's the timing. I don't see any objections.

Mr. John Williamson: How about noon, so we can give the clerk a chance to send it around before we all knock off for the recess?

Mr. Garnett Genuis: Yes. Maybe Friday at two o'clock is fair, or noon.

The Chair: As long as we can agree on something, that would be helpful. I'm just looking for agreement.

Mr. Garnett Genuis: Sure.

The Chair: Is there an objection to Friday at two o'clock? Does everyone agree?

Some hon. members: Agreed.

The Chair: Okay, that's agreed, then.

Thank you very much to the witnesses. You are now excused.

We'll set up for the next panel, Madam Clerk.

● (1940)

_____(Pause)_____

● (1945)

The Chair: I call this meeting back to order.

I would now like to welcome, as an individual, Christopher Parsons, senior research associate for The Citizen Lab at the Munk School of Global Affairs and Public Policy, University of Toronto. We also have Mr. Janis Sarts, director of the NATO Strategic Communications Centre of Excellence, who is joining us from Riga, Latvia, where I think it's very late. Thank you both very much for being here.

I think it's 1:30 in the morning, in fact, for Mr. Sarts.

Perhaps we can start with you for your opening remarks, and then we'll go to Mr. Parsons.

Mr. Sarts, please proceed. You have five minutes.

Mr. Janis Sarts (Director, NATO Strategic Communications Centre of Excellence): Thank you very much, Mr. Chair, and thank you for the invitation.

I'll probably first describe the institution I represent, which is the NATO centre of excellence for strategic communication. It is a NATO-affiliated organization that researches and looks into the issues of influence operations, how hostile actors are using this for undermining the democracies, and how it works in the information space and increasingly into what we call cognitive conflict.

The views I will present today are views of my own, based on the research by the centre, and are not agreed positions of NATO itself.

With that caveat, I will sketch out how we see China in the influence operations. Of course, as a NATO institution, we have been looking for many years at Russian activity, but over the last few years we have increasingly been looking at Chinese activity.

To quickly look at how we see that activity, the way they process their influence operations through more soft touch, soft power angle of trying to create a favourable image of China has transformed, increasingly adopting hard-handed and assertive measures against countries—not only within their own neighbourhood, which was the case some time ago already, but increasingly adapting these measures also to countries that are further away, especially when there are key elements of contention where they believe Chinese interests are at stake. Of course, one has to point out the different value systems that democratic countries and China have.

If I look at the areas of influence that they are good at, in our view, they are very good at using the leverages they have, especially on the economic front and the infrastructure front. They are very active in the technology landscape, first and foremost in cyber activities, hacking and espionage, but also at more nuanced technology activities, like data and emerging technologies. They are also quite good in most of the cases, but not always, at targeting Chinese communities for their influence.

Where they are not yet very good, but they're quickly gaining ground, is in what we call the information warfare. We've noted that in most of the cases they've used what I would call an old-school methodology of the communist propaganda system that has not worked very well. However, they have been quickly adopting...in particular, some of the Russian tactics have been adopted on the information front as we speak.

As next steps, we see that they will increasingly try to leverage their technological powers and try to gain more say into the infrastructure of the future of these technologies. I believe they see data and AI as very critical future technologies where they would want to have strong leverage, not only within China but also outside.

We look at the social scoring systems they have developed, which we believe are not the way the technology has to be used, but we see, with a concern, the export of this technology and the possible impact of the social scoring system on western companies wanting to operate on Chinese territory, which I think will have significant impact.

All in all, as the Chinese modus operandi changes to a more hard-handed approach, we foresee that there will be more contention, more pressure, especially given that the core elements of the Chinese system and the way they view the world are fundamentally different from those of democratic countries. Therefore, there is in-built conflict on the values system side.

● (1950)

We therefore see an increase in not only the competition but also the influence operations from China. They will increasingly try to leverage especially the technology but also the economic and infrastructural positions they have.

Thank you, Mr. Chair.

The Chair: Thank you very much, Mr. Sarts.

Mr. Parsons, you have five minutes. Please proceed.

Mr. Christopher Parsons (Senior Research Associate, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, As an Individual): Thank you.

Good evening. My name is Christopher Parsons. As mentioned, I'm a senior research associate at the Citizen Lab. I appear before this committee in a professional capacity that represents my views and those of the Citizen Lab. Comments are based on our research into Chinese technology companies. The Citizen Lab is an academic institution, and our work operates at the intersection of technology and human rights.

In my time today, I want to point to some of the ways by which we can develop trust in the products and services that are manufactured in, transited through or operated from China. I do so by first turning to the issue of supply chain dependencies.

A rising concern is the extent to which Canadian companies, such as our telecoms, might become dependent on products made by Chinese companies, inclusive of Huawei. Dependency runs the risk of generating monocultures or cases in which a single company dominates a Canadian organization's infrastructure. In such cases, up to three risks can arise.

First, monocultures can enable foreign governments to leverage dependencies on a vendor to apply pressure in diplomatic, trade or defence negotiations. Second, monocultures can create a path dependency, especially in 5G telecommunications environments, where there's often a degree of vendor lock-in into vendors' telecom equipment. Third, monocultures risk hindering competition among telecommunications vendors, to the effect of increasing capital costs to Canadian telecommunications providers.

All of these challenges can in part be mediated by requiring diversity in Canadian telecommunications companies' networks, as has been recommended in the past by CSE's deputy chief of information technology security, Scott Jones. In this case, trust would come from not placing absolute trust in any given infrastructure vendor.

I now turn to building trust in software and hardware systems more generally. Software and hardware errors are often incidentally placed into digital systems. Some errors are egregious, such as including old and known vulnerable code in a piece of software. Others are more akin to spelling or grammar errors, such as failing to properly delimit a block of code. There are also limited situations where state agencies compel private companies to inject vulnerabilities into their products or services to enable espionage or attack operations.

No single policy can alleviate all of the risks posed by vulnerabilities. However, some can enhance trust by reducing the prevalence of incidental vulnerabilities and raising the cost of deliberately injecting vulnerabilities into digital systems. Some of these trust-enhancing policies include, first, requiring companies to provide a bill of goods that declares their products' software libraries and dependencies, as well as their versions. This would help ensure that known deficient code isn't placed in critical infrastructure and also help responders identify vulnerable systems upon any later discovery of vulnerabilities in the libraries or dependencies.

Second, Canada and its allies can improve on existing critical infrastructure assessments by building assessment centres that complement the U.K.'s, which presently assesses Huawei equipment. Working collectively with our allies, we'd be better able to find incidental vulnerabilities while raising the likelihood of discovering state adversaries' attempts to deliberately slip vulnerabilities into systems' codebases.

Third, Canada could adopt robust policies and processes to ensure that government agencies disclose vulnerabilities in critical infrastructure to appropriate vendors and communities, as opposed to potentially secretly hoarding them for signals intelligence or cyber-operations.

I will now briefly turn to increasing trust in Chinese social media platforms. Citizen Lab research has shown that WeChat has previously placed Canadians' communications under political surveillance to subsequently develop censor lists that are applied to China-registered WeChat accounts. Our research into TikTok, released today, revealed there's no apparent or overt political censorship or untoward surveillance of Canadians' communications on that platform.

Based on our findings, we suggest that social media companies be required to publish more information on their activities to enhance trust. This would include publishing detailed content moderation guides, publishing how and why companies engage in monitoring and censoring behaviours, publishing how organizations interact with government agencies and address their corresponding demands, and publishing annual transparency reports that detail the regularity and effects of state and non-state actors who make requests for users' data.

Platforms could also be compelled to make available algorithms for government audit where there is reason to suspect they're being used to block or suppress lawful communications in Canada or where they're being used to facilitate influence operations. Platforms could also be compelled to disclose when user data flows through or is accessible by parts of their organizations that have problematic human rights, data protection or rule of law histories.

To conclude, we at the Citizen Lab believe that the aforementioned sets of recommendations would ameliorate some of the cyber-related risks linked with the Chinese supply chain management issue, and social media platform issues more broadly. However, we also believe these policies should be applied in a vendor- and country-agnostic way to broadly improve trust in digital systems.

● (1955)

I would just note to the committee that the brief we have also submitted provides additional details and recommendations, especially as applied to Internet standards, which I have declined to get into in this.

Thank you for your time, and I look forward to your questions.

The Chair: Thank you very much.

[*Translation*]

Mr. Paul-Hus, we will begin the first round of questions with you. You have six minutes.

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

Gentlemen, thank you for joining us tonight.

My first question is for Mr. Sarts.

I served for three years as Vice-Chair of the Defence and Security Committee of the Canadian NATO Parliamentary Association. We often had discussions about Russia and the various physical or cyber threats. We also talked a little about China. For the last few years, we had difficulty understanding the NATO alliance's somewhat unclear position on those cyber threats.

Can you tell me briefly whether you feel that the alliance is better able to stand together against cyber threats like those from China?

[*English*]

Mr. Janis Sarts: Well, the alliance is the collective nations. As you know, for nations to agree, it takes time, and also to develop the capabilities, it takes time.

I think in the last decade, basically, the alliance has zoomed much more on the cyber-defence. Instead of just being a national business, it has been moved to the collective business. The cyber realm has been named a new domain for NATO as an alliance, and certainly the collective capabilities have increased. However, of course, as we know—

● (2000)

Mr. Pierre Paul-Hus: Thank you, sir. I must continue. Thank you very much.

[*Translation*]

My next question is for you, Mr. Parsons. It's good to see you again.

In your report, you state that our country has a 5G strategy problem. It is linked to the fact that the Government of Canada lacks a principle-driven set of integrated, industrial, cyber security, and foreign policy strategies that directly and meaningfully address the challenges raised by the current and expected 5G landscape.

Can you tell us more about this lack of a comprehensive strategy and how this leaves Canada vulnerable to China?

[*English*]

Mr. Christopher Parsons: In the work that the Citizen Lab has done, one of the points we have made is that there's a concern that we have in that there's a great deal of attention focused on Huawei and the vulnerabilities in Huawei equipment. While it's appropriate to be concerned about that vendor, there's an equal need to look at how other companies that may serve a 5G infrastructure operate. We believe that both Ericsson and Nokia, as well as Samsung and other parties, should similarly go through strong assessments to ensure that all equipment that goes into Canada's infrastructure is strong.

It's not sufficient to remove Huawei and then let in other vendors who may have security deficiencies.

[*Translation*]

Mr. Pierre Paul-Hus: Yes, all communications companies should be subject to assessments to protect Canada.

The Chinese government was recently accused of being behind cyberattacks on Microsoft Exchange. How capable do you think Canadian government infrastructures are of countering these types of attacks? For example, we have heard that the Prime Minister's Office had to shut down its website to protect itself. Do you have any information on that?

[*English*]

Mr. Christopher Parsons: Even in the context of critical infrastructure development, such as telecoms, Canada can't go it alone. Indeed, for most services, Canada can't go it alone. As a result, one of the things the Citizen Lab has recommended is that Canada, along with like-minded friendly nations, figure out ways of doing information assurance collectively. That may mean that in the hardware space, one country looks at Samsung, another at Huawei, another at Ericsson. When it comes to services, such as Microsoft's challenges, again, a coordinated analysis by the NSA, the CSE, the GCHQ and other intelligence alliances is important to assess and identify these vulnerabilities.

[*Translation*]

Mr. Pierre Paul-Hus: I referred to the paragraph in your report in which you clearly mention that Canada lacks clear policies on cybersecurity management and that it is not ready to properly administer this area.

Right now, the government's and the Prime Minister's systems are already under cyberattack. Should we be concerned about that? Do you really think our infrastructure is sufficient to defend us?

[*English*]

Mr. Christopher Parsons: The concern that I and my colleagues have written about in the past is that there does seem to be an ongoing incoherence to the way that Canada has developed its cybersecurity strategy.

I would note that, while there is a federal policy, it is somewhat out of date, and the instrumentalization of that policy has not seen the light of day, so if it exists, it's not public to date.

[*Translation*]

Mr. Pierre Paul-Hus: The U.S. government has a blacklist of Chinese companies that pose a risk to American national security. Moreover, the Chinese army is conducting cyber espionage operations. We know that such operations are conducted from Chinese territory. Actually, computer technology makes it possible to know where the connections are.

According to the information you have, do some operators carry out cyberattacks from Canada?

[*English*]

Mr. Christopher Parsons: I believe that was directed to me.

Thank you for your question.

Unfortunately, the Citizen Lab does not have that kind of intelligence.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

My time is up.

● (2005)

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

[*English*]

We'll now go to Ms. Zann for six minutes.

Do we have Ms. Zann, or has she been disconnected for some reason?

If I don't have Ms. Zann, I think I'll have to go on to Ms. Yip.

Go ahead, Ms. Yip, please.

Ms. Jean Yip: Thank you for coming before us at this committee.

My question is directed to Mr. Parsons.

You mentioned in your brief that you don't feel that it should be only one vendor—there should be many vendors—because it makes us vulnerable across our entire spectrum. How can we build a strong 5G network?

My next question is this: How can we, with so many vendors potentially participating, make it a coherent network if things tend to be sticky between the networks?

Mr. Christopher Parsons: I believe, and this is paralleled by the CSE, that what's required is to ensure that our networks have multiple vendors operating in them. That may mean that there's a combination of Samsung, Ericsson, Nokia and other vendors as appropriate.

In order to assess them, again, I think we would work collaboratively with our international partners to ensure that the technologies that are going in are fit for duty. Moreover, we're talking about billion-dollar purchases. We can impose some sort of expectations on interoperability.

Further, with regard to stickiness, there's a process taking place right now called Open RAN, which would, in a way, democratize some of the way telecommunications equipment is set up. It would basically let you take equipment off the shelf, as opposed to highly specialized equipment, and use that to develop parts of the 5G radio network.

I believe that the Canadian government pushing towards that would be one way of improving the network and reducing some of the stickiness at least.

Ms. Jean Yip: How concerned should Canada be about China's involvement in developing the Open RAN standards?

Mr. Christopher Parsons: Because it is an open standard, I think it's something to be mindful of that China is involved, but it makes sense economically for their carriers as well.

I think it's an area where Canada has to actively engage, and one of the ways of doing it—in addition to, of course, the Government of Canada directly participating—is finding ways of encouraging our corporations, businesses and academic units to also participate, which could involve some sort of fund set up by the Government of Canada to enable academics or non-profits to participate and possibly find other ways based on tax incentives to encourage our companies to also get involved in those discussions.

Ms. Jean Yip: Would they be willing to do this if there were intellectual property concerns?

Mr. Christopher Parsons: One of the aims and aspirations of the Open RAN alliance is to ensure that the technology is in fact open, a series of standards that aren't inherently captured by one organization or one company or another.

They are self-interested in getting involved in that because, right now, if you purchase equipment from any of the large vendors, it's quite expensive, and Open RAN currently promises to reduce those costs, so there is an incentive, even if they don't own the IP, to be involved in developing the standard itself.

Ms. Jean Yip: In regard to your recommendations on Chinese social media, are there any western social media platforms that operate at this level of transparency, and if so, what actions were taken by the governments to have them give up this information?

Mr. Christopher Parsons: There aren't currently any in North America that adhere to all of the recommendations we have. We are certainly trying to advocate for increasing trust writ large, so not just in Chinese social media but also companies that we're very familiar with, such as Facebook, Twitter and the rest.

There are some elements on which we're seeing movement in North America. As an example, we have more robust transparency reports that are available in other jurisdictions. Facebook and others do disclose their lawful access handbooks. They're quite useful and quite accessible. However, we don't have things like algorithmic transparency or accountability, nor do we necessarily have the degree of awareness as to how companies interpret the law, which is almost more important than anything else, because how a company interprets the law versus how the law is written can often be not one to one.

● (2010)

Ms. Jean Yip: You mentioned in your brief that the most significant breach of cybersecurity in recent history happened when SolarWinds was hacked over the course of nine months last year. To your knowledge, what has the impact been for Canadian organizations using SolarWinds products?

Mr. Christopher Parsons: To the best of my knowledge, and based on open-source information, there has been a relatively minimal breach of Canadian organizations to date, although we are learning almost on a daily or weekly basis that the number of victims is going up. The current impact seems to be relatively minimal, but I suspect that the actual assessment of that will take a considerably longer period of time.

Ms. Jean Yip: During your last appearance before a House of Commons committee, in February 2019, you addressed the issue of encryption and how Canada needs to adopt a national encryption policy. Could you tell us how this would protect us from foreign interference?

Mr. Christopher Parsons: Encryption is one of the few things that can be relied upon to keep data safe. One of the things that the Citizen Lab has argued for repeatedly is the availability of what's called end-to-end encryption. It's encryption where a message is secured from your device, goes to someone else's device, and only the two parties can access it. That's especially important as we see more and more systems move to the Internet, because it ensures that when and if the network is compromised, whoever is compromising the network can't gain access to the communications that are transmitted across it.

The Chair: Thank you very much.

Thank you, Ms. Yip.

Ms. Jean Yip: Thank you.

[*Translation*]

The Chair: Mr. Bergeron, you have the floor for six minutes.

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

I would like to thank the witnesses for being here, for giving us their time and for enlightening us with their comments. I am clearly grateful to Mr. Parsons, but particularly to Mr. Sarts, given the very late hour. I will address Mr. Sarts first.

On February 22 of this year, the European Parliament held a meeting of the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation. You participated in that meeting and discussed how disinformation works. When we look at your findings on the 2019 European parliamentary elections and the 2020 American election, we have every reason to be very concerned about what's next.

You will be able to enlighten me on this, but one might think that all NATO countries are facing this same sort of foreign intervention in elections. But it is a bit surprising that, according to Greg Austin, who leads the Cyber, Space and Future Conflict Programme at the International Institute for Strategic Studies, China's cyber defence capabilities are far below those of the major western powers, including Canada. For example, Canada ranks 9th of 155 countries assessed, while China ranks 27th.

Aside from the fact that they rely heavily on private companies, why would western powers allow themselves to be put in this vulnerable position without reacting?

Mr. Janis Sarts: Thank you for the question.

[*English*]

We've been looking.... Most of these social media companies that we use for everyday life have become the agora for democratic process. Most of the elections actually play out in these platforms. We've detected that most—basically all—of those platforms are manipulable by robotic networks to put the messages and to game the algorithms—including during the election processes—to advance particular interests, including of hostile actors.

We've been measuring, every year, how well the platforms do in taking out these robotic networks from platforms, and the results have been very disappointing. Back in 2019, when there were European Parliament elections, we bought 55,000 different actions through robotic accounts on social media—of course, neutral effects—for 300 euros. During the EU parliamentary elections, 90% of that got delivered.

We repeated the same experiment during the U.S. presidential election, once again in a neutral manner. We were able to buy likes, shares, views, custom-made comments and all of that, but this time 300,000 for $300. About 70% of that got through. Basically, there was an option for outside actors to influence the discourse.

Most of the companies were incapable of eradicating that process. If I had to measure the companies, typically Twitter is the best at it. Facebook is less so. Last year, we measured TikTok for the first time. TikTok is basically defenceless. You can do any gaming of that system that you wish. Of course, the more potential electors there are out there, the more malign things can be happening.

Clearly, that goes back to Mr. Parsons's point that there is no way to oversee what the social media companies are doing. They're declaring great success, but when we turn to the vendors of these manipulations, it's cheap, available and effective. We have to have oversight to make sure that it is neither simple nor easy.

Thank you.

● (2015)

[*Translation*]

Mr. Stéphane Bergeron: Thank you for that very detailed answer. But I would like to come back to the question I asked you, Mr. Sarts.

China is considered to have a cyber defence capability that is far inferior to that of most western powers. I suppose one could say exactly the same thing about Russia. In this case, why are western powers content to put themselves in a vulnerable situation? Why don't they use their superior capabilities to establish a system of deterrence, to discourage powers like China or Russia from engaging in these sorts of practices, or face strong retaliation?

[*English*]

The Chair: You can give a 10-second answer, Mr. Sarts.

Mr. Janis Sarts: I think the U.S. just did it in 2020 by discouraging Russia, as we've seen from open-source reports, so it is possible to do if you have leverage, resources and the political will.

The Chair: Thank you very much.

We'll go to Mr. Harris, for six minutes, please.

Mr. Jack Harris: Thank you, Chair.

Thank you, both, for your interesting presentations.

Mr. Sarts, you just described, in the EU elections, the ability to buy data and then send messages to that data. Can you give us an example of where that would come from? Would this be private operators providing this information for sale to make money, or is this part of some other effort that might be done by a state actor?

Mr. Janis Sarts: Both. There are private actors that do it for sale. There are what we believe to be—by continuously following these networks—state actors. In some cases, there are hybrid networks where most of the time they would do business-related things for gaming marketing or influencer posts. About 10% to 15% of the time they would do the political impact. There are a variety of players in the field.

Mr. Jack Harris: So you can influence an election by getting information about who likes what and then sending targeted messages. Is that exactly how it works?

Mr. Janis Sarts: That is one of the ways. Of course, you can use these automated robotic networks, which seem like humans, to create reactions en masse in the online media, gaming the algorithm—for instance, making some posts much more visible than others, making specific comments at the political leaders' social media presence discouraging, or making false appearances. There are many ways one can use that infrastructure for effect.

● (2020)

Mr. Jack Harris: Is there any technical or technological defence to any of it? How do you deal with it?

I was reading a comment about when you testified at the United States Senate Select Committee on Intelligence in 2017, suggesting that public awareness campaigns could counter and influence operations that target populations.

Of course, that was 2017, and we've seen an awful lot happen since then. Are you optimistic? Was that an optimistic statement, that public awareness campaigns could be a defence against this, or are there other techniques that might be possible now?

Mr. Janis Sarts: First, public awareness campaigns are important, because if we don't do them, then we are even more vulnerable. But on the particular issue, obviously part of the defence is within the social media companies.

In our assessment, they are not doing [*Technical difficulty—Editor*] public discourses that are happening on these platforms, and therefore some kind of regulatory framework on our side would be necessary.

Mr. Jack Harris: How would they stop them, Mr. Sarts?

Mr. Janis Sarts: Actually, it is very simple. You can create algorithms that see these things for what they are. For instance, if we buy this robotic accounts effect, you can see that account. We report that account to Facebook or Twitter.

Most of the time, their algorithm doesn't detect it. It's just a matter of upgrading their algorithms and being better at their jobs. That is not the case, at this point.

Mr. Jack Harris: You're saying that these companies could actually police that activity, if they were motivated to do so, shall we say.

Mr. Janis Sarts: Yes, if there were a better business case for them, I believe they could.

Mr. Jack Harris: You also talked about another tool that's used, called data scraping. I guess that's what we're talking about here, using artificial intelligence, algorithm and data scraping to influence behaviour.

You referred to some event actually influencing the behaviour of military operatives by obtaining information. Could you explain how that works and what the dangers can be in something like that?

Mr. Janis Sarts: Yes. Two years ago, we tried an experiment trying the hypothesis that open-source data can be used to influence human behaviour. We did an experiment together with the Latvian armed forces, during a military exercise, where we scraped the open-source data for the soldiers. Based on that data, we tried to impact their behaviour during the military exercise.

We succeeded in making soldiers disobey orders, making them leave the positions they were supposed to defend, just based on the data that was available. This basically underlined the future risk of big data that is available. If it's used in a malign way, it can not only bring, as it does currently, the marketing product; it can also shift beliefs and behaviours. In the wrong hands, it is a very dangerous tool.

In that respect, I would highlight the future risks of 5G. It's not only about the infrastructure; it's also about the data that is going to flow in that system. It is incredibly valuable, if you look from the hostile actor's perspective, to get access to that kind of societal data, because with certain AI capacity you could actually sway the behaviours of the other societies.

Mr. Jack Harris: That's fascinating. I was in Riga at one time with the NATO Parliamentary Association; I think I've been at your centre. There was a lot of concern in those days about the disinformation campaigns of the Russians, trying to undermine the interest in democracy in the Baltic states.

Is that still going on?

Mr. Janis Sarts: Yes, it is of course still going on, but as we see, from a Russian perspective they have moved their eyes more towards other, bigger players. They're spending most of the resources there. Of course, the Baltics are still a target, but not the main target.

The Chair: Thank you very much.

Thank you, Mr. Harris.

As we only have a few minutes remaining, what I propose to do is try to distribute it equitably, with three minutes to Mr. Williamson and three minutes to Ms. Zann.

[*Translation*]

Then, Mr. Bergeron will have one minute and 30 seconds.

[*English*]

Finally, Mr. Harris will also have one and a half minutes.

Mr. Williamson, you have three minutes.

Mr. John Williamson: Thank you.

Mr. Parsons, I see you co-authored a report a couple of years ago, "The Predator in Your Pocket". It touched on DNA sourcing and DNA transfers. You referenced 23andMe.

We now fast-forward a year and a half. The world's largest biotech firm, BGI, was given approval by Health Canada to offer COVID-19 testing in this country.

Do you have concerns about the transfer of the health information and DNA of Canadians to mainland China for use in that country?

● (2025)

Mr. Christopher Parsons: I haven't looked specifically into that case. Certainly what we have seen in our research and analysis of other parties' research is that DNA information is incredibly sensitive.

There is a concern, of course, when any highly sensitive data is moving to any country outside of Canada, and that would be inclusive of China.

Mr. John Williamson: Can you talk about the information on 23andMe and expand on why you felt the need to highlight that in the paper and why that was a risk?

The difference here is that this is on an individual basis where that information is being collected and possibly shared, versus the BGI, which is possibly collecting it on hundreds of thousands of Canadians. Could you just address why for 23andMe and that transfer it's critical to have a handle on it?

Mr. Christopher Parsons: Yes, absolutely.

The first concern is how that data will be used to affect the individuals themselves. It's collected under a certain set of terms. Will that set of terms be applied on an ongoing basis?

The secondary concern is that while it does reveal information about the individual, it also reveals information about their entire family, including members who may not yet be born. The ability to use genetic information to drive information about your current or forthcoming next of kin is something that we really can't predict. Genetic technology is just exploding. The actual uses are pretty broad.

Mr. John Williamson: As I understand it, it is possible with that information for scientists to even proactively discover and then reach out to individuals and say, "You could very well develop this disease...or this medical treatment." I think that just puts the emphasis on how this data is important.

What do you think Canada should do to safeguard the biodata of Canadians?

Mr. Christopher Parsons: It's a very good question. I can only speak in the commercial context, as I'm not sufficiently aware of how it's being handled in China.

Generally, I think there should be strong requirements that delimit how information can be used, inclusive of no secondary uses can be used, or no more applications of primary uses can be used, without the affirmative and meaningful consent of the individual.

The Chair: Thank you very much, Mr. Williamson.

Ms. Zann, you have three minutes.

Ms. Lenore Zann: Thank you very much.

I have to say, it's been very interesting, both the meeting and the presentations. I want to thank both gentlemen for the very interesting information they've shared with us. I wish I had longer.

Mr. Sarts, I would like to ask you about "Disinformation as a Threat to National Security", in your book *Disinformation and Fake News*.

You must have been extremely concerned when you saw what was going on in the United States with regard to the storming of Washington, of the capitol, and with all of the disinformation that has been propagated on social media and really continues.

Can you please explain to us how you think we can best fight against the creation of divisions in society and the widening of existing fractures that undermine trust in government, the military, and the country's security systems?

Mr. Janis Sarts: I would say first, yes, we're undergoing profound change in the information environment, the very core of what creates and makes the democratic process run, the bloodstream of a democracy. It's changing in a way that is not helpful for society coming together.

To a large extent it is because the social media companies have found a way to monetize that environment through promoting information that is biased, creating echo chambers or information bubbles, and increasingly putting the citizens within those bubbles. It is with outside interference that it happens, and of course, outside hostile actors just exacerbate that situation.

Therefore, going back to the fundamentals, we have to make sure that the rules and laws we have in a normal democratic discourse would be applied to the same place. At least the algorithmic transparency is a must, and of course, then we would see how to make it more adequate.

● (2030)

Ms. Lenore Zann: Thank you.

I've also read that the more explosive a statement can be on social media, the more it attracts the eyes of people. You can tell the biggest lie and make the most extravagant statement, and that's the sort of thing people are attracted to.

Could you expand on that a little, please?

Mr. Janis Sarts: That's what the neuroscience says on how the human brain works. We are attracted to the emotional and instinctive things, and it is much harder to go about the rational decision-making.

The algorithms of those social media companies are actually using that element for gaining our attention. The more attention there is, the more money they can make, and I think that's actually the wrong thing with this.

Ms. Lenore Zann: Thank you. I appreciate that.

The Chair: Ms. Zann, your time is up.

[*Translation*]

I will now give the floor to Mr. Bergeron for one minute and 30 seconds.

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

My question is for Mr. Parsons.

Adam Segal, director of the digital security program at the Council on Foreign Relations, believes that both WeChat and TikTok should not be installed on the phones of U.S. officials or government employees.

In your brief, you mention that the Canadian Security Intelligence Service apparently warned members of Parliament that they should avoid using WeChat, because of nebulous cybersecurity risks.

Should Canadians and Quebeckers also be concerned about WeChat and TikTok, and follow the recommendations from CSIS?

[*English*]

Mr. Christopher Parsons: I believe what is important when looking at these platforms and systems is to appreciate that some people have greater or less great risks than others. Elected officials, in one case, might be concerned about the data that is being collected. However, in our research on TikTok we found no overt surveillance and no overt censorship. It might happen at some point, but not in our research.

In the case of WeChat, we saw that there has been the usage of Canadians' communications to build up a censor index that is then applied to individuals who operate or live within China. Therefore, I think Canadians are right to be concerned, in particular about the way that WeChat has historically, at least, used their communications to build that censor index.

Currently, we have no evidence of a clear problem with TikTok.

[*Translation*]

Mr. Stéphane Bergeron: Do I have any time left, Mr. Chair?

The Chair: Your time is up.

[*English*]

Now we'll go to Mr. Harris for one and a half minutes.

Mr. Jack Harris: Thank you, Mr. Chair.

Mr. Parsons, I have lots of questions for you but not very much time to ask them.

One very important one is that you make six recommendations regarding what companies should be required to publish with respect to their social media platforms, including publishing guidelines explaining the way they're subject to state mandate and surveillance, that they make their algorithms available for government audits, that they provide transparency reports, and so on.

Do we have the means to actually force companies to do those things in order to be able to operate in this country?

Mr. Christopher Parsons: For some of them, we certainly do. As one example, I think we could compel Facebook and other companies to explain how they interact with perhaps Chinese companies as well as Canadian companies.

In other cases, I believe we would have to work with our allies—the United States, Europe and other jurisdictions—to put pressure on the companies and/or pass legislation in the countries out of which they operate.

Mr. Jack Harris: Is there any activity coordinated to do that work, or is that something you're recommending we should start to do? Is it happening already?

Mr. Christopher Parsons: I think we're seeing pieces of that in the United States and the European Union, but it isn't something I would say is an agreed-upon position by respective governments. It's a place where Canada can participate with our closest allies to make movement on this.

● (2035)

Mr. Jack Harris: We'd better get cracking if we're going to have any control over this monster.

Mr. Christopher Parsons: We certainly hope this will be something the government looks at.

Mr. Jack Harris: Thank you.

The Chair: Thank you very much, Mr. Harris.

Mr. Parsons, thank you very much for understanding how much we appreciate you, and thank you, Mr. Sarts, for whom it's now 2:30 in the morning. I'm sure you won't mind us making a particular fuss about the fact that it's so late. We very much appreciate both of you being with us this evening.

The meeting is adjourned.