



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 027

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Thursday, June 2, 2022

Chair: The Honourable Jim Carr



Standing Committee on Public Safety and National Security

Thursday, June 2, 2022

• (1100)

[English]

The Chair (Hon. Jim Carr (Winnipeg South Centre, Lib.)): Good morning, everyone. I call this meeting to order.

Welcome to meeting number 27 of the House of Commons Standing Committee on Public Safety and National Security. We will start by acknowledging that we are meeting on the traditional, unceded territory of the Algonquin people.

Today's meeting is taking place in a hybrid format pursuant to the House order of November 25, 2021. Members are attending in person in the room and remotely using the Zoom application.

Pursuant to Standing Order 108(2) and the motion adopted by the committee on Thursday, March 3, 2022, the committee is resuming its study of the assessment of Canada's security posture in relation to Russia.

With us today are the Honourable Bill Blair, Minister of Emergency Preparedness, and Mr. Rob Stewart, deputy minister of the Department of Public Safety and Emergency Preparedness. Welcome to you both.

Minister, I now turn the microphone over to you for your opening statement.

Hon. Bill Blair (Minister of Emergency Preparedness): Thank you very much, Mr. Chair.

I'd like to also take the opportunity to thank the members of this committee for your kind invitation to have me appear before you today.

While this is not my first time before many of you, today marks my first committee appearance in my new role as president of the Queen's Privy Council and as the Minister of Emergency Preparedness.

Your study on Canada's security posture when it comes to Russia is an important one. I'm very pleased to have the opportunity to speak before you today and to discuss some of the ways in which Canada has been and continues to prepare itself to deal with any eventuality.

Russia's invasion of Ukraine on February 24 was a blow to the sovereignty of that nation and an immediate threat to all democracies around the world. The death toll of this conflict for the Ukrainian people is staggering. As of June 1, the UN High Commissioner for Human Rights has recorded over 4,000 civilians killed, including 267 children. Thousands more are recorded in-

jured, and the UN acknowledges that the actual figures could very well be considerably higher.

We continue to join our allies in condemning Russia's unjustified and unprovoked actions. Our government, and particularly my cabinet colleagues, Minister Anand and Minister Joly, are working tirelessly to impose severe costs on Russia for their actions and to ensure that Ukraine has the tools and support it needs to continue the fight. Throughout this situation, we remain on the lookout for all potential Russian threat activity within Canada and affecting Canadians' interests around the world.

Canada is operating in an increasingly complex domestic and global threat environment. We are emerging from over two years of a global pandemic. The impact of climate change is accelerating, leading to more frequent and more severe natural disasters. As our national security agencies regularly caution, our country remains a target of foreign actors who seek to advance their interests to the detriment of Canadians and Canada.

Threats from countries like Russia can take on many forms. Espionage, cyber-attacks and various methods of foreign interference are only a few examples. Disinformation, which is a subject that I know is of great interest to this committee, is another. Federal national security agencies like CSIS, CSE and the RCMP continue to play a key role in deterring and dismantling many of these threats before they can cause harm to Canadians. I understand that Minister Mendicino has also been invited to appear before you on this study. I fully expect he'll be able to go into greater detail about the work of the agencies under his purview.

As the Minister of Emergency Preparedness, part of my responsibility is not only to prepare for future emergencies but to look at where we can proactively mitigate risks. In this country, we have adopted an "all hazards" approach to this work. If disaster does strike and threaten the safety of Canadians, one of the responsibilities of my office is to play a coordinating and convening role to support the Prime Minister and the cabinet through our immediate response.

In times of crisis, Canadians expect their governments to work together efficiently, expeditiously and effectively in order to ensure their safety and to address the situation at hand. One of the key ways in which the federal government coordinates during an emergency is through the federal emergency response plan, which I'll refer to hereafter as FERP. The federal government turns to the FERP when an emergency is so significant that it requires an integrated federal response. The FERP is intended to cover hazards of all kinds, including both domestic and international emergencies.

The FERP was last updated in 2011. As our threat environment continues to evolve, we must continually assess our response plans to ensure they remain relevant and effective. To that end, Mr. Chair, I've been given a mandate by the Prime Minister to look at the renewal of the federal emergency response plan.

The quick and accurate flow of information is also critical in an emergency. That is why I would also like to take an opportunity to recognize the important work of the government operations centre. In any active situation, the GOC's public servants play an essential role in monitoring, keeping all implicated partners informed and providing assistance in coordinating the response. It is a 24-7 responsibility. I take the opportunity to commend them for their extraordinary work, particularly over the past two years, when we've seen enormous requirements and demands upon them through the pandemic and through natural events such as the floods in British Columbia, the wildfires experienced right across this country, and many other similarly challenging events.

As we speak, Russian forces remain within Ukraine's borders. The harm they have already caused—the destruction of cities and the widespread loss of life—is something they must be held accountable for.

As a government, we remain committed to ensuring the safety of all Canadians. We will continue to work closely with our partners on mitigating risk, building resiliency and ensuring we are ready if and when an emergency occurs.

Mr. Chair, thank you for the opportunity to provide my opening remarks. I look forward to the committee's questions.

• (1105)

The Chair: Thank you, Minister. You won't have long to wait, because those questions begin right now.

The first slot goes to Mr. Lloyd.

Sir, you have six minutes, whenever you want to begin.

Mr. Dane Lloyd (Sturgeon River—Parkland, CPC): Thank you, Mr. Chair.

Thank you, Minister and your official, for coming out today.

You certainly haven't had any shortage of natural disasters to deal with since you took on your role, Minister. It feels like your role in emergency preparedness is overwhelmingly or almost entirely focused on these very serious natural disasters. However, we know from this committee that Canada is not immune to emergencies related to foreign espionage, specifically cyber-attacks. We've seen that Russia is particularly adept, but there are other countries as well.

You didn't mention anything about cyber-attacks. I know the FERP hasn't been updated since 2011. You said there is an update coming.

What are we going to do about the threat to our cybersecurity? What are you doing as in your role as minister?

Hon. Bill Blair: Thank you very much. Mr. Lloyd. It's a very important question.

I want to assure you that the whole of government is seized of our responsibility. The response is primarily led within our government by the Communications Security Establishment, the CSE, which is under the Minister of National Defence. It also involves the important work of other national security intelligence agencies, such as CSIS, and any criminal investigation arising is the responsibility of our federal policing service, the RCMP.

I will tell you that Canada and its allies have attributed malicious cyber-activity to Russia in the past, including in 2018 for the development of what was called the NotPetya malware, which was used to indiscriminately attack critical financial, energy, government and infrastructure sectors around the world. In addition, in 2021, you may recall that Canada joined its allies in attributing SolarWinds compromises to Russian state-sponsored actors, involving malware being installed in an attempt to steal data and cause costly mitigation activities.

In Canada, we are very fortunate to have laid an important foundation in the national cybersecurity strategy, which is intended to help protect Canadians. This has already led to the establishment of the Canadian Centre for Cyber Security, which is a single, authoritative source for expert technical advice and support for Canada and Canadians. The centre provides public advisories and—

Mr. Dane Lloyd: Thank you for that.

Hon. Bill Blair: There's a great deal more information, Mr. Lloyd. I'll happily go into it with you if you have time.

Mr. Dane Lloyd: Thank you. We have a short time.

You noted that you've attributed the SolarWinds attack in 2021 and a previous cyber-attack in 2018 to Russia. You talked about disinformation.

Has your government identified disinformation in the 2021 federal election as being from foreign sources?

• (1110)

Hon. Bill Blair: I can advise you—I checked in anticipation of your question—that I have not received any information that Russia was involved in any effort at foreign interference in the last federal election.

Mr. Dane Lloyd: I understand that, but if Russia sees that one country can influence our elections, they might be emboldened to try to do that themselves.

Has your government identified any foreign interference in the 2021 federal election?

Hon. Bill Blair: I can tell you that our agencies were very active. It was during the period of the caretaker regime, on which perhaps the deputy minister could provide more information, but they were very alert and vigilant with respect to foreign interference in our last election.

I have not received directly any information that would provide evidence of—

Mr. Dane Lloyd: Are you personally aware, even anecdotally, of any foreign interference in the 2021 federal election?

Hon. Bill Blair: I think we've all heard anecdotes and various opinions laid, but I have not directly received any information from our intelligence services that provided evidence of that foreign interference. Perhaps the deputy minister—

Mr. Dane Lloyd: Deputy Minister, is that something that you guys are pursuing? Are you investigating the potential for foreign interference in the 2021 federal election?

Mr. Rob Stewart (Deputy Minister, Department of Public Safety and Emergency Preparedness): Absolutely. We had the security in elections task force and a cabinet-established panel of five deputy ministers who would be in receipt of that information.

Mr. Dane Lloyd: When can Canadians expect a report on that, if any?

Mr. Rob Stewart: The panel was stood up to monitor the election and to make sure there was no threat to the overall integrity of the election, and that was—

Mr. Dane Lloyd: Did it conclude that there was no threat to the election?

Mr. Rob Stewart: There was no threat to the overall integrity of the election.

Mr. Dane Lloyd: What about in individual ridings? Did they determine that there was any impact on individual ridings?

Mr. Rob Stewart: No. We did not adjudicate individual ridings.

Mr. Dane Lloyd: You are saying today that your intelligence has said that there was no impact on individual ridings of foreign interference in the 2021 election?

Mr. Rob Stewart: I am not saying that.

Mr. Dane Lloyd: You said you couldn't say that there was an impact on any ridings.

Mr. Rob Stewart: There was no threat to the overall integrity of the election. There were, as you would expect, activities on social media that would constitute disinformation and attempts by various parties to influence votes in various—

Mr. Dane Lloyd: Minister, you've now heard from the DM that there was foreign influence in the 2021 election. What do you have to say about that?

Hon. Bill Blair: Perhaps I misheard, but I heard the deputy minister say that there was no foreign interference impacting on the integrity of the election.

Mr. Dane Lloyd: On the overall election, but the deputy minister did just clearly state that there was foreign...

You did say that there was foreign interference in the election.

Mr. Rob Stewart: No, sir, I did not.

Mr. Dane Lloyd: You just said that the overall integrity of the election was protected, but you did cite social media attempts at foreign interference in the 2021 federal election.

Mr. Rob Stewart: No, I said there were social media efforts to influence the outcome of the votes, which we did not adjudicate to be foreign interference.

Mr. Dane Lloyd: Oh, you have not adjudicated that to be foreign interference.

Mr. Rob Stewart: No, we did not adjudicate individual ridings, and we did not adjudicate them to be foreign interference.

Mr. Dane Lloyd: Is the case now closed on that, or are you continuing to investigate that?

Mr. Rob Stewart: No, we're not continuing to investigate. We're obviously monitoring, in both public and national security institutions, the environment for—

Mr. Dane Lloyd: Are there any lessons that you learned from that?

The Chair: We're out of time.

Mr. Dane Lloyd: Okay. Thank you.

The Chair: I'm glad we were able to clarify at the end exactly what was said so that there was no misinterpretation of what the evidence might have said to us all.

Now I will call upon Mr. Noormohamed.

I think you're with us virtually, sir. You have six minutes from whenever you take the floor.

Mr. Taleeb Noormohamed (Vancouver Granville, Lib.): Thank you, Mr. Chair.

Thank you, Minister and Deputy, for being with us today.

I'm very pleased that my colleague Mr. Lloyd led off with the question about cybersecurity, at least at the outset of his question, because I think it's important for Canadians to hear directly from you, Minister, about the preparation we have for our critical infrastructure, our grid, our water supply and so on and so forth in respect of potential cyber-effects.

Can you share with us a little of your view as Minister of Emergency Preparedness around how prepared we are and the type of work being done by your department and others to ensure that Canadians can feel assured that the power supply, water and other critical infrastructure will indeed be in a position to withstand potential cyber-attacks that may affect computer and other systems that regulate that infrastructure?

Hon. Bill Blair: Thank you very much. It's a very important question, Mr. Noormohamed.

First of all, I've had a number of discussions with, for example, the Communications Security Establishment, which is the federal department that primarily has responsibility for ensuring the protection of our government systems. I am assured that the world that we sometimes would define as the "gc.ca" data environment is very robust in its resiliency and security. There's been significant work done by CSE and all of government in order to make sure that those systems are well protected.

We're also working very closely with the provinces and territories, as well as municipalities and the private sector. Critical infrastructure is quite diverse and spread across the country, and is often under the purview, authority and responsibility of the provinces, territories, and in many cases municipal and even private sector interests.

I will tell you that I believe there's a strong level of resiliency and strength within the financial sector and with other certain areas of critical infrastructure, but we have seen quite recently cyber-attacks that are directed towards critical infrastructure in the United States, for example, with pipelines. In this country we've seen similar attacks, sometimes taking the form of ransomware attacks, which are not necessarily foreign interference but rather criminal attacks on systems that are directed towards health care data, for example, in one of our provinces. We've seen attacks on municipal transportation networks, which also form part of our critical infrastructure.

It's an important part of the work that both CSE and CSIS and our government are doing, working with our provincial and territorial partners and with private industry in order to go out and provide them with support and information to help them become better prepared in the face of these types of attacks, and also developing supports. We provide that support to our provincial, territorial and private sector partners when they are subject to these types of attacks. Our government goes in and provides expert assistance to help them recover.

• (1115)

Mr. Taleeb Noormohamed: Thank you, Minister.

Deputy Minister, you cover a very large remit. You have a lot, indeed, to be worried about. I want to make sure you understand that the question I'm asking you now is not at all intended to be a political question, but one for a public servant whose service we value. I would very much like you, as a public servant, to give us an answer from the perspective of the public service.

One thing that this committee has looked at in great detail is misinformation. We have looked at the way in which the voices of the far right, the conspiracy theorists, etc., have been amplified by Russians in order to sow discontent, to foment discord and frankly to destabilize Canadian society. As a public servant with purview over our national security and public safety establishment and our preparedness establishment, how concerned are you about this? Can you share with us some of the things you are doing to buffer and to prepare our institutions against these concerns and potential risks?

Mr. Rob Stewart: As a starting point, I will say that we are constantly trying to monitor and improve our ability to monitor the risks associated with mis-, dis- and mal-information. There is an institution in the Global Affairs portfolio called the rapid response mechanism, which was agreed to by the G7 and was tasked with the monitoring of media and social media for this kind of threat. It works in concert, obviously, with allies.

Inside the national security community and in the policing community, we are also doing the same thing. We are obviously concerned about the risks that mis-, dis- and mal-information pose to Canadians and to the stability of our democracy. We feel that this is

an area in which we have to spend a lot of time and a lot of effort. That is certainly something we are doing.

Mr. Taleeb Noormohamed: Thank you.

Minister, I'll go back to you.

As a British Columbian, I would be remiss if I didn't take this opportunity to, first of all, thank you for your visit to B.C. recently and to ask you this as we head towards summer and hopefully not another forest fire season.

We've seen terrible devastation of infrastructure in British Columbia over the course of the last year or so and responses from all levels of government to address it. With the experience of the last couple of years, how prepared do you feel we are as a province and how prepared do you feel the federal government is to be able to respond to risks that are likely to find their way to British Columbia again through the forest fire season this summer and beyond?

Hon. Bill Blair: I will tell you that we work very closely with Emergency Management B.C. on its firefighter response. After a number of years of experience in working with them, I will tell you that they are quite expert at this and provide a very robust response; however, as a result of the fires that we've seen over the past few years—

• (1120)

The Chair: I'm sorry, Minister; you have 10 seconds, please.

Hon. Bill Blair: We're investing a lot of money in training additional firefighters and providing additional equipment. We're also investing pretty significantly in a new wildfire detection satellite system. Although we have a robust response, we know it needs to be better.

By the way, we're including traditional indigenous knowledge and greater engagement with aboriginal communities in that response.

The Chair: Thank you very much.

I now invite Ms. Michaud to begin her six-minute slot.

The floor is yours.

[*Translation*]

Ms. Kristina Michaud (Avignon—La Mitis—Matane—Matapédia, BQ): Thank you, Mr. Chair.

Thank you, minister, for being with us today. Welcome back to the committee.

I also thank you, Mr. Stewart, for being with us.

Minister, in your opening remarks, you mentioned the economic sanctions imposed on Russia by Canada, in an attempt to isolate Russia after the invasion of Ukraine. We are studying the situation in committee. The Standing Committee on National Defence is also looking at it. Since the situation fluctuates considerably, it is difficult to anticipate. In the same way, we did not anticipate the invasion of Ukraine at all.

Do you think that Canada could be adversely affected in the short to medium term because of these economic sanctions?

Are you preparing for it and, if so, how?

[English]

Hon. Bill Blair: That is a very important question. When we imposed these sanctions, we looked very carefully at whether we were vulnerable to reciprocal actions on the part of Russia.

Canada does not use Russia as a particularly significant trading partner, but there were some impacts. For example, a very significant impact is that Russia is a source of much of the nitrogen fertilizer essential to Canadian agriculture and farmers across this country. The sanctions that were imposed had an impact on the availability and the cost of that much-needed fertilizer. I know this is an issue that Agriculture Canada is very much seized with and is working on in order to provide support and assistance to our farmers impacted by that measure.

We're obviously seeing, as a result of the sanctions—not just imposed by Canada, but imposed globally, particularly among Europeans—a very significant impact on supply chains and, in particular, around energy products such as petroleum and liquid natural gas. The impact is most severely felt in Europe, but it's having a reciprocal impact here. We're seeing impacts on the supply chains here and in the cost of gasoline for Canadian consumers.

Those are all issues of significant concern to this committee and to all Canadians, that we all, unfortunately, have to pay a bit of a price for our response to Russia's illegal invasion of Ukraine, but our support for the people of Ukraine is unwavering and we have joined a global effort in order to respond with these sanctions.

I believe that the sanctions are quite impactful on Russia. They are often motivated by the profits they make from their trade, in particular in gasoline and liquid natural gas. Those sanctions, I believe, will have a detrimental effect on them.

[Translation]

Ms. Kristina Michaud: When it comes to security and cyber security, do you have any concerns?

In Quebec, for example, critical infrastructure has been targeted for several months now. This happened to Hydro-Québec and certain aluminum smelters, which were attacked by Russian hackers.

You said you are working with provinces, municipalities and the private sector. How are you working with them to ensure that our critical infrastructure is protected?

How can you prevent these kinds of attacks? They've happened before, and it's likely that they'll get worse over time.

[English]

Hon. Bill Blair: First of all, our strategy, as I've already mentioned, involved the creation of a number of federal agencies and bodies, including the national cybercrime coordination unit under the RCMP, responsible for conducting criminal investigations. Very importantly, we know that cybercrime events can impact our provincial and territorial partners and our critical infrastructure. We're delivering programs that are focused on industrial control systems for critical infrastructure.

We've been working very closely with stakeholders in providing training, testing response and recovery capabilities and promoting security awareness. Just a few weeks ago, a multisector network meeting was held with critical infrastructure stakeholders, including our provincial and territorial partners, to discuss threats and mitigation measures. In our budget 2022, funding of nearly \$700 million is provided over five years to support how we fight cybercrime and defend critical government and private sector systems, including for our provincial and territorial partners, in order to improve and increase our collective resilience in these types of attacks.

• (1125)

[Translation]

Ms. Kristina Michaud: Thank you, minister.

In our study, experts told us that Canada wouldn't have the tools to fight hackers effectively until 2023. That would be because we didn't start addressing this problem 15 years earlier, as the Americans and Europeans did. We may not get it done. We won't have the system needed to deal with the situation properly.

What government strategy have you established to make sure you have the tools you need to fight computer attacks, such as ransomware? There are many tactics and many terms to describe them.

In your opinion, is Canada falling behind other countries?

How will the country be able to catch up, if at all?

[English]

Hon. Bill Blair: First of all, let me provide you with some assurance that we work very closely, particularly with our Five Eyes partners, and it's not just a government-to-government relationship. In fact, among our senior officials, and particularly among the members of the national security intelligence community within Canada and among our Five Eyes partners, there's a great deal of collaboration and working together on the sharing of tools and responses to improve our resiliency.

Some of the questions you ask, I believe, would be more appropriately answered by the Communications Security Establishment and perhaps the Minister of Defence. However, I work very closely with them—both I and the deputy minister do—and I can provide you with assurances that I believe the CSE and our officials have been incredibly vigilant and vigorous in their response to cyber-attacks. There is a high degree of expertise. When we have had cyber-attacks among our provincial and territorial partners that have affected critical infrastructure systems there, we've been able to respond very quickly to send the expertise there, help them in their recovery and provide them with a great deal of support and advice.

Although there's always work to do, I would acknowledge that they're doing a pretty good job.

The Chair: That's a lot of thank yous.

Now, for the last person in the first round of questions, I invite Mr. MacGregor to begin his six-minute slot.

Mr. Alistair MacGregor (Cowichan—Malahat—Langford, NDP): Thank you, Mr. Chair.

Thank you, Minister Blair, for coming before our committee.

Canada and Russia of course have the longest coastlines in the Arctic Ocean, and we know about climate change and its effect on the Arctic and the retreating sea ice. That retreating sea ice creates a vicious circle, because the more ice we lose in that ocean, the worse the climate change effects will be.

I guess one of the worrisome consequences of the war in Ukraine is that we see incredibly antagonistic attitudes from our Russian counterparts in a vitally important ocean. I'm wondering about this from your perspective, Minister. In spite of the war that's going on and the antagonistic relations between our governments, there is still a great need for co-operation between our two countries with respect to climate change, given the fact that we share coastlines in the Arctic Ocean and we both stand to lose a lot with the melting of the permafrost.

Could you update the committee on what the status of co-operation is between our respective scientific communities with respect to research and science in climate change? Is there still the possibility of any kind of co-operation in addressing this very real and most dire threat in the 21st century?

Hon. Bill Blair: It is a very important question, Mr. MacGregor.

Let me acknowledge that the illegal invasion of Ukraine by Russia has impacted a number of diplomatic discussions and efforts. I was most recently at a UN platform on disaster risk reduction, and I can tell you from experience that the Russians' illegal invasion of Ukraine directly impacted some of those discussions.

However, and I think it's an important however, you highlight some very significant issues with respect to climate change, Arctic sovereignty, and our shared responsibility with all of those who have an interest in the Arctic, to take collective and coordinated action in response to some of the risks that exist, particularly as they relate to climate change in the Arctic.

I believe, notwithstanding the obvious and understandable impact on some of our diplomatic discussions, the important work of

ensuring that the right thing is done in the Arctic will continue. We'll assess the impact of Russia's illegal actions as it impacts on those discussions. That work is ongoing. That is not directly by me, by the way, but by Global Affairs and the Canadian military and others, in addition to our other international partners. There are important forums where those discussions will continue.

• (1130)

Mr. Alistair MacGregor: In the context of emergency preparedness, we know that in an increasingly globalized world, and with climate change, we as a human population are being exposed to more and more novel diseases. They, of course, are mutating. I think the next pandemic is something that we have to keep top of mind.

In our response to COVID-19, as a country, we were having to fight a rearguard action against disinformation and misinformation on vaccines. To some extent, I think that hampered how successful we could have been.

We know that foreign state actors have played a role in advocating some of those disinformation campaigns. We've heard that evidence here at this committee. Looking forward to the next pandemic, when it comes, what lessons have you learned as the Minister of Emergency Preparedness?

In your opening remarks, you said that your mandate is all about taking that proactive approach to managing risks. What lessons have you learned about trying to prevent foreign state actors from interfering and causing those misinformation campaigns, which may very greatly hamper our public health efforts in Canada?

Hon. Bill Blair: Thank you for a very important question.

I've just come from a meeting of the COVID committee, where we had a presentation on this very subject with the chief medical officer of health. There is a robust discussion going on in Canada about how we counter misinformation and provide Canadians with accurate, data-based evidence on the nature of disease and pandemics and risk, and how we put better data surveillance systems in place and have greater collaboration internationally. It's also important that information be trusted, and I think that's the point.

I agree with you that what we have seen, not just in Canada but around the world, is the importance of providing, for Canadians in particular, information they can trust and will trust with respect to the steps they should take in order to keep themselves safe. There has been a real challenge, with misinformation primarily, and disinformation, which is slightly different, obviously, and has perhaps a more nefarious intent. Certainly misinformation has resulted in some significant challenges in how we move forward.

The obligation of government is to make sure that we have robust data collection systems that are transparent, so that Canadians can see the basis of the scientific advice and evidence that we're acting upon and that is being shared with them. They can then make informed decisions in their best interests and in the collective interest of everyone's health.

We've learned a lot of lessons from COVID, and one thing we learned is that our strategic stockpiles were not adequate to the task. With a lot of our data collection and information that we were relying on with respect to the nature of COVID as a disease, but also generally to disease and pandemic threats, we're seeing the emergence of a number of variants and illnesses coming forward. It's very important that we get good information to enable Canadians to make good decisions.

The Chair: Thank you very much.

Colleagues, I look at the clock and we have exactly enough time for a full second round of questions.

Ms. Dancho, we will lead with you. You have a five-minute slot.

The floor is yours, whenever you grab it.

Ms. Raquel Dancho (Kildonan—St. Paul, CPC): Thank you, Mr. Chair, and thank you, Minister, for being with us today.

I'd like to carry on with the theme of cybersecurity.

I recently received a briefing from the public safety department concerning cybersecurity. When I asked, very bluntly, what the Pearl Harbor moment would be in terms of a cybersecurity attack, they mentioned pipelines in the middle of winter—presumably, gas pipelines. As you know, these provide significant heat to our homes, hospitals, grocery stores, government buildings and schools.

Would you agree this would constitute a major emergency—a cyber-attack on a pipeline in the middle of winter in Canada?

Hon. Bill Blair: Yes, of course I would, Ms. Dancho. Supply lines are a very important part of critical infrastructure—all of our supply chains. I would consider any interference with those supply chains to be a significant emergency, rising to the level of a national emergency.

Ms. Raquel Dancho: What would your first call be? You get a call about this happening: A pipeline has gone down in the middle of winter and millions of people are without heat. What would your first step be?

Hon. Bill Blair: A couple of things would have to happen very quickly. If it was related to a cyber-attack, my first call would be to CSE. I'd call the director at CSE and get her working on it right away. They have the expertise within our government. Many of those pipelines, by the way, are administered by the private sector, but we've already built those relationships. We've already made those connections. We're meeting regularly with those people.

We would build upon that in order to get them back online as quickly as possible, but there would be other considerations, because, very quickly, the absence of those pipelines would have an impact further downstream on refineries. It also wouldn't take long for it to begin to impact heating and other energy requirements for

Canadians. We would look for alternative ways to deliver those products, as quickly as possible. There would be a number of responses triggered immediately.

• (1135)

Ms. Raquel Dancho: I'm sure you're very familiar with the Colonial pipeline ransomware attack a year ago last month, which shut down a significant source of energy for the United States. There were 17 states of emergency, including in Washington, D.C., and it took several hours to get them back online. That was less than a day, but if it had been longer, in the middle of winter in Canada, you can imagine, as you've mentioned, it would be very serious.

What sort of elements would you pull in? Would you be calling the military or the RCMP? What would that look like on the ground, and what sorts of conversations have you had with your cabinet colleagues in preparation for a worst-case scenario?

Hon. Bill Blair: As far as resources go, we would call anything that was required—everything that was required. As we've demonstrated over the past two years, we understand the importance of moving quickly in order to respond to requests for assistance from the provinces, territories or private sector, or even to respond to something we would consider a national emergency...so the resources that are appropriate.

If it was, for example, a cyber-attack—perhaps a ransomware attack, as it was with the Colonial pipeline—certainly, the police would have to become involved immediately.

Ms. Raquel Dancho: What if it were a physical attack? As you know, we recently saw the Coastal GasLink attack: 20 armed assailants with axes. They caused millions of dollars' worth of damage on the Coastal GasLink. I'm sure you're very familiar with this. We are seeing a rise in violence against our pipeline infrastructure.

Are you concerned there could be a physical attack or, God forbid, a bombing of our infrastructure? How would you handle that?

Hon. Bill Blair: The police of jurisdiction have responsibility for that. They respond in the first instance and, when the situation exceeds the capacity of the police of jurisdiction, there are mechanisms to elevate that request to bring in resources from wherever they are required. Those are reciprocal arrangements in place with the police and managed very ably by the RCMP.

Ms. Raquel Dancho: Since the event in, I believe, February, have you had discussions about emergency preparedness should there be a physical attack from these extremists on our pipeline infrastructure?

Hon. Bill Blair: We have not, specifically, because it did not rise to the level of exceeding the capacity of the police of jurisdiction to respond.

Ms. Raquel Dancho: You've had no conversations in terms of how you would handle it, should this increase in severity.

Hon. Bill Blair: We have processes in place should it rise to a threshold that exceeds the capacity of the local police of jurisdiction to manage. Those processes are well established and well understood right across the country, but we have not had an event that required it, up to this point.

Ms. Raquel Dancho: Are you concerned that Canada could be subjected to more attack events on our pipeline infrastructure?

Hon. Bill Blair: I'm always concerned about the security and integrity of all our critical infrastructure, and we work hard to be prepared.

Ms. Raquel Dancho: Are you concerned that none of the assailants from the Coastal GasLink pipeline attack have been caught?

Hon. Bill Blair: Again, as minister, I'm not going to comment on any ongoing investigation. That would be entirely inappropriate. I have confidence in our police agencies, and particularly in the RCMP, to do their work.

Ms. Raquel Dancho: I asked because I can see you take this very seriously, as the Minister of Emergency Preparedness. I have concerns that the assailants have not been caught. That sets a precedent for copycats. "They got away with it; maybe we can, too." I would ask that you have more discussions with your cabinet colleagues to ensure these individuals are held accountable.

Thank you, Minister.

The Chair: That is perfect timing.

I will now turn to Mr. McKinnon for five minutes of questioning.

Mr. McKinnon, go ahead whenever you're ready, sir.

Mr. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.): Thank you, Mr. Chair.

Thank you, Minister, for joining us today. It's always a pleasure, and it's good to hear the breadth and scope of what you're working on.

I know you're working a lot on natural disasters—forest fires, earthquakes and stuff—but in the context of our study on the security implications of what's going on in Ukraine with Russia and so forth, we've talked about cyber; we've talked about the economic blowback from sanctions; we've talked about the possible harm to international agreements, and so forth.

I'd like to hear from you on what you see as the greatest threats that Canada faces in regard to this situation.

Hon. Bill Blair: There are a number of things that we're monitoring very carefully and out of an abundance of caution. That's the approach I like to bring to it, to provide that abundance of caution and care to ensure the health and safety of all Canadians.

Because of our distance from the conflict in Ukraine, probably the most significant threat that Canada would face from this would be cyber-related, but having said that, we take an all-hazards approach, and we're monitoring the situation very carefully.

I also would comment that there are 1.4 million Ukrainian Canadians who have a very strong interest, and they have family and perhaps business interests, and at the very least they love their

mother country. I think we also have a duty to them to be particularly vigilant in order to make sure they are not subject not just to undue influence, but to any kind of interference or threat.

Sometimes we see, for example, that when they advocate for Ukraine, the response on social media can be very challenging for them, particularly for certain vulnerable members of that community, so we remain vigilant in our support of Ukrainian Canadians, as well as protecting Canadian critical infrastructure and interests.

• (1140)

Mr. Ron McKinnon: Thank you, Minister.

I'll segue from there to individual Canadians.

What can we do? This threat from Russia is somewhat distant in some respects, but it's also very close to home in many other respects. What can ordinary citizens do? What should they be doing to take prudent precautions to prepare themselves for the future in relation to this conflict?

Hon. Bill Blair: I always remind myself that in any kind of emergency, the first response is always the public. The more information we can provide to the public about potential threats and risks, I think the better Canadians can respond to protect their interests.

For example, I think we can help Canadians to be alert to the possible impact of misinformation and disinformation, so they can perhaps make better-informed decisions and not be inappropriately influenced by information that is intended to cause them to react in a certain way. I think we have a responsibility to do that.

Let's also acknowledge, Mr. McKinnon, that Canadians are feeling the impact of the sanctions on Russia. We're seeing it at the gas pumps, and our farmers are experiencing it in the acquisition of the fertilizer they need. We're seeing real impacts from the sanctions and from the conflict in Ukraine.

Perhaps no one is experiencing the impacts of that more than Ukrainian Canadians here in this country.

We all have to remain alert and vigilant and supportive of those who are being impacted in a particularly difficult way by all of the outcomes of the invasion of Ukraine.

Mr. Ron McKinnon: I have one last question.

I was interested to hear your discussion of upgrading the federal emergency response plan. I wonder if you could speak to us more about that. Where does it need to be upgraded, and what kind of time frame are we looking at for that?

Hon. Bill Blair: I was previously, as you'll know, the Minister of Public Safety and Emergency Preparedness. We've learned lessons from the impact of the pandemic, but also by what we are witnessing in this country with an increase in the frequency and severity of climate-related natural disasters. We've seen it with heat domes in British Columbia and very significant floods last fall, and then again this spring. We've seen a very challenging wildfire season, and of course concerns about pandemics and disease are accelerating. It requires that we keep up with the times.

I believe, in the business of emergency preparation and preparedness, if we maintain the status quo we fall behind, because the situation is actually accelerating and getting more difficult. It requires, through the federal emergency response plan and all the ancillary work that goes on around that, that we continue to build upon our ability to create greater resilience and awareness of the impact of these types of events.

The Chair: I turn to Ms. Michaud for two and a half minutes of questioning.

Please go ahead.

[Translation]

Ms. Kristina Michaud: Thank you, Mr. Chair.

Minister, I'm going to ask you a question that Mr. Stewart can elaborate on, if necessary.

We know that Russia is using the concept of hybrid warfare to destabilize certain countries. Experts believe that it may have contributed to the trucker convoy phenomenon. We know that there were foreign interference and funding, namely from the United States.

Based on the information you have gathered, was there Russian involvement in the trucker convoy?

If so, how did this take place?

[English]

Hon. Bill Blair: If I may begin, I saw you were trying to direct that to the deputy, and I'll turn it over to him for a second.

I will tell you that I've received no information and no intelligence that indicates that Russia was involved in any activity related to the protests, convoys and blockades.

• (1145)

Mr. Rob Stewart: That's right.

[Translation]

Ms. Kristina Michaud: Thank you very much.

Do you have any other examples of groups in Canada incited by Russia to get involved in politics? We were concerned that such groups were actively interfering in our institutions' affairs and our democracy.

Do you have any concerns about other groups in terms of disinformation and cyber security?

[English]

Hon. Bill Blair: I can tell you that a number of the entities that we have recently listed as terrorist organizations have origins in Russia. That doesn't necessarily reflect the activities of the state, so I would differentiate between hostile activities of a state actor, such as Russia, and activities that originate in Russia that are primarily criminally based.

[Translation]

Ms. Kristina Michaud: I imagine you agree with that.

Recently in the House, we voted in favour of a motion requiring that your government develop a strategy, based on the Australian model, to fight foreign interference.

Can you tell us if, since the adoption of this motion, anything has been done in this regard?

Do you intend to put in place a plan to counter foreign interference soon?

[English]

Hon. Bill Blair: Yes. I don't want to get too far ahead of that work, but, in response to that, I can tell you that our government is very much engaged on a number of different fronts at looking at how we can better manage and protect Canada and create greater resiliency against foreign interference. Part of that is on the basis of the cyber world. Part of it is concerning information, misinformation and disinformation. Some of that work is also the responsibility of our national security intelligence agencies.

The Chair: Thank you, Minister.

We'll move to Mr. MacGregor for two and a half minutes.

Mr. Alistair MacGregor: Minister, on Monday, your colleague, Minister Mendicino, introduced Bill C-21, and while a lot of the attention on that bill has been focused on the national handgun freeze, there are also some significant amendments within it to the Nuclear Safety and Control Act, for people who operate high-security sites. These are sites where you have category I or II nuclear materials, which are basically our nuclear power plants. If this bill goes through, the amendments to that act are going to require those sites to have an on-site nuclear response force that is composed of nuclear security officers, designated as peace officers, who will be proficient in all manner of firearms.

I guess that in your role as Minister of Emergency Preparedness, you have to try to proactively manage risks. Minister, have there been any instances in Canada that have prompted this amendment to the legislation? Did you find that there was a serious gap in the physical security of our sites? Were there any risks manifested that prompted this amendment?

Hon. Bill Blair: If you don't mind, I'll rely on my previous experience as a police chief in Toronto. We have a nuclear plant nearby, and there was an established.... Initially, the policing and security of that was being provided by the police of jurisdiction, but they formed their own security services.

There has been significant work done on potential risk assessments of those facilities, and I am very much of the belief that it is necessary that we have a robust and properly equipped security response in order to protect those types of facilities because of their criticality and the potential risk involved. They are already able to provide the type of armed response that you describe. We're just building it within the act so that they'll be able to continue in light of the prohibitions that we've put in place.

Mr. Alistair MacGregor: I'm guessing the danger from a foreign state actor that might trigger article 5 of NATO would be relatively low, so are the risks more on the cyber front than on the physical front?

Hon. Bill Blair: Frankly, both are risks. It is possible that it could be a hostile state actor. It's also a site that could potentially be targeted by others—terrorists or other types of criminal intent. Therefore, it is necessary for the protection of citizens. There are risks associated with nuclear facilities, and those risks have to be properly mitigated by appropriately equipped security services.

The Chair: Thank you, Minister.

Now I will turn to Mr. Van Popta for five minutes.

• (1150)

Mr. Tako Van Popta (Langley—Aldergrove, CPC): Thank you, Mr. Chairman.

Thank you, Minister, for being here, and also thank you to the deputy minister.

I have a question about Canada's infrastructure, or perhaps international infrastructure, and how Canada's vulnerability might play into that.

I was reading in a BBC publication from about a year ago that a Russian ship carrying submarines was tracked sailing around the British Isles. It was likely mapping the locations of underwater cables and optic fibres, which are the world's information superhighway.

Is that a threat to Canada? Are we prepared for something like that?

Hon. Bill Blair: Frankly, any effort by a hostile state actor to gain access or to in any way interfere with our information systems.... I will tell you that information and communication technology is one of our critical infrastructure sectors, so ensuring the security and integrity of those systems is an issue of national concern. Yes, we would be concerned by such activity, and certainly we would be vigilant against it.

Mr. Tako Van Popta: Of course we'd be concerned and of course we'd react to it, but is there risk mitigation? Would we have a plan B if something like that were to happen?

Hon. Bill Blair: Again, that's a question perhaps better put to the ministers responsible for that.

By the way, there are 10 sectors of critical infrastructure in this country. Each one of them is the responsibility of a particular minister. In addition, every one of those ministers is responsible for developing an emergency response plan, which includes mitigation and prevention measures. That forms part of the federal emergency response plan.

I don't have the particulars in front of me, unfortunately, of that plan, but it does form part of our overall federal emergency response plan.

Mr. Tako Van Popta: Good. Thank you.

I have a question about the North Warning System and NORAD, which is a partnership we have with the United States of America.

We had witnesses appear before this committee telling us that the infrastructure and the technology are woefully out of date and need to be upgraded. The infrastructure is designed to track a bomber, for example, coming over the North Pole to North America, but it is not designed for hypersonic missiles today.

I know it's a national defence issue as well, but in your department is this a matter of concern at all?

Hon. Bill Blair: Yes, of course, and of course we've had discussions.

As you quite correctly pointed out, national defence is responsible for that. I know the Minister of Defence has, within her mandate provided by the Prime Minister, a responsibility for the renewal of NORAD. You're right that the system as it was designed many years ago was to deal primarily with airplane incursion into Canadian airspace. Now there is an evolving series of threats, including, obviously, hypersonic missiles. That renewal is part of that responsibility.

I'm aware of that work, but questions with respect to its progress are better put to the Minister of Defence.

Mr. Tako Van Popta: I understand that. I respect that.

Deputy Minister, do you have anything to add to that?

Mr. Rob Stewart: Yes, indeed, I could add to that.

Underneath the federal emergency response plan that is under the responsibility of Minister Blair, we have a layered set of plans, including those for events such as attacks. In the realm of emergency preparedness, they are to deal with warning, early response, coordination and early recovery.

It's not about defence as much as it is about managing what would happen on the ground. That's a shared responsibility with the provinces and territories, so we have a very joined-up system of response in the event of a certain set of scenarios.

Mr. Tako Van Popta: Thank you.

I'll pass on my time.

The Chair: Thank you.

We will turn for the last slice to Mr. Chiang.

Mr. Paul Chiang (Markham—Unionville, Lib.): Thank you, Mr. Chair.

I'd like to thank the minister and the deputy minister for joining us today for this important discussion about our national security.

Minister, in March you chaired an incident response group meeting discussing Russia's ongoing violation of international law and military aggression towards Ukraine.

Could you provide an update to this committee on the work that is being done within your department to address these serious issues?

• (1155)

Hon. Bill Blair: Let me also characterize that work as a whole-of-government response, certainly as it pertained to discussions around the sanctions that Canada has imposed, and that has been largely led by our Minister of Foreign Affairs. With respect to the support that we've been able to provide to the Ukrainian military, again these are questions more appropriately, I think, put to the Minister of Defence.

What we have learned about our response to emergencies of all kinds in this country is that they are not siloed into one ministry. One of my responsibilities in chairing that committee, for example, is to bring about a greater collaboration and coordination among all of the ministries so that we can all work more collaboratively together. There's also a responsibility to work very closely with our partners, both internationally and domestically, and with the provinces and territories.

For example, we have a table of senior officials responsible for emergency management, who also work very closely together to bring collaboration between the provinces, territories and ourselves. I think some really important work is also going on with both the private sector and with indigenous communities to bring that level of collaboration. That's really the responsibility that my department has in ensuring that we all work really well together and that nothing falls through the cracks.

Mr. Paul Chiang: Thank you, Minister.

I understand we've been talking about cybersecurity or cyber-attacks, but due to the war in Ukraine, has Canada stepped up to high alert for cyber-attacks from Russia or any other nation?

Hon. Bill Blair: I can acknowledge that there is a heightened vigilance currently in place, particularly with the Communications Security Establishment, the RCMP and CSIS, with respect to any form of interference, including cyber, that could take place in this country. We're working with our partners in the private sector as well. We have met with them and encouraged additional vigilance and better preparation on their part as well.

The work of building resilience into our critical cyber systems in this country is ongoing, because those who seek to attack it are innovative. They come up with a new way to attack us every day, so it requires just as much vigilance on our part to always be prepared to respond.

Mr. Paul Chiang: Thank you, Minister.

We know that together Russia and Ukraine account for about 29% of global wheat exports, and Ukraine is also a major exporter of corn. As the world becomes increasingly concerned about the global food emergency resulting from this war, what steps are you taking to ensure that Canada is adequately prepared to address these issues of food shortage?

Hon. Bill Blair: We're working on a couple of fronts. First of all, we are developing our own national strategy on securing supply chains in this country, because we recognize their importance not just for agricultural products and food products—although food security is a very important issue of course for us—but also with respect to energy and other essential supplies and trade corridors.

We are also recognizing that there's going to be a significant global impact—exactly as you described—and there are countries in the world that are heavily reliant on food products, particularly wheat, that traditionally come from Ukraine and Russia, all of which have been interrupted by the conflict that's currently taking place as a result of the illegal invasion of Ukraine by Russia. There is an impact globally.

I'm aware, because I've been involved at the table in discussions, of the efforts of Canadian agriculture in an effort to respond. I will tell you that although there's obviously an inflationary impact on food products as a direct result of that conflict, Canada is prepared to provide assurances of a secure food supply for this country. However, we are very concerned about the global impact that it's going to have, and there are other regions of the world that are particularly vulnerable to the impacts of that conflict.

Mr. Paul Chiang: Thank you very much, Minister.

Deputy Minister, would you have anything to add to this food shortage issue we have?

Mr. Rob Stewart: I would add only that this is an issue of global significance and concern, and it is in discussions in global fora around the world on food security.

Mr. Paul Chiang: In other words, it impacts everybody, not just Canada alone.

Mr. Rob Stewart: That's correct.

Mr. Paul Chiang: Thank you so much. That's it for my questions.

The Chair: Thank you very much.

Colleagues, on your behalf, I want to thank the minister and the deputy for sharing this hour with us. We can only imagine the intensity of the conversations that are happening, and you're ever alert. Every day offers a new challenge and a new vulnerability. We're very grateful that you have shared with us your best perspective and intelligence on the current state of play.

On behalf of members of the committee and, indeed, all parliamentarians, I thank you very much for your appearance in front of the committee today.

• (1200)

Hon. Bill Blair: Thank you, Mr. Chair and colleagues, for the opportunity to come and speak with you today.

The Chair: Colleagues, we have a short break and then we go in camera.

[Proceedings continue in camera]

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <https://www.ourcommons.ca>

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante :
<https://www.noscommunes.ca>