HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

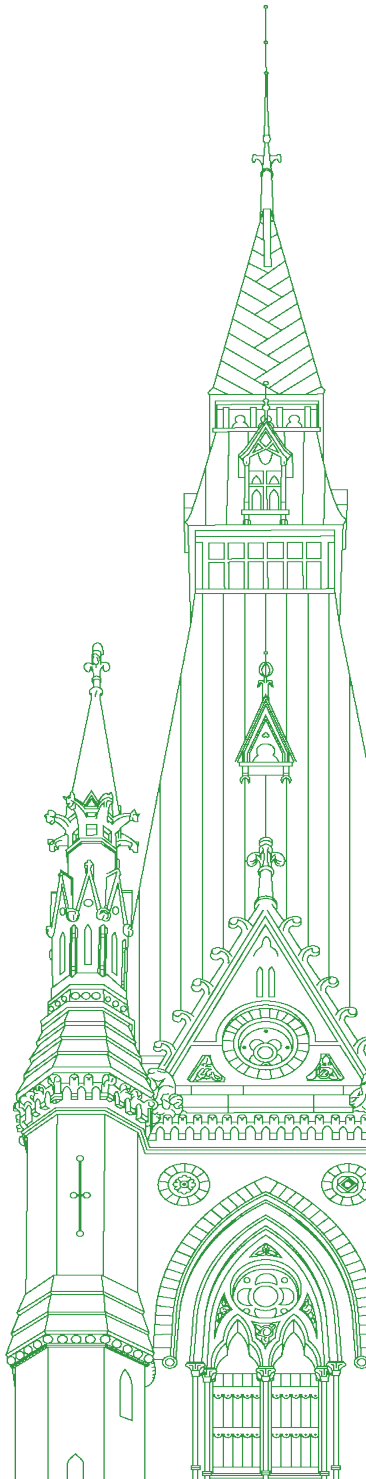
44th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 095

Thursday, February 15, 2024



Chair: Mr. Heath MacDonald

Standing Committee on Public Safety and National Security

Thursday, February 15, 2024

● (0815)

[*English*]

The Chair (Mr. Heath MacDonald (Malpeque, Lib.)): I call this meeting to order.

Welcome to meeting number 95 of the House of Commons Standing Committee on Public Safety and National Security.

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

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

Please wait until I recognize you by name before speaking.

To prevent disruptive audio feedback incidents during our meeting, we kindly ask that all participants keep their earpieces away from any microphone. Audio feedback incidents can seriously injure interpreters and disrupt our proceedings.

As a reminder, all comments should be addressed through the chair.

Pursuant to the order of reference of Monday, March 27, 2023, the committee resumes its study of Bill C-26, an act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other acts.

Appearing before us today are the Honourable Dominic LeBlanc, MP and Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs; and the Honourable François-Philippe Champagne, MP and Minister of Innovation, Science and Industry. Welcome.

Witnesses from the Department of Public Safety and Emergency Preparedness include Patrick Boucher, senior assistant deputy minister, national cyber security branch; Colin MacSween, director general, national cyber security directorate; and Kelly-Anne Gibson, acting director, national cyber security directorate.

Witnesses from the Department of Industry are Éric Dagenais, senior assistant deputy minister, spectrum and telecommunications sector; and Mark Schaan, senior assistant deputy minister, strategy and innovation policy sector.

Please note that the ministers will be with us for one hour and 30 minutes. The officials will stay for the rest of the meeting in order to answer questions from members.

Colleagues, we need about 10 to 15 minutes before the end of the meeting to deal with committee business items, such as budgets and the committee schedule.

Welcome to all.

I now invite Minister LeBlanc and Minister Champagne to make an opening statement of up to 10 minutes each.

Thank you.

Minister LeBlanc, will you start?

Hon. Dominic LeBlanc (Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs): I will with pleasure, Mr. Chair—with a lot of pleasure.

[*Translation*]

Thank you, Mr. Chair.

Thank you, colleagues, for inviting me to speak about Bill C-26, which pertains to cyber security.

I am pleased to be here with my colleague François Philippe Champagne and the other officials kindly named by the Chair.

[*English*]

Our critical infrastructure is becoming increasingly interconnected, interdependent and integrated with cyber systems. Canada's critical infrastructure plays a vital role in the delivery of essential services and the necessities of daily life. In order to safeguard our economic and national security, we need to take a more complete picture of the cybersecurity threats facing Canadians. We believe that Bill C-26 would be an important step in accomplishing that task.

This proposed legislation will protect Canadians and bolster cybersecurity across the federally regulated financial, telecommunications, energy and transportation sectors. These sectors are all critical contributors to both Canada's economy and the security of Canadians. Because of their vitality, they are also, obviously, attractive targets for malicious cyber-enabled activity, such as espionage, data and intellectual property theft, and of course sabotage itself.

These concerns are not just hypothetical. Recently the Canadian Centre for Cyber Security joined Five Eyes' operational partners in warning that People's Republic of China state-sponsored cyber-actors are seeking to pre-position themselves for disruptive or destructive cyber-attacks against the United States' critical infrastructure in the event of a major crisis or conflict with our neighbour to the south.

Cyber incidents are happening in our critical infrastructure sectors on almost a daily basis. In January 2023, CBC News reported that a territorial and Crown corporation, and the sole energy distributor in Nunavut, fell victim to a cyber-attack. In June of last year, the Calgary Herald reported that Canadian energy company Suncor suffered a serious cyber incident that shut down debit and credit processing at Petro-Canada gas stations across the country. We all remember the cyber incidents that paralyzed the Newfoundland and Labrador health care system in 2021.

Bill C-26 would help to defend our critical infrastructure and the essential services that Canadians and Canadian businesses rely on every day. This new act would increase collaboration and information sharing between industry and government and would require designated operators to report cybersecurity incidents to the Communications Security Establishment, which, as colleagues know, is an agency within the Department of National Defence.

By improving the government's awareness of the cyber-threat landscape in these critical, federally regulated sectors, we can warn operators of potential threats and vulnerabilities so they can take action to protect their systems and to protect Canadians as well.

● (0820)

[*Translation*]

However, the government can't do it alone. That's why we're committed to working closely with our industry partners, through the formal regulatory process, to create a clear, consistent and harmonized regulatory regime across all provinces and territories.

[*English*]

We must and we will work alongside our allies, in particular the United States, to make sure that our interconnected critical infrastructure is protected.

This legislation is consistent with the cybersecurity approaches of our allies, and we have been engaging with international partners to identify opportunities for further collaboration. As recently as Tuesday of this week I participated in a Five Eyes ministerial call, during which Secretary Mayorkas, the U.S. Homeland Security secretary, raised many of the issues we're going to talk about this morning.

[*Translation*]

We found that stakeholders broadly support the intent of the bill and agree that we must work together to protect our critical infrastructure from cyber threats. However, some expressed concerns about certain aspects of the bill. We have, of course, listened carefully to the points raised by our colleagues in the House of Commons and others concerning transparency, accountability and the protection of Canadians' privacy.

Fundamentally, this bill will help protect the privacy of Canadians' personal information. Canada's critical infrastructure systems, while secure, are not impenetrable. By requiring Canada's critical infrastructure operators to maintain high levels of cyber security, we are also reducing the likelihood of personal data breaches on their systems.

I look forward to working with you, Mr. Chair, and Committee members, on all these issues. Of course, if the Committee deems it necessary, we are prepared to consider amendments that could strengthen the bill. In addition, we look forward to working with you to ensure that this bill is passed and that Canada remains a safe, competitive and connected country in a more secure environment.

Thank you.

I look forward to hearing what my colleague Mr. Champagne has to say—which is why I'm here this morning—and to answering questions from Committee members.

● (0825)

[*English*]

The Chair: Thank you.

Mr. Champagne, go ahead, please.

[*Translation*]

Hon. François-Philippe Champagne (Minister of Innovation, Science and Industry): Thank you, Mr. Chair.

It is a great privilege to appear before you today. It's been over eight years since I had the privilege of becoming a Member of Parliament and testifying before committees. This morning is particularly important, especially as I have the privilege of testifying with Minister LeBlanc. For the people watching us, Canadians from across the country, it demonstrates the significance of the issue.

We should first ask ourselves why we are here this morning. Minister LeBlanc outlined the reasons. People should be reassured to see Minister LeBlanc, and his department, working in concert with the Department of Industry on an issue that affects not only all Canadians, but Canadian businesses across the country.

The issue of cyber security affects our small and medium-sized enterprises, or SMEs, families, all institutions across the country and even internationally. I can tell you that in the various international forums I've attended, the issue of cybersecurity is of paramount importance, especially when you add in everything to do with quantum technologies and artificial intelligence. That's why I'm proud to testify today with Minister LeBlanc, a great friend who also sees the importance of our two teams working hand in hand to accomplish this today.

As I was saying, I'm pleased to be able to discuss a legislative text of paramount importance with you, dear colleagues. People across the country expect us to respond quickly to a situation that is evolving just as quickly.

One of the most important things we can do as legislators is to protect our critical infrastructure across the country.

[*English*]

As Minister of Innovation, Science and Industry, I take a particular interest in securing Canada's telecommunications system. Telecommunications networks are vital to the safety, prosperity and well-being of Canadians. When you've seen disasters striking around the nation, citizens expect their telecom networks to work. That's why adding, as we would be doing in this law, the concept of security as an objective under the Telecommunications Act is so crucial. It's not only about cybersecurity, but it's about protecting Canadians in the times they need it most. That's why we are committed to protecting the telecommunications system that underpins much of our critical infrastructure in the country.

Take the emergence of new technologies, such as 5G, as one clear reason we need to redouble that focus. As you know, 5G is going to have a network that is far more decentralized. You're talking about the Internet of things, you're talking about connecting almost everything. The object will become intelligent and connected. If you think about the impact of cybersecurity you'll understand the size of the problem, and not only the emergency powers we need but also the duty to act we all have as parliamentarians.

[*Translation*]

The threats targeting these technologies and systems are increasing in number. I'm talking, among other things, about threats to our supply chains and cyber security threats from state and non-state actors, of course.

With these threats in mind, the government undertook a thorough review of 5G technology. In fact, I'd like to thank all the Ministry of Industry officials and the Ministry of Public Safety and Emergency Preparedness officials who are here today. They carried out extensive consultations with stakeholders across the country.

We carefully examined the issue from a technical and economic standpoint, as my colleague Minister LeBlanc said, as well as from a national security standpoint.

[*English*]

It is clear that while this technology will bring significant benefits, it will also introduce new security concerns that malicious actors could exploit, as 5G networks are more interconnected than ever. Therefore, threats will have a more significant impact on the safety and security of Canadians, including our critical infrastructures, than in previous network generations.

It is in light of this security examination that the Government of Canada found serious concerns about suppliers such as Huawei and ZTE. You will recall that in May 2022 we announced the intention to prohibit Canadian telecommunications service providers from using Huawei and ZTE products and services in their 5G and 4G networks.

● (0830)

[*Translation*]

Our statement specified that the proposed measures would be subject to consultation.

However, the risks associated with telecommunications go far beyond cybersecurity, as I was saying. We took action in May 2022, when we made this announcement.

[*English*]

Canadians watching will remember the famous Rogers outage in the summer of 2022, which probably impacted 12 million Canadians for a number of hours. With the after-effects of Hurricane Lee in Atlantic Canada in September 2023, my colleague, Minister LeBlanc, was really involved in restoring the services that people need.

I want colleagues to understand that this is not just about national security, but the role of the industry minister is to ensure resiliency. If you think about hurricanes, if you think about the network outage we had, in the case of Rogers we were successful in getting a voluntary undertaking in the memorandum we signed with them in September, but I think Canadians will be reassured that the minister would have legislative power to compel companies to do what's right.

We know that these risks are not something the market can solve on its own, that's why we need rules for industry, rules that protect Canadians, our networks, our businesses and our data.

[*Translation*]

Bill C-26, which we are discussing today, is designed to address those risks and evolving threats. It will enable the government to act quickly, if necessary, to ensure network security.

In my opinion, the powers granted to the Minister of Industry would enable him to act quickly. In an emergency, temporary measures must be adopted, but it must be done quickly to prevent bigger problems across the entire network.

The second part of Bill C-26 will also strengthen the protection of our critical cyber systems. I believe Minister LeBlanc was heavily involved in that portion.

[*English*]

Our telecommunication network is probably the backbone of infrastructure. I know people at home may think of infrastructure as bridges that we need to protect, they may think about nuclear power stations, but the telecom network, which is basically enabling everything else, is one of the key networks that we need to protect.

Mr. Chair, we want to make sure we get it right. As Minister LeBlanc said, that's why we listened carefully to the debates in the House of Commons and comments from stakeholders and colleagues, who are here because, when it comes to national security, that's not a partisan issue. That's why we are committed to making sure that we do that in the best possible way.

I am happy to see that there seems to be broad support for the bill and the objective of securing our telecom network.

[*Translation*]

We want to work constructively to get the best possible bill, but I must add that action is urgently needed. People who would like to inflict harm on Canada are obviously seeking potential loopholes in the system. So it's urgent to provide the government with the powers it needs to do things right. That's important.

I therefore eagerly await the passage of Bill C-26 to better protect our critical infrastructures.

Mr. Chair, my colleague Minister LeBlanc and I will be pleased to answer our colleagues' questions.

Thank you.

[*English*]

The Chair: Thank you to both of you for your comments.

We're going to move right into questions.

I'm going to start with Mr. Shipley, please, for six minutes.

Mr. Doug Shipley (Barrie—Springwater—Oro-Medonte, CPC): Thank you, Chair.

Thank you to the ministers and the officials for being here this morning.

We are definitely talking about a very serious issue here with cybersecurity and Bill C-26.

Minister LeBlanc, Public Safety Canada recognizes 10 critical infrastructure sectors, one of which is government. A recent NSICOP report noted that several departments and Crown corporations are not subject to Treasury Board policies related to cyber-defence or they apply those cyber-defence policies to their departments inconsistently. This leaves them vulnerable to cyber-attacks. In fact, just recently it was revealed that Global Affairs Canada was suffering from a massive data security breach.

Minister LeBlanc, why is your own government not adhering to the same cybersecurity standards as the designated operators listed in this bill whose confidential business and personal information you're planning to collect and store?

Hon. Dominic LeBlanc: Obviously, we took note of the work done by NSICOP. These are, for our government and for our department, important road maps to better public policy and better legislation.

I'm aware of procurement initiatives under way across the government to improve many information systems that are either outdated or arriving at the end of their useful life and needing to be reinforced. It's something that industry and businesses do every week and every month. The government has the same obligation

The premise of your question is whether we have, in the Government of Canada, an obligation to hold ourselves to at least the standard we would expect of private industry, and the answer is, of course, and we're actively looking at ways. You mentioned the foreign affairs department, and I'm aware that, in the Public Safety portfolio, we're actively investing in modernizing systems and are constantly looking for good ideas and better solutions, including with our allies.

● (0835)

Mr. Doug Shipley: Thank you.

We heard almost unanimously that this is an important bill, but this is also a poorly drafted bill. Business groups, civil liberties groups and cybersecurity firms are all united in the fact that Bill C-26 gives the government too much power with almost zero oversight. There's no requirement for regular reporting, no independent review and no requirements for production of written reports. In fact, most of the powers in this bill would be exercised in secret.

Do you think that the sweeping powers that you're attempting to give yourself have enough oversight mechanisms attached to them?

Hon. Dominic LeBlanc: We've obviously taken note of the concerns expressed by the people our colleague referred to. We would expect that, in the work of this committee, if there are amendments that, in your view, answer some of these concerns, of course we would be open to working with the committee and to ensuring that collectively we get the best legislation we can.

We recognize that these are extraordinary powers in many ways that require, as you noted, the appropriate oversight. There is an element of judicial oversight, but we also recognize that the threat landscape is evolving as well and evolving very quickly. According to some of the briefings I have from security officials, including at CSIS, the threat actors, including malicious state actors, are seeking to do some of the damage and disrupt some of these systems that we talked about. We require the ability to move quickly, and we require the ability to help identify potential risks and hopefully prevent incidents from happening. That's why there are these powers, but we recognize that these powers come with an obligation of transparency in every case possible and the appropriate reviews, including judicial reviews.

François-Philippe, you had a point on the judicial review.

Hon. François-Philippe Champagne: If I may, Mr. Chair, I just want to add that, obviously, it's an important question, and we believe in oversight, as I said, the judicial review and also the concept of proportionality.

I just want to remind colleagues that, when we had major storms, particularly on the east coast, I had premiers calling and asking us to take action. As I said, in the telecom area, although now we have the memorandum we signed voluntarily with the telcos, I think that Canadians and members of Parliament would want any future minister of Industry to also have the power to take action very quickly.

You may recall that, in some instances, we were asked to direct the telcos to do certain things. I can assure you that, when you don't have access to 911 and you're facing an emergency, Canadians are very worried about that. For us to be able to take remedial action or compel telecom companies to do certain things—now they've done it voluntarily—I think it's a good thing—

Mr. Doug Shipley: Thank you.

Hon. François-Philippe Champagne: I don't think Canadians would want to rely on a voluntary basis.

Mr. Doug Shipley: Thank you.

I'm almost out of time, but I have one last question for you, Mr. Champagne.

Many stakeholders have noted that the proposed penalties related to this act that would reach up to $15 million and five years of jail time are touted as being intended to promote compliance rather than to punish; however, I think that we can all agree that a penalty of this nature would be very challenging for a small business to absorb.

Has any consideration been made about the impact that these large fines would have on small and medium enterprises?

Hon. François-Philippe Champagne: I would say respectfully to the committee that it's always a matter of balance. I would also say respectfully to members of the committee to have a fine that is proportionate, because obviously you're referring to small and medium-sized businesses. Let's be clear that the systemic risk to our network with very large players is the danger of going too low, and colleagues would agree that, if the fine is of that nature when you're talking about the big telcos, it's kind of irrelevant. I'm not sure that this would give power where the Minister of Industry would have to compel them to take action.

I don't suggest they do that, but they could do a cost-benefit analysis and decide to ignore the minister because, at the end of the day, the fine is so low that it's just business as usual.

In cases of emergency, I can tell you that, the Rogers outage touched 12 million Canadians. In this case, you need a kind of stick to make sure that people will comply, because you're talking on behalf of millions of people.

● (0840)

The Chair: Thank you.

We're moving on now to Mr. Schiefke, please.

[*Translation*]

Mr. Peter Schiefke (Vaudreuil—Soulanges, Lib.): Thank you very much, Mr. Chair.

I'd like to thank the witnesses for being here today.

Mr. Champagne, drawing on your experience, having worked with our economic partners around the world, including the U.S. and Europe, can you walk the Committee through the importance of passing C-26 to protect not just our own businesses, but the businesses we work with every day under free trade?

Hon. François-Philippe Champagne: That's an excellent question, Mr. Schiefke.

We never want to be perceived by state and non-state actors as the weakest link in the chain, the one that attracts these kinds of malicious acts, which can harm Canadian companies or even critical systems. Intelligence and public safety specialists can tell you that.

I always try to compare ourselves to the G7 countries and the Organisation for Economic Co-operation and Development, or OECD. As Canadians, we want to be among the best and have modern tools. To me, it's about modernization. When I saw, for example, that the Telecommunications Act did not include security as an objective, I thought it a glaring omission. Among our allies, I don't think there's a country where the Minister of Industry or the person in charge of a network as important as telecommunications doesn't have security as an objective. Today, it's essential. People know we need this.

The bill we are proposing will enable us to live up to the expectations of our economic partners. You're right, it's a step in the right direction.

Mr. Peter Schiefke: Thank you very much, Minister.

[*English*]

Mr. Leblanc, the same question is for you.

I'm glad that you mentioned our Five Eyes partners. With the interconnectedness of our economy growing day by day, how important is it for Canada to do our part to advance our cybersecurity protection efforts, specifically with relation to Bill C-26?

Hon. Dominic LeBlanc: This legislation is consistent with measures that are in place with our Five Eyes partners. As I've said, the Five Eyes public safety ministers had a virtual meeting this week. This is always a sort of standing item—what we can do to deal with threats in the cybersecurity domain. The nature and the evolving threat landscape is such that I would suggest one country alone won't be able to have all of the good ideas and all of the best practices. That's why, as François-Philippe said...the ability to work with G7 countries, particularly in the security context with our Five Eyes partners.... MI5 and MI6 in the U.K. have done a lot of research in this area.

One thing that obviously our American allies worry about is the rise of disinformation. They're in an election year. There's the chance that malicious state actors can either encrypt or paralyze cyber-systems in the United States and insert disinformation and malware. The very basic tenets of a democracy are reliant, as François-Philippe said, on a series of private sector and government actors in the basic transmission of information.

In our perspective, the Government of Canada thinks the adoption of this legislation will put us in a similar position to our five allies. If we're not able to, in this Parliament, adopt this legislation, I think it would conversely send a signal to our allies—particularly to the United States. I refer to that, because the interconnectedness of our economies and industries, which my colleague knows better than I do, means that basic services to Canadians, which we rely on for daily life, would be, in our view, subject to a threat that can be mitigated and can be contained.

Mr. Peter Schiefke: Thank you.

My last question in the minute and a half that I have left is for you, Minister Champagne.

The bill is often talked about in terms of cybersecurity, but part 1 is also very important. It's about creating authorities to secure the network, which has applications beyond cyber-threats, including how we respond during natural disasters.

It's important for my community of Vaudreuil—Soulanges and many others across the country. In my particular case, last year, when we had our ice storm in Quebec, I could not actually pick up the phone and call the mayors and my provincial counterparts to coordinate a response to help support those who had no power and were stuck at home—seniors particularly.

Can you speak to how important that is for us to be able to respond and better support Canadians in their time of need?

● (0845)

Hon. François-Philippe Champagne: Yes, I would say one word: resiliency.

The purpose of this act is to ensure resiliency of the telecom network in particular. Like you said, natural disasters come more frequently, they seem to be more violent, and they seem to come in different forms. Therefore, from forest fires, to hailstorms we had in Quebec, to floods in Atlantic Canada, we should not just look at this bill in terms of security, but also, when it comes to many of these crucial networks, as resiliency.

You would want a future minister of industry to have some power. Like I said, last time, in light of that, we signed this memorandum of understanding. Basically I gathered the CEOs, and I said we need to do better—you need to do better to protect Canadians. We did it.

I think it is wise, I would say, for a nation like Canada to have statutes in the book to be able to compel...not only relying on the goodwill of actors, which they did. Like you said, for people in times of need, these systems become critical. When you can't access the phone line and you're subject to a flood or another natural disaster, these powers would at least compel us to take certain actions. Obviously, it would be for the service provider to take these actions. At least you would have a kind of power, not just a soft power to convene and ask. Then you could compel others to do things.

The Chair: Thank you, Ministers Champagne and LeBlanc.

We're now moving on to Ms. Michaud, please.

[*Translation*]

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

Thank you, Ministers, for being with us this morning.

First, I want to talk to you about an article published in *La Presse* entitled "*Quand Ottawa veut jouer au gérant d'estrade*". The article appeared in 2022, shortly after you tabled Bill C-26. The bill was tabled some time ago—over eighteen months. One wonders if cyber security is indeed a priority for the Canadian government.

The article was written by Ms. Célia Pinto Moreira, a public policy analyst at the Montreal Economic Institute.

She begins her article as follows: "Imagine a referee at a Habs game approaching a player to explain how to shoot the puck into the net. He'd likely lose his job: it's neither among his duties nor his field of expertise."

She goes on to say that this is what Ottawa is doing with Bill C-26. She says, "Instead of minding its own business, the federal government wants to interfere in the implementation of companies' digital security plans."

She adds, "In digital security, things move at breakneck speed. When a company discovers a flaw in its system, it knows full well that it has every incentive to fix it quickly; otherwise it exposes itself to significant legal, reputational and financial risks […]"

She goes on to say that the federal government is slow or inefficient, citing the passport saga.

We remember that saga. It's been a while. Other examples include Phoenix, Canada Life, the border. I think the government has been slow and inefficient in those situations.

All in all, it seems likely that Canadian companies are currently well prepared. They already have to deal with cyber security incidents. It's said that in 2021, Canadian companies invested over $10 billion to prepare for this type of breach. So they're already doing the work.

In practical terms, what will Bill C-26 change for Canadian companies?

Hon. François-Philippe Champagne: Thank you for the question, Ms. Michaud, and thank you to the author of the article.

Let me give you an example that I think will answer your question.

You know that preventing harm is also part of the government's role. Remember the Rogers case. Twelve million Canadians lost access to telecommunications services, which even prevented them from making payments, since Interac services were connected to the Rogers network.

In this instance, the government was swift to act. I believe I was in Japan, but I spoke to the president and CEO, or CEO, of Rogers within hours, asking him to take very concrete action. On the one hand, one could say that Rogers is a large company that probably invests hundreds of millions of dollars in cyber security, but on the other hand, 12 million Canadians were without telecom services for hours.

At that point, I challenged not just the CEO of Rogers, but all the CEOs of the major telecom companies, telling them that they all had to deploy their teams that day to help Rogers. It was no longer a matter of competition, but an emergency, because Canadians were unable to go to the grocery store or put gas in their car. Their payment cards were no longer working.

You're going to argue that there should be resilience within the system. But in subsequent hearings, we realized that, curiously, there wasn't as much resilience or redundancy in the system as we thought. Yet everyone was saying that the Interac card operator obviously had to have a back-up system.

I think the facts have shown that things needed to be improved. I also think it's the government's role to protect the public interest.

You're right that most companies do it well, but I think the Rogers case is a great example of the role government plays. At the time, we did it voluntarily. For that matter, I'd like to thank the various companies for their willingness to help. They even signed a memorandum of understanding on the subject. The number of pages it contains proves that there was a great deal to be done.

I think that, for future such emergencies, having powers at our disposal and the ability to tell companies that they haven't done their job and that it's hurt Canadians, would be a good thing. I think it's justified.

● (0850)

Ms. Kristina Michaud: Thank you, Minister. I know you can speak at length on a subject you're passionate about, but we don't have much time.

What stands out for me in this bill is that it confers enormous powers on the Governor in Council and the Minister of Industry, meaning you. You strike me as a trustworthy man. If you do all this secretly, things may go quite well, but some Canadians and Quebecers are worried. Transparency issues are being raised.

Can you explain why all this has to happen in absolute secrecy and what this could mean for small or medium-sized businesses?

You mentioned large companies, such as Bell and Rogers, who can afford to be fined a few million dollars by the government if they don't comply with requirements.

But what does that mean for a small Quebec company? You know how important small and medium-sized businesses are to the Quebec economy.

What does this mean for a small telecom company with a few hundred or a few thousand subscribers, offering its services only in part of the territory?

What about the company that doesn't have the workforce to implement a security plan that complies with your plan? Will it be fined a few million dollars?

What powers can you wield? People tell us they read in the legislative summary that the Minister of Industry can make orders and decrees, but they don't know what they are.

Can you explain all this to us?

Hon. François-Philippe Champagne: Thank you for your trust. I'm grateful for it.

I have two points to make.

First, this matter is subject to judicial review. We talked about this, and Minister LeBlanc referred to this earlier. I don't want to play lawyer before the committee. However, as you know, in the case of a judicial review, the measures taken must be proportionate.

Second, in terms of national security, some of these orders must be secret for a reason. I'll provide an example, and you'll immediately understand the issue. If we find a flaw in a system, obviously we don't want state and non-state actors to take advantage of the flaw before we can fix it. That's what we would be risking if we were to release all our orders.

Think about a cyber attack. In the case of 5G technology in particular, it will be decentralized. The weakest link in the chain could be attacked. In keeping with the interests of the company, the organization and Canadians, we should have the opportunity to issue a secret and confidential order in this type of situation, saying what must be repaired.

As we said, there will be feedback. We can report on the situation. The issue is that, in our democracies, state and non-state actors who want to harm the country don't play by our rules. If I release information stating that the weakest link in our system is found in a given telecommunications system or service, I'm practically summoning the bad people before we've had time to repair the breach in our system.

I think that this would put the whole network at risk. That's why, in some cases, we must keep this information secret and confidential to protect national security.

[*English*]

The Chair: Thank you.

Now we're moving on to Mr. Julian, please.

[*Translation*]

Mr. Peter Julian (New Westminster—Burnaby, NDP): Thank you, Mr. Chair.

I want to thank the ministers for joining us. They're always welcome here.

We would be delighted to see you more often in the committee, Mr. LeBlanc.

● (0855)

Hon. Dominic LeBlanc: Not as often as I would like, Mr. Julian.

Mr. Peter Julian: As you said earlier, this is an issue of national importance. We know that the number of cyber attacks keeps increasing.

The government tabled this bill in June 2022. We're still studying it. Everything is happening slowly. It's 2024, and the bill hasn't been passed.

Why doesn't the government seem to consider this a priority when we know it's a major issue?

Hon. Dominic LeBlanc: Mr. Chair, I would like to thank my friend and colleague Mr. Julian for his question.

I admit that things haven't moved forward as quickly as we would have liked.

Mr. Julian, you're a House leader. You know that the parliamentary process can often be slowed down by other issues at certain times. This isn't an excuse at all. I agree that we would certainly have liked to see the bill passed before 2024. I don't disagree with you.

We're ready to do whatever we can. This includes working with this committee on amendments and making sure that all our departments' resources are available to help you move forward if the committee decides to proceed.

I accept this criticism in good faith. I acknowledge the urgency, and we'll do our best. I don't need to remind you that I've been the Minister of Public Safety only since July. You and I worked together over the summer. You know all about this.

Mr. Peter Julian: Thank you.

I'll move on to another question.

[*English*]

We've heard testimony. Mr. John de Boer from BlackBerry testified that, from September to December of last year, there were over 5.2 million cyber-attacks, and 62% of them targeted critical infrastructure. We heard from the Canadian Bankers Association that the number of priority one cyber-attacks has tripled over the course of the past year.

Is the government—Public Safety and Industry—tracking the number of cyber-attacks across all sectors? Do you have that information available? To this date, we haven't been able to consolidate the number of attacks by sector. In fact, in many cases, we've been told by witnesses that they simply don't gather those figures.

Hon. Dominic LeBlanc: Thank you for identifying what we think is one of the positive elements of this legislation, the obligation to report. We take the good faith of many of these important private entities in working with the Government of Canada, but it probably isn't at the level that it needs to be. That's why the positive obligation to report would ensure that we have reliable and accurate data on the alarming increase that you identified.

The Communications Security Establishment as I mentioned at the beginning, would be the federal agency that would be in a position to gather this data and share it across the government. The briefing's I've had from Public Safety and from the director of CSIS and others confirmed that alarming trend.

Patrick, you may have details on what we or the CSE are tracking. Could you briefly provide Mr. Julian with that information?

Mr. Patrick Boucher (Senior Assistant Deputy Minister, National Cyber Security Branch, Department of Public Safety and Emergency Preparedness): To add what Minister LeBlanc said, currently, all reporting is done on a voluntary basis, and that's great when it happens, but obviously there are gaps in that. Part of this legislation as a foundational piece, as Minister LeBlanc said, is to make sure we regularize that reporting so CSE can take that information in, utilize the expertise that resides at CSE and propagate that out to build resilience in other sectors as well.

Mr. Peter Julian: Thank you, but that actually wasn't my question. I certainly understand how Bill C-26 attempts to correct that problem. What I'm asking is what the figures are now? Do you have figures you can share with us, even if they've been reported on a voluntary basis, that indicate the extent and scope of cyber-attacks in Canada?

Mr. Patrick Boucher: We can definitely go back to talk to our partners at CSE, which is under the portfolio of DND, to see if there's some readily available information related to that.

Mr. Peter Julian: That would be very helpful for the committee to have.

Hon. Dominic LeBlanc: I'm happy to ensure we get that information as quickly as possible to share it with the committee.

Mr. Peter Julian: Thank you very much.

Mr. LeBlanc, one of your other portfolios is foreign interference in our election process. We've been talking about the Communications Security Establishment. They flagged late last year that Russia's, China's— and I think we can add to that allegations of India's—cyber-threat activity includes “attempts to conduct...attacks against election authority websites, accessing voter personal information or information relating to the election, and vulnerability scanning on online election systems.”

We've seen foreign interference have a dramatic impact in the United States in the election of Donald Trump and in the United Kingdom in the Brexit referendum. In what way would Bill C-26 reinforce our election system, our democracy, to protect against those cyber-attacks that have had such a marked influence in other democracies?

● (0900)

Hon. Dominic LeBlanc: I certainly share your concern. I think you are absolutely right about the risk. This is, as I noted, a U.S. election year, so those same actors who we understand had some success in 2016 will be at it again this year. This is a subject for another committee, but Canada Elections Act amendments may come in the coming weeks. The fact that we have a paper ballot system is, the Chief Electoral Officer says, one of the best ways to secure our voting system.

In my conversations with the Chief Electoral Officer, we're obviously governed by his advice and his recommendations. I think where this legislation might bump up into the important job of securing election systems is, for example, if the Canada Elections Act were to allow people to apply online for a mail-in ballot—I'm just using one example off the top of my head—where those requests would go across the telecommunications channels people have, the private businesses my colleague referred to. That is not an Elections Canada system per se, but it's vital for people having access to democracy. So if we're working on making voting more accessible in 2024, 2025, it will necessarily involve the Internet, it will necessarily involve telecommunications systems.

The voting process per se is a paper ballot, but Elections Canada is very concerned about this. We've invested in this and we've allowed the Communications Security Establishment to work with Elections Canada to strengthen their systems. As my colleague would know, we've had Government of Canada officials be available to political parties to help them secure their systems. It is a source of concern we share and we're prepared to do everything we can in that regard.

The Chair: Thank you so much.

We're moving on to the second round.

Mr. Lloyd, please, for five minutes.

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

Thank you to the witnesses for coming today.

Ministers, building resiliency for natural disasters, building resilience against cybersecurity threats, these are things I think all Canadians and all parties can get behind. We know there needs to be increased investment in cybersecurity and resiliency, but something both ministers said today gave me some pause, when they referred to this bill as giving the government, in their words, “emergency powers” and “extraordinary powers”. I think it's very concerning to Canadians who want to know why the government needs “emergency powers” and “extraordinary powers” when we're really talking about trying to boost resiliency against natural disasters and trying to get companies to invest more in cybersecurity. Why does the government require legislation that gives them the power to conduct courts in secret, to announce legislation or block people from being part of the telecommunications sector in secret? Why are these emergency powers needed when what we need to do is get more investment in cybersecurity?

Hon. François-Philippe Champagne: I'll be happy to respond to that.

First, thank you for saying this is not a partisan issue. I think, like you said, we're all trying to do the best thing.

I'll give you a very concrete example. In 5G, I think everyone would agree that this is going to be very decentralized. When you go from 4G to 5G, it's a different world. We're not in the same kind of network. The future will be that you have intelligent products, so that everything is interconnected. If we were to find that there is a failure or an intrusion in the network that could have a systemic effect, you would want the Minister of Industry in the future to be able to say, “You, stop,” or we disconnect that particular person or entity that is the source of the infection of the entire network that could have a systemic effect. The kind of power you need, you need to act very quickly, because you're talking about—

Mr. Dane Lloyd: Why do you need secret courts, Minister?

Hon. François-Philippe Champagne: I'll tell you. It's very simple, because you would not want the actors, the ones who are trying to infiltrate our system, to be aware that you're asking them to plug the gap—

Mr. Dane Lloyd: What safeguards are you going to put in to ensure that this power is not abused? We've had lots of witnesses talk about how concerned they are about these powers, and you've called them “emergency powers.” It's very concerning.

Hon. François-Philippe Champagne: People should be equally concerned that today—imagine—the Minister of Industry doesn't have the power to ask that particular entity to plug, for example, the failure in their system that could have a systemic effect that could affect millions of Canadians. The check and balance on that, I would say, as a lawyer, is you have judicial review, and under judicial review you have proportionality and the Charter of Rights and Freedoms. All of these bills and legislation still apply.

● (0905)

Mr. Dane Lloyd: The Privacy Commissioner has stated that there isn't proportionality in this bill. What can we do to bring more proportionality to this bill?

Hon. François-Philippe Champagne: I would say that under judicial review, as you know, it's well established in jurisprudence that you need to have proportionality in terms of the act of the government, but I think you should see it in a positive way. Imagine the reverse of not having the power, and you come to know that somewhere in the network someone is infiltrating, which could have a systemic effect and be damaging both economically and otherwise to millions of Canadians. Think about the reverse.

Mr. Dane Lloyd: Thank you for that, Minister.

Minister LeBlanc, Canada has faced over the past few years a significant issue, in that nearly 100 churches have been burned down or attacked in this country, most recently, the Blessed Sacrament Church in Regina. Leading up to Christmas there were four churches in Alberta that were burned down. We haven't heard anything from you, in your role as public safety minister, to denounce these attacks. I just want to give you an opportunity today to assure the Canadian people, the Christian community and other communities of faith that you denounce these attacks against churches in Canada.

Hon. Dominic LeBlanc: Of course our government, and I, personally, and all of us denounce what is an alarming increase of attacks against religious and cultural communities. I talk to the RCMP commissioner often about what we can do as a national police force, with local and provincial police, to better protect communities, including the examples that our colleague identified. We're concerned about an alarming rise in hate speech and acts of hate crimes, so I'm happy to join everybody in denouncing those particular incidents.

Mr. Dane Lloyd: I do appreciate that, Minister. I am concerned, though, that departments under your control—such as CSIS, for example—have not talked about this. This is a threat that we're facing across Canada, and in some cases I believe this rises to the threshold of terrorism. What are we doing to stop these terrorist acts against communities of faith in this country? What are you doing, Minister?

Hon. Dominic LeBlanc: I'm working daily with the RCMP and other security partners to ensure they have the tools necessary to best protect Canadians. The decision around terrorism is properly in the hands—it's not a political decision—of prosecutors, investigators, the national police force and local police partners. However, we recognize that the increase of hate crimes means that the RCMP needs to work with local police to understand the nature of that threat and to ensure that local police forces and the RCMP—in the case of transnational organized crime—have all of the tools they need to protect Canadians.

The Chair: Thank you.

We're now moving to Ms. O'Connell, please.

Ms. Jennifer O'Connell (Pickering—Uxbridge, Lib.): Thank you, Chair.

Thank you, ministers, for being here.

We heard a lot about privacy and privacy concerns, and we heard that from witnesses, certainly. I think my colleague across the way misquoted the Privacy Commissioner, but there was a conscious effort in this legislation to provide foundational legislation here, in Bill C-26, and then a conscious effort to deal with some of the specifics through regulations. What the Privacy Commissioner spoke about was wanting to be involved in the development of those regulations to specifically address concerns of privacy, details around SMEs and indigenous communities that may need specific help and foundational work to actually implement the goals of this objective. Can you speak to how regulations and the work with the Privacy Commissioner would be engaged to deal with privacy concerns?

Hon. Dominic LeBlanc: Obviously, nothing in this legislation affects the applicability of the Privacy Act. As I noted in my opening comments, if we can better help critical infrastructure sectors of the Canadian economy—things as important as banking and telecommunications companies—better secure their systems, and help each other, obviously with the CSE, that is also a protection against the loss of privacy and private information.

I remember my conversations with Premier Furey of Newfoundland and Labrador, when some ransomware had been inserted and they had exported data from a health authority, which covered 40% or 50% of the population of the province, so you can imagine the vulnerability that people in that province felt. It was resolved with the help of the CSE. If this legislation in some ways better incentivizes, which would be a polite word for it—or "compels" is another word for it—private sector partners to do everything they have to do to secure the data, we think that's also important.

Ms. O'Connell, again, we would be happy to respond specifically to the question around amendments, to work with the Privacy Commissioner and to listen to other experts in this area. We respect and appreciate the application of the Charter of Rights, the Privacy Act and other legislative measures that are important. We think that this legislation, done properly, is in fact part of improving and securing the private information of Canadians. We look forward to the deliberations of this committee and the Privacy Commissioner, of course. His views will be very important in our getting this balance right.

● (0910)

Ms. Jennifer O'Connell: It has also been suggested that there are somehow secret courts, but when dealing with matters of national security—for example, even CSIS with the CSIS Act—there is already legislation that all governments have used, judicial reviews and the court process. Does this legislation go beyond what already exists in Canadian law, in terms of the protection of national security but allowing the judicial process to ensure that no government overreaches past legislative authorities?

Hon. Dominic LeBlanc: That is a good question. You served on NSICOP as well. You would have seen and been aware of some of these national security threats. You would also know, and you correctly referred to, processes in the CSIS Act. I as minister sign, for example, CSIS warrants. They are appropriately reviewed by the Federal Court of Canada, in the appropriate closed proceedings with amicus curiae there.

I get it. I've been a member of Parliament for a while. “Secret courts” is a nice clip. It doesn't reflect something that's new or different, and the words are loaded to get a reaction.

This is the appropriate balance that's no different from other legislation that you referred to, and is subject to judicial review as, obviously, is appropriate.

However, Mr. Champagne wants to add something briefly.

Hon. François-Philippe Champagne: I want to rebase that also with the comments that were made by a colleague before. The power of the Minister of Industry is, “to take action to promote the security of the Canadian telecommunications system”. People say, “Those are broad powers,” but they have a very clear objective and they're not very extended: They are to promote the security of the telecommunications system in Canada. Therefore, like I said, under supervision of the court, people would look, in a judicial review, at what the objective was and whether the action was in line with the objective stated, which is the security of the network. I think that is confining the powers, which are given under the act, to act very quickly. It's a very specific objective.

The Chair: Thank you.

I go to Ms. Michaud, please, for two and a half minutes.

[*Translation*]

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

Ministers, I'll be honest with you. I think you already know this. When studying a bill, the Bloc Québécois likes to make sure that the jurisdictions of the provinces and Quebec are respected.

There's a concern about Bill C-26. Electricity Canada officials told the committee about this concern. Bill C-26 includes interprovincial and international power line networks in its list of critical systems. We can read between the lines that an organization such as Hydro-Québec could be affected by this bill. Correct me if I'm wrong.

The Electricity Canada officials said that they would like to see the bill amended to avoid duplication, overlap or redundancy with the jurisdictions of the provincial agencies already involved.

For example, Hydro-Québec, the pride of Quebeckers, could receive a financial penalty of up to $15 million for failing, for any reason, to comply with certain ministerial orders.

Is that right?

What does Bill C-26 mean for Hydro-Québec, for example?

● (0915)

Hon. Dominic LeBlanc: Mr. Chair, I would like to thank Ms. Michaud for her question.

Hydro-Québec should be the pride of all Canadians, not just Quebeckers. I share my colleague's enthusiasm for this vital institution for the country.

I discussed the issue with the Quebec minister responsible for cyber security. We had a good discussion. He raised exactly the same concerns as Ms. Michaud. Obviously, we want to respect the Quebec government's jurisdictions. However, the legislation also gives the Government of Canada certain jurisdictions in certain areas of the economy. We also want our jurisdictions respected. You brought up Hydro-Québec. There will obviously be areas of intersection.

Personally, I think that we need to work with the Quebec government. The Quebec government's objectives are the same as ours. I was impressed by my Quebec counterpart's efforts to secure critical systems in Quebec. Once again, Quebec is setting an example for the rest of Canada.

We certainly won't try to pick a fight. We'll try to work closely with the Quebec government. However, we'll uphold our responsibility at the national level, without taking anything away from the provincial governments.

The Department of National Defence's Canadian Centre for Cyber Security is probably a national leader. We must work with the provinces and share our knowledge and expertise with our provincial counterparts.

[*English*]

The Chair: Thank you.

We have Mr. Julian for two and a half minutes, please.

Mr. Peter Julian: Thank you very much, Mr. Chair.

The coalition of national groups, including the Canadian Civil Liberties Association, la Ligue des droits et libertés, and the Privacy and Access Council of Canada, have been critical of the bill, but have also proposed some concrete solutions.

One of those, given the fact it is clear in their understanding that Bill C-26 would restrict the applicant's access to evidence, is to create a special advocate to enable evidence to be tested in a court of law without being disclosed to outside parties. This recommendation, of course, borrows from the Immigration and Refugee Protection Act.

I have two questions for you, Mr. LeBlanc, on their suggestion around a special advocate. First, why didn't the government consider creating that special advocate in the legislation initially? Second, does the government now support the idea of improving this legislation, which has some major weaknesses, by the creation of a special advocacy?

Hon. Dominic LeBlanc: We have taken note of that suggestion that you properly raise.

I'm by no means an expert in this area of national security law, but you referred to examples under the Immigration and Refugee Protection Act where these advocates are able to participate in these closed proceedings and have access to all of the appropriate intelligence information.

I know in the context of CSIS, there are amicus curiae who can participate in these Federal Court hearings, so we would look favourably upon suggestions or amendments that this committee would want to make to ensure that we get that balance right. There's certainly no principled objection from our part if, in the wisdom of this committee, that were an amendment that would be inserted, which, I hope, would answer some of those very legitimate concerns. We would look favourably upon exactly that kind of *démarche*.

Why it wasn't included in the beginning, I can't speak to that particular instance, but I'm more than happy to work with colleagues if that's deemed to be an oversight or something that can be corrected. I'm happy to accept the suggestion in a collaborative way.

Mr. Peter Julian: Thank you for that.

Other testimony we heard from Electricity Canada—and Madame Michaud noted that just a few minutes ago—was the fact that there are different regulations around NERC, the North American co-operative of energy, and what would be required in terms of Bill C-26. The recommendations from Electricity Canada were to ensure there wasn't a doubling up of regulations or requirements.

To what extent did the government consult with industry groups, such as NERC, over the course of the production of the bill? Is the government open to having more harmony between regulations that are already put in place by the industry groups and the provisions of Bill C-26?

● (0920)

The Chair: Mr. Julian, your time is up. I've been more than generous.

We're moving to Mr. Lloyd, please.

Mr. Dane Lloyd: Thank you, Mr. Chair.

Minister LeBlanc, Bill C-26 deals with cybersecurity. We know that the government's in-house IT capabilities are limited, and they are often dependent on contractors and consultants. We learned yesterday that GC Strategies has received $258 million from your government in contracts.

Has this two-person IT company working out of their houses received any contracts from your department related to cybersecurity and measures in this bill?

Hon. Dominic LeBlanc: Obviously, as we've said, there are serious concerns around this particular business. All contracts have been suspended with that business since last fall. There are internal audits and investigations going on at the Canada Border Services Agency. I know that the Treasury Board and the procurement department are also looking at this.

I'm not aware of specific contracts with this particular business that the public safety department has around IT security, cybersecurity. There are well-known elements with the Border Services Agency, but I'm happy to undertake to get that information to the committee.

All of that is part of these internal investigations that are ongoing. Of course, as we've said, if there was inappropriate behaviour it will face severe sanctions.

Mr. Dane Lloyd: Thank you.

We know that CBSA has awarded this company 134 contracts. Are any of these contracts related to Canada's cybersecurity?

Hon. Dominic LeBlanc: Again, I think the Border Services Agency clarified the number of contracts you are referring to. It referred to amendments to actual contracts. The number is much lower than that. Again, regarding this particular business's implication in cybersecurity, I'm happy to get back to the committee with a specific answer.

That's obviously a concern we have—I'm not diminishing it—and that is subject to these internal investigations. I spoke with the president of the Border Services Agency as recently as this morning on this same suite of issues, but I'm happy to get back to the committee with that information.

Mr. Dane Lloyd: Thank you. Is that a commitment from you, Minister, to get that information to this committee?

Hon. Dominic LeBlanc: It is, to understand the nature of where that particular business might have been working on cybersecurity issues.

Mr. Dane Lloyd: Thank you.

My follow-up question is to Minister Champagne.

ISED has given GC Strategies 25 contracts. Were any of these contracts related to cybersecurity or to provisions in Bill C-26?

Hon. François-Philippe Champagne: As Minister LeBlanc mentioned, there are ongoing internal investigations to assess exactly the nature of these contracts. I'm happy to get back to the committee to provide further details if any of them, as my colleague suggested, relate to anything with respect to cybersecurity.

I suspect not, but we will confirm and get back to the committee.

Mr. Dane Lloyd: Mr. Chair, we know that at National Defence there have been six contracts awarded to GC Strategies, and we know that at Global Affairs there have been 12 contracts awarded.

I don't expect you to know if those were also related to cybersecurity. Would you know?

Hon. François-Philippe Champagne: I do not, but what I think Minister LeBlanc and I can commit to this committee is to ask our colleagues to follow exactly the same kind of procedure we will undertake, to confirm to the committee—

I suspect not, but again, we will endeavour to get back to the committee.

Mr. Dane Lloyd: I'd like to give the rest of my time to Mr. Motz.

Thank you, Mr. Chair.

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

The national strategy for critical infrastructure lists 10 areas that are critical to the security of our infrastructure, yet this bill only talks about five or six of them.

Is there a reason we've left health, food, water, manufacturing and those sorts of things out of this bill, which are critically important to sustaining the safety of Canadians?

Hon. Dominic LeBlanc: Obviously this legislation can only apply to federally regulated sectors. We as a government want to collaborate with partners in provinces and territories that, for example, would manage health systems. I identified that as a vulnerability. We can't legislate in that particular area. We would seek to sign agreements where possible with other partners.

● (0925)

Mr. Glen Motz: What efforts have you or Mr. Champagne undertaken with provinces, territories, municipal governments and first nations governments to deal with these issues that are critically important so that they, too, are adequately secured from a cyber perspective in this case?

Hon. François-Philippe Champagne: That's a very good question that you're asking, and as Minister LeBlanc said, we are in consultation with them.

I would say that those we have identified are also the backbone; the telecom system is an enabler of a lot of these other sectors of the economy. We initially targeted those that are providing systemic sustainment to some other field. At the end of the day, cybersecurity could cover a very wide area because, as I said, Canadians are impacted; SMEs are impacted, but those we have targeted in federal jurisdictions are kind of the backbone.

As Minister LeBlanc said, we are in discussions to see how we can do that, and we're certainly always looking to make sure that every sector that could be impacted by cybersecurity has adequate protection.

The Chair: Thank you.

Mr. Gaheer, please.

Mr. Iqwinder Gaheer (Mississauga—Malton, Lib.): Thank you to the ministers for appearing before the committee.

My first question is for Minister LeBlanc. We know that the legislation introduces a mandatory reporting requirement for critical infrastructure operators in the different industries.

Mr. Julian touched on this point. Electricity Canada raised the point that if an industry or a company is going through a cybersecurity attack, then mandatory reporting requirements, specifically immediate reporting requirements, could be cumbersome. Could you speak to why mandatory, as opposed to voluntary, reporting requirements are important?

Hon. Dominic LeBlanc: You're right. This would set up a system, a regime of mandatory reporting. We recognize that it is a burden or a circumstance that we're imposing on private businesses, but for the reasons my colleague identified, these private businesses are increasingly the backbone of basic services that Canadians rely upon for the Canadian economy, for the safety and security of people in their homes, driving their cars.

While many will want to voluntarily report, the obligation to have mandatory reporting will, to Mr. Julian's point, give us data on exactly the nature and the number of these threats, but it will allow us to work with other businesses to better protect them as a particular defect is identified or a particular threat or activity is successful.

The objective will be to quickly work with other players in that sector or similar sectors to ensure that they have the best resiliency and the best protection possible.

Mr. Champagne had something he wanted to add to that.

Hon. François-Philippe Champagne: I would like to say, to colleagues of the committee, think about the interconnectivity of that. When some telecom networks have gone down, in the case of natural disasters, it was related to a power outage. I think you cannot look at that in silos.

You have to take a systemic view. For example, if you had an attack on one system in the electricity network, that could well have an impact then on the telecom network because, without power and backup power, we may not be able to continue to function on the telecom network.

I think that's why you see this information that allows us to act very quickly to prevent a more systemic damage to interconnected networks. As I said, when you look at telecom, when you look at power, they are very connected. In all the disasters that we have had, and particularly in eastern Canada, when I talk to premiers, one of the things they mention is always power, because without power, the towers are not operational, even with backup power.

If we were to see an attack, a cyber-attack on the electric grid, we would want to know very quickly what impact that could have on the telecom network as well. Think about 5G with the Internet of things. If you have an attack on power, that could have a spillover effect in so many other ways. Colleagues were mentioning health, hospital functioning and equipment in hospitals. This is a systemic view of how to protect Canadians.

Mr. Iqwinder Gaheer: Thank you.

During the course of this committee, we've heard a lot about the transparency of the powers that are included in this bill on the use of those powers. Would the government be open to some sort of reporting of the number of orders that are issued under this bill for transparency, while protecting security details?

● (0930)

Hon. Dominic LeBlanc: That again is a good suggestion. We would want to take the advice from the chief of the CSE or the director of CSIS or other senior officials who have in many cases under law the responsibility to protect this information.

This is a discussion we're having with the foreign interference judicial inquiry: What's the best way to share with Canadians the nature of the threat of foreign interference? To use a similar example, cyber-attacks, many of them originating from foreign state actors, hostile state actors, might be a similar context.

The necessity to protect this information is precisely not to enable other hostile actors to have a nice road map into how to infect an electricity delivery system in Montreal or a health care system in some province. I have confidence in the officials who will do this work to respect the Charter of Rights and to respect the Privacy Act.

Again, at this committee, I'm happy to make officials available to work with you to understand the nature of that reporting requirement, but if there were sort of an aggregate report that *x* number of orders were issued in a particular year.... I would be happy to work with the committee, but I'm not an expert.

There's something called the "mosaic effect", as I've learned from the director of CSIS. Sometimes if you release certain pieces of information it appears innocuous in one particular context, but a hostile state actor, who may be deciding to do something very dangerous to Canadians, is in a position to piece together various pieces of public information and come to a conclusion—even if it's the wrong conclusion—and may not necessarily be bound by the responsibility to get beyond a reasonable doubt.

I just want to make sure that it's not interconnected and we're not committing to something that would be dangerous, but I'm happy to work with the committee.

The Chair: Thank you.

We're moving now to the third round.

We're starting with Mr. Motz, please.

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

Again, Ministers, we've heard from various witnesses here at committee through their written submissions that there are many flaws with this bill as written and tabled: overreach, lack of accountability and transparency.

Did you consult others on this bill? Obviously, it appears that maybe you didn't listen to the consultations.

Hon. François-Philippe Champagne: There was a wide consultation, and I would say, Mr. Motz, think about the danger of inaction as well. I respect the views of everyone, but the threats we've been talking about are in the telecom sector, the energy sector, financial services and transportation. If you look at our peers in the world, I think it's the responsible thing to do for Canadians to have these powers.

Like I said, in the telecom sector, as you will recall, we've been able to get a voluntary commitment, but I think that Canadians watching at home would want to make sure that government would have powers to compel the right thing to do to protect systemic failure that could happen to our fibre networks—

Mr. Glen Motz: Thank you, Minister. I apologize.

I'm going to turn my remaining time over to Mr. Lloyd.

Mr. Dane Lloyd: Thank you.

The Auditor General, in her recent ArriveCAN report, has made some damning revelations about cybersecurity related to your department, as follows: "There were deficiencies in the testing of the ArriveCAN application" and "Cybersecurity testing completed by resources" that were "not security-cleared or identified on task authorizations". Further, the Auditor General found that some of the "resources that were involved in the security assessments" did not have the proper "security clearance".

Minister, how can we be assured that your government has the security of Canadians as their highest priority when companies that are being contracted to provide cybersecurity on your priorities are not even being cleared for security clearance? Can you guarantee to Canadians that none of their personal information using the ArriveCAN app was compromised by these companies that did not have security clearance?

Hon. Dominic LeBlanc: We obviously were concerned with those Auditor General findings. My discussions with the president of the Border Services Agency have reassured me that she—before the Auditor General's report, as you know, the procurement ombudsperson also looked at this—has put into place a series of measures that will not allow that circumstance to happen.

● (0935)

Mr. Dane Lloyd: I appreciate that going forward, Minister, but can you guarantee that Canadians' personal information was not compromised by these companies that did not have security classifications to provide cybersecurity testing on the ArriveCAN app? Can you tell Canadians that their information was not compromised?

Hon. Dominic LeBlanc: What I can tell Canadians is that our government and organizations like the CSE, which would have an overarching responsibility around the protection of federal IT systems, are very effective at doing everything we possibly can to protect all systems that would contain the personal data of Canadians.

None of this work is perfect, and that's precisely why we work with allies around the world, the Five Eyes. That's precisely why this mandatory reporting will be an important—

Mr. Dane Lloyd: Minister, are you investigating whether this possible information was compromised?

Hon. Dominic LeBlanc: All of the circumstances around the ArriveCAN app, the development of that and the role of some private contractors, are being investigated. Also, as I say, I have every confidence that those incidents identified by the Auditor General have been corrected.

I'm reminding the committee that in the context of those first months of COVID, there was, across governments across the country, provincial governments—I was the Minister of Intergovernmental Affairs—a rush to do what was necessary—

Mr. Dane Lloyd: There's no excuse when Canadians' private information is put at risk.

The Chair: Thank you.

We're moving on to Mr. Bittle for four minutes.

Mr. Chris Bittle (St. Catharines, Lib.): Thank you so much, Mr. Chair.

Mr. LeBlanc, Mr. Motz brought up the provincially regulated industries and the importance they have to the security landscape. Can you comment on the role of the federal government with respect to this and whether there is an opportunity to amend the legislation to highlight the role of the provinces in regard to protecting Canadians in provincially regulated industries?

Hon. Dominic LeBlanc: That's very much at the heart of the exercise that I think all of us are trying to achieve in Bill C-26.

Our federation gives our partners in provinces and territories jurisdiction over things as important as health care systems and highway infrastructure. We're all thinking of examples where these particular critical infrastructure sectors can be subject to these cyber-attacks. I've spoken to mayors of cities. Saint John, New Brunswick, it was reported—a small Canadian city—was subject to a pretty concerning cyber-attack.

The only way we're able to do that work is in partnership with provinces and territories and, of course, they are responsible in the case of municipalities as well. We would be wide open to signing agreements with provinces and territories. We think Bill C-26, if it's adopted and receives royal assent, can be a model for some other provincial legislation that should be companion pieces to this federal legislation.

As colleagues would want, we're always looking to respect provincial jurisdiction.

[*Translation*]

This is certainly a priority for us. However, we won't shy away from being a partner and a leader or from sharing information, as long as it's safe to do so. We'll be signing agreements with the provinces specifically to enable us to share information.

That said, we acknowledge that urgent situations arise in areas of provincial jurisdiction. That's why I gave the example of Newfoundland and Labrador. At the time, the premier of Newfoundland and Labrador told us that the province was completely overwhelmed in terms of resources. He asked the Government of Canada to step in. Of course, we did everything possible at the time to help them resolve the situation.

[*English*]

Mr. Chris Bittle: Thank you very much.

Either of you might like to answer this question.

This bill is one piece of Canada's effort to improve cybersecurity. Can you comment on the pressing need to ensure we have programs and legislation in place to keep Canadians' information and critical infrastructure secure and what else, if anything, we're doing on that front?

Hon. François-Philippe Champagne: Actually when we look back, we've been doing a lot. The work of this government started back in 2013 with the establishment of the security review program. Then in 2018 we released the national cybersecurity strategy. In 2019 we saw significant investment, north of $100 million, to develop a critical cyber-systems framework. In 2021 we did the interdepartmental 5G security examination.

I would say what is very compelling is that in May of 2022 we indicated very clearly that it would no longer be Huawei or ZTE equipment in one of our most important networks, which is the telecom network in this country.

I think you've seen, at every step of way that, along with the Department of Public Safety, we have been trying to stay ahead of the game, because in matters of cybersecurity, malicious actors will always try to catch up, one way or another. We have been working with our Five Eyes partners, working with our G7 partners and working with allies around the world to make sure we identify the threat, we disrupt these malicious actors and we protect our critical network.

The piece we have in front of us is essential for Canadian businesses, particularly for the sectors that are being protected. I would come back again to the point that the telecom network is one of those, because with the Internet of things and 5G, this is going to be everywhere. That's why the work of the committee is so important today.

● (0940)

The Chair: Thank you.

We'll move to Ms. Michaud.

Go ahead, please.

[*Translation*]

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

The issues that often came up during the consultations held here in the committee obviously concerned transparency and privacy.

Some colleagues have already addressed these issues. According to the Office of the Privacy Commissioner of Canada, it might be a good idea for the government to consult the office before making any decisions on Bill C-26. Perhaps this would reassure Quebeckers and Canadians.

Obviously, Bill C-26 currently doesn't set out a time frame from when the government accesses personal information held by companies, for example, to when it deletes this information under the bill. We also know that there are many data leaks, and that the government isn't necessarily immune to these leaks either.

How can we strike a balance between the right to privacy and the highly confidential power grabs and orders?

Where does the balance lie in all this? How can you reassure Quebeckers, Canadians and SMEs?

Hon. François-Philippe Champagne: First, the powers granted are meant to ensure the security of designated systems. The objective is clear, and it's security. In the event of a cyber attack, which could affect everything from telecommunications and banking to the country's transportation network, you'll understand the urgent need to act.

It's just as urgent to take action when natural disasters strike or, to use the example of Rogers again, when 12 million Canadians don't have access to any payment system in the country.

For all these reasons, we're looking for the right balance. I understand the desire for consultation. Take the example of a cyber attack on 5G technology, which could affect all systems. If we were to publicize the details of the failure involving a player in the industry, this could encourage bad people to pounce on the breach. This would increase the systemic risk.

I think that we're trying to strike this balance. The proposed powers are tied to a clear security objective. Administrative law applies, along with judicial review and the Canadian Charter of Rights and Freedoms, for example.

[*English*]

The Chair: Thank you.

Mr. Julian, go ahead, please.

[*Translation*]

Mr. Peter Julian: Thank you, Mr. Chair.

The Auditor General's report on the ArriveCAN application speaks specifically about this bad practice for handling confidential information.

[*English*]

This is something we need to learn from.

On Bill C-26 we've had testimony from The Citizen Lab at the University of Toronto. One of the recommendations was that relief should be available if the government mishandles confidential, personal or de-identified information, and that the legislation should be amended to enable individuals and telecommunications providers to seek relief if the government has mishandled that information.

I'll direct this question to Minister LeBlanc.

Do you believe that it's appropriate that we incorporate into that legislation lessons learned from ArriveCAN?

● (0945)

Hon. Dominic LeBlanc: It is absolutely, because I, like all my colleagues and I think all Canadians, have taken notice of the Auditor General's findings. I was also briefed on other internal review processes before the Auditor General's report, and all of that makes me think that this is an opportunity to avoid exactly some of those concerns. We have explained the context in which these things were developed. It in no way justifies the financial circumstances around that or perhaps more importantly the protection of the personal information of Canadians.

If the committee has suggestions around an appropriate way to ensure there is a positive obligation on the Government of Canada to ensure that those circumstances identified by the Auditor General are never repeated, we would welcome exactly that kind of work.

Mr. Peter Julian: We also had a recommendation to prohibit the disclosure of personal or de-identified information to foreign organizations. That came from the coalition.

Is that a recommendation you support?

Hon. Dominic LeBlanc: I also took note of that recommendation. I would want to hear from some of the heads of our security agencies such as CSIS or the Communications Security Establishment on, as we said in a number of answers to colleagues' questions, the ability to effectively partner with allies, particularly the United States in this context. They have amongst the most sophisticated cyber-defence systems in the world. We need to learn from them. That does not mean we're callous or that we mishandle the personal information of Canadians. It would have to be subject to applicable laws and the Charter of Rights.

If the committee wants to look at that, I would make myself available. The committee will make its own decisions in terms of amendments of course. I am not an expert in determining the appropriate balance of sharing with foreign partners. I think we have to allow for some of that. We have to ensure that it's properly framed and that the right protections are there for the private data of Canadians. I think if we're going to undertake this effort successfully in terms of securing critical infrastructure, it will come full circle, because to some extent we're also securing the private data of Canadians that is held by private sector actors right now. I think of what my bank would have in terms of financial information on me or on any of us. They take that very seriously of course, but is there a way for the Government of Canada to partner with them?

It comes full circle. I'm looking at Mr. Julian, whom I've known for a long time. He will be concerned about the balance in that work, as am I. If the committee wants to find the right way to ensure that we get that balance, I'd be happy to work with the committee and to make sure experts who may have views much more informed than my own would be able to provide that perspective.

The Chair: Thank you.

Before we suspend, I would ask you to bear with us, witnesses. I appreciate you coming in here today with your teams.

Members, up next we do have witnesses, some of whom we have seen for a technical briefing and have asked questions to. We do have some committee business that the clerk needs to have verified by us as a committee. If you feel we've had enough questions relevant to this today with the ministers, I would ask for unanimous consent to allow the ministers and the next witnesses to leave so we can do our committee business and move on.

Is everybody okay with that?

Mr. Dane Lloyd: Mr. Chair, I would like to get just one quick round in with the witnesses. Then we can move onto committee business quickly.

The Chair: All right. We'll suspend for five minutes.

Thank you.

● (0945)

_____(Pause)_____

● (0955)

The Chair: I would like to welcome the additional officials who have joined us.

From the Department of Industry, we have Wen Kwan, senior director, spectrum and telecommunications sector; and Andre Arbour, director general, strategy and innovation policy sector.

We're going to go to about three minutes each, if we can. If we need to shorten it up, we will.

I will start with Mr. Lloyd, please.

Mr. Dane Lloyd: Thank you, Mr. Chair. I'll keep this really quick.

Thank you, officials, for coming.

There's been some concern by some of the witnesses that this legislation, while increasing costs to prevent cyber-attacks and preserve their cyber-infrastructure, will lead to a drastic increase in compliance costs.

If you know what the estimated increase in compliance costs for all the industries affected by this bill will be, can you tell this committee today? If not, I'd like to get a commitment that you would send that information to this committee before we start our clause-by-clause consideration.

Mr. Patrick Boucher: There's still a lot of work to be done through the regulatory process, and that's something that I think is foundational to this bill moving forward.

Mr. Dane Lloyd: But you don't have that answer right now.

Mr. Patrick Boucher: I will say that the cost of breaches to cyber-systems far exceeds—

Mr. Dane Lloyd: I understand.

I just want to know what those estimated costs are—

Ms. Jennifer O'Connell: On a point of order, Mr. Chair, in all fairness, at this committee the questioner asks a question, and you give a chance for the witness to answer. It's not right to cut them off.

The Chair: Mr. Lloyd.

Mr. Dane Lloyd: A yes or no question doesn't require that much time, Mr. Chair.

To the witnesses, I'd also like it if you could provide this committee with information on any estimates on the net increase in full-time equivalents that the government would possibly need to hire in order to administer the provisions under this legislation.

Do you have that information on you now? If not, can you commit to this committee to get us that information?

Thank you. That's my last question.

Mr. Patrick Boucher: Again, I think there's an extensive regulatory process that will be done, not only in partnership with industry but with provinces and territories, to further flesh this out and identify thresholds for how this act will apply to them.

This is a real partnership approach that we're taking here with stakeholders and with partners, and those are some of the details that we're going to have to work together with partners to identify.

Mr. Dane Lloyd: Can you get those estimates to us at least?

Do you not have economic modelling on what the red tape impacts, GDP impacts...? Do you have any of that modelling, and can you share that with this committee?

Mr. Patrick Boucher: There's no red tape impact being anticipated for implementation of this bill. This is about working with industry—

Mr. Dane Lloyd: There's no increase in compliance costs from this legislation?

Mr. Patrick Boucher: This is about working with industry to make sure that we're protecting critical infrastructure on which Canadians rely on a daily basis.

The Chair: Thank you.

We'll go to Mr. McKinnon, please.

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

Thank you to the witnesses for being here.

We've heard from witnesses who allege that this bill will result in government accessing, collecting and, most particularly, misusing personal information, including personal cell phone information.

Is that likely to happen, and why or why not?

I would ask Mr. Schaan.

[*Translation*]

Mr. Mark Schaan (Senior Assistant Deputy Minister, Strategy and Innovation Policy Sector, Department of Industry): Mr. Chair, I want to thank the member for the question.

[*English*]

With regard to the collection of personal information, as noted in Bill C-26, the minister has order-making powers that will allow him to be able to issue orders to protect the security of the telecommunications system.

There are two things that I think are really important to note. The actions and orders related to the minister's order-making power have to be connected to that security objective and ring-fenced in that regard. Similarly, there's a proportionality test that applies as a function of administrative law to the orders that the minister is making.

Two things that I think are really important to note as well are, one, that the Privacy Act continues to apply, both to the Minister of Industry and to the minister's officials through the department; and, two, that the Personal Information and Protection of Electronic Documents Act, PIPEDA, continues to apply to the telecommunications providers for whom order-making would be done.

There are privacy protections in place on both entities, both on the government side and on the private sector side, and there are limitations to the order-making capacities of the minister.

● (1000)

Mr. Ron McKinnon: Thank you.

We've heard a lot about protecting our infrastructure from malicious actors, but we also heard of the need to protect ourselves from natural disasters and so forth—forest fires and floods and whatnot.

Can you tell us how this bill might facilitate that effort?

Mr. Mark Schaan: I'm happy to.

[*Translation*]

Thank you for the question.

[*English*]

I think it's important to note that the telecommunications security objective, as the minister outlined, actually allows for a broad reach of application, in the sense that security is fundamental to a number of contexts. While we often think about that as related to cyber, in this particular zone I think we need to think about security in things like whether you can securely access the telecommunications system in the event of natural disasters, which are increasingly common.

The industry minister has order-making powers under Bill C-26, for instance, to allow for a telecommunication service provider to develop a security plan in relation to its services, networks or facilities and—

The Chair: Thank you.

Ms. Michaud, please.

[*Translation*]

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

I think that the public servants gave good information to the ministers of their respective departments. All my questions were answered.

I'll give up the rest of my time, because I want us to discuss the time available to submit our amendments.

[*English*]

The Chair: Thank you, Ms. Michaud.

Mr. Julian, please.

Mr. Peter Julian: Thanks for being here.

Earlier, I asked the question about NERC, the North American Electric Reliability Corporation, and the corresponding regulations. To what extent are the ministries reaching out to vital infrastructure associations like that to ensure we are not ending up in a compliance issue around the legislation and regulations that means a company or an entity might be pulled in two different directions?

Mr. Patrick Boucher: Through the development of this bill, there has been extremely extensive engagement with associations like the one you're referencing. That will continue through the regulatory process in establishing those regulations.

We also want to ensure we're engaging with provinces and territories to ensure for industry—possible entities that are subject to federal legislation like this, for example, and to provincial legislation—that there's harmonization within the implementation of those various laws. That's a commitment that I think is foundational to this bill and is something that we're going to continue to do through further engagement.

Mr. Peter Julian: When you say “harmonization”, are you suggesting, then, that the legislation or the anticipated regulations are being changed to some extent to ensure there isn't that duplication or contradiction between two different directions to assure cybersecurity? Or is the intent of the harmonization to get the other organizations to change their rules? Those are two very different approaches.

Mr. Patrick Boucher: I think it's to ensure that there is that harmonization, the first aspect you touched on, making sure that they're not contradictory to each other, that these organizations aren't being pulled in two different directions.

Again, this is more engagement that we want to do with provinces. It's something we've committed to through our engagement to date with provinces and territories and with industry to make sure that through the regulatory process we get it right for industry.

Mr. Peter Julian: One of the aspects of the legislation is immediate notification around cyber-attacks. There have been I think strong suggestions from a number of witnesses that there needs to be a clearer period.

Some are suggesting a 72-hour notification period, the objective being to respond to the cyber-attack to stop the cyber-attack initially, hopefully. They are suggesting that the reporting and notification requirements have become onerous, so that you're not able to handle the attack and you're not fighting back against the attack. If you're spending more time being concerned about following the letter of the law rather than responding to the cyber-attack, this can be a real difficulty.

How does the ministry define immediate notification? Do you agree with what numerous witnesses have said, which is that what we need is a clear period, but one that allows the organization, the company or the entity to stop the cyber-attack first before they have to engage in a notification?

Mr. Patrick Boucher: Yes, I would agree that there needs to be a clear period for reporting.

This is something that we've discussed through engagement to date and something that we want to identify through further engagement as we establish that through the regulatory process, again, balancing the need for making sure we're aware of the threat so that we could apply the expertise we have at the CSE, but also to warn other sectors, for them to be able to build resilience measures within their own infrastructure while also considering the realities that you just elaborated on.

Absolutely, I think we're going to have to be clear on that, and that's something we're committed to working on with partners to establish.

● (1005)

The Chair: Thank you.

Before we go any further, we have some administrative housekeeping that the clerk would like to get some answers on.

We talked about this at our last meeting. If the committee wishes to start clause-by-clause consideration of Bill C-26, on Monday, February 26, I recommend to establish the deadline for submitting amendments as Wednesday, February 21, at noon.

I know there was some conversation surrounding this, so I'll ask if that's still good.

Mr. Shipley.

Mr. Doug Shipley: Thank you, Mr. Chair.

After the study we've just done, and what was heard today, I believe there are a fair number of amendments coming forward. I think next Wednesday is going to be a little tight to get those in. If we can maybe bump those back to the Wednesday when we're back, that gives us next weekend.

We don't have as many resources as the government side. Everybody knows that. We're going to try to get ours in, too, but an extra week would be helpful.

The Chair: Madam Michaud.

[*Translation*]

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

My comment will tie in with my colleague's remarks. Our resources are also quite limited. Preparing amendments and verifying their compliance with the legislative counsel is time-consuming. There's a great deal of back and forth.

February 21 is less than a week away, which gives us very little time. Remember, we'll start studying the bill the following week. We'll then be in our constituencies for two weeks. I think that we'll need to hurry to get our work done. The bill will then be put on hold, since we'll be spending a number of weeks in our constituencies in March.

I propose that we have a bit more time to submit our amendments. It seems reasonable to give us an extra week, as Mr. Shipley suggested. In the meantime, the committee could begin its study on car theft.

[*English*]

The Chair: Thank you.

Mr. Julian, please.

[*Translation*]

Mr. Peter Julian: I agree with my colleagues.

We could start our study on car theft in a week and a half. By next Tuesday, we could submit the list of witnesses for Ms. Michaud's proposed study on car theft. We could set the deadline for submitting amendments for the following week.

I would like to suggest something for the following week. In the next seven weeks, there are just two sitting weeks. If we conduct our study on car theft next week, I suggest that the committee hold longer meetings to discuss the proposed amendments to Bill C-26.

Honestly, I find it difficult to discuss amendments for two hours and then to continue our discussion three days later. The amendments are often connected. I think that it would be more useful to hold a meeting from 3.30 p.m. to midnight, for example. If we did that, we could finish studying the bill that week. I'm talking about the second sitting week in March.

I propose that we hold longer meetings, extend the deadline for submitting amendments and start our study on car theft the week after next.

● (1010)

[*English*]

The Chair: Thank you.

Ms. O'Connell.

Ms. Jennifer O'Connell: Thank you, Mr. Chair.

While I appreciate the need for a little bit of extra time, I would hate to lose both meetings in our next week here. We have the 26th and 29th. If we want to start auto theft on the 26th, that's fine—and allow for amendments—but I wouldn't suggest that we lose the 28th as well. We need to keep in mind that there is only one sitting week in March, and one of those meetings we have already confirmed—the 21st—is with the minister on his mandate.

That essentially leaves us with two meetings if we're looking at February 28 and March 18. As we have heard from testimony even today, the threat is incredibly real. Everybody has agreed that this bill is urgent.

I would agree with Mr. Julian that we would support having later sittings, but I would suggest that amendments be in by February 26. That would allow the start of clause-by-clause on February 28. We could still start auto theft on the 26th for that specific meeting.

That's a compromise in terms of extending amendment dates but not losing both meetings in February. I would also suggest extended sittings.

The Chair: Mr. Shipley.

Mr. Doug Shipley: Thank you.

There are a lot of discussions going on about different dates. I think we need to get it clarified just a little bit.

We're going to put off doing the amendments for an extra week. Then, when we come back on the Monday, we're going to start on auto theft. Is that what I'm hearing, Ms. O'Connell? Then the Thursday of that week we will be into what? I'm sorry. Is it clause-by-clause?

Proceeding after that, then, would we go every other meeting, like we talked about, doing auto theft.

Ms. Jennifer O'Connell: That motion wasn't carried. I think we finish clause-by-clause as we would only have two sittings. I would take Mr. Julian's point that we extend the two days that we have. Then, once clause-by-clause is finished, we would continue on auto theft.

Mr. Doug Shipley: Thank you for that.

The only issue is that on some of those days.... Some of our members do sit on more than one committee, and they would have other committee work those nights, so I don't know if that would fall into—

Mr. Glen Motz: What I find rather interesting is that this has been on the books since June 2022, so we're 20 months into this, and now we want to rush through a process that we have heard many witnesses.... We also have significant recommendations to make in clause-by-clause to go through and fix this, and it's the responsibility of this committee to do that.

I don't know why there is the rush of an extra day or week or two to go through this. I don't support the extra length of meetings. We have other responsibilities as well, so I definitely don't support the need to sit extra.

I think we should get at the study on auto. When we're done with our recommendations and have them submitted, then we can go back and work on the clause-by-clause of Bill C-26. That, for sure, is going to take a lot longer than a couple of meetings of extended time.

Ms. Jennifer O'Connell: Security isn't that important.

Mr. Glen Motz: You guys have sat on it since June 2022.

The Chair: Mr. McKinnon.

Mr. Ron McKinnon: Thank you, Mr. Chair.

I certainly agree with Ms. O'Connell, and I support the extended sittings when we get to it.

With regard to Mr. Motz's concern that this bill has been tabled since June 2022, we should remember that it came to this committee in March 2023. Therefore, we have had it for just about a year, so any delay on this bill is really on us, not on the government.

It's a very important bill. We need to get going on it. That's why the extended sittings are critically important. It's not a matter of just delaying another week because we're going to lose most of March.

I think that once we start this bill, clause-by-clause, we should do it as soon as we can in keeping with Ms. O'Connell's suggestion. We need to take every meeting that we can to proceed with it.

● (1015)

The Chair: Mr. Julian, go ahead, please.

Mr. Peter Julian: Thank you, Mr. Chair.

I will say, in answer to Mr. Motz's comments about having other things to do, that every NDP MP—and I think it's the same with the Bloc—has four hats they have to wear. If we can find time to come here, I think Conservatives should be able to as well.

If what I'm hearing from my Conservative colleagues is that they are going to try to slow down or block the bill, that is different from our having good faith on all sides to actually proceed through. For example, if we have a meeting from 3:30 to midnight on Monday, when we come back that second week, we should actually be able to make real progress if there's good faith on all sides to improve the bill of course. But there is a difference between having an extended hearing with a filibuster and having an extended hearing at which we are systematically working through amendments.

We all agree that this bill has to be improved. I think in good faith we can do that the second week back. That would allow the first week back to be focused on auto theft. If we have agreement to have extended hearings during that second week, I don't think any party would object to doing two hearings on auto theft the week after next. But if we don't have agreement around having extended hearings in that second week, then I think the first week will become more problematic.

If we're all working together to get this bill improved and through committee and back to the House, then I think we have a game plan: two meetings on auto theft the week after next, a deadline for amendments the following week, and then when we come back we will have extended hearings, including potentially an extra meeting on Tuesday night to allow us to work through the amendments.

The Chair: Thank you.

Madam Michaud, go ahead, please.

[*Translation*]

Ms. Kristina Michaud: Thank you.

I would like us to recap our discussion on dates.

I don't think that it's a bad idea to extend meeting hours. That said, sitting until midnight seems a bit like a closure procedure.

I agree that we could do more over four or five hours, such as Monday evening from 4:30 p.m. to 8:30 p.m. or 9:30 p.m. I don't see any issue with that.

Mr. Chair, please confirm that we can set the date for submitting amendments for February 26, and that the February 26 meeting will focus on car theft.

At the meeting on Thursday, February 29, we would begin the study of Bill C-26. By then, the clerk would have already sent us the amendments proposed by the other parties, because we need to take time to study these amendments.

Since it will be on Thursday morning, we can't really extend the meeting. That brings us two weeks later, to Monday, March 18. I imagine that this meeting would be extended a bit. On Thursday, we would meet with Mr. LeBlanc.

We would continue the study of Bill C-26 on April 8.

Is that right, Mr. Chair?

[*English*]

The Chair: Thank you.

I will just note that the clerk has mentioned to me that on February 26 the amendments would have to be in by noon.

Mr. Shipley, go ahead, please.

Mr. Doug Shipley: Thank you, Chair.

There have been a lot of dates.

Mr. Julian, I think you had a good solution. I hope this is what you said. If not, correct me, please.

When we return, the first week back we would do auto theft on the Monday and the Thursday, and then when we return after that we could do the extended sittings. I think we can agree to that.

Mr. Peter Julian: It think it's a quid pro quo. If there is agreement to have extended hearings to go through the amendments on Monday and potentially Tuesday when we get back, then I think everyone would be in agreement with having auto theft for those two days.

Mr. Doug Shipley: Chair, I'm sorry, but just to sort of recap, it's a riding week next week. The first week back both meetings would be on auto theft, and then when we returned after that we would do extended sittings for Bill C-26. Is that what I'm hearing, Mr. Julian?

Mr. Peter Julian: That's what I'm proposing.

Mr. Doug Shipley: I think that's a good compromise. We would agree with that, Mr. Julian.

An hon. member: That's with the understanding that on the Monday that we're back—

The Chair: Ms. O'Connell, go ahead, please.

Ms. Jennifer O'Connell: Thank you.

Mr. Chair, I recognize the fact that there also needs to be time to review amendments, but if there are available hours even in that February 26 week, why wouldn't we ask for additional hours? We could still do auto theft in our regular meetings, but ask for additional hours if they were available.

We can do two things at once, but we'll leave it with you to figure out.

● (1020)

The Chair: Okay. As the chair, I will do my magic.

Mr. Dane Lloyd: I'm somewhat concerned about your magic.

The Chair: Maybe that was a poor choice of words.

Mr. Dane Lloyd: I think there's kind of an understanding, at least among the majority of the committee, that we want to do two auto theft days next week and then we would start using extended hours in March on Bill C-26. That's my understanding.

I just don't want to get surprised when the notice comes out, Mr. Chair, and we have a huge extended February meeting coming out of nowhere when it's not very clear that the committee has agreed to that.

The Chair: I think the chair has heard everybody's opinions, and I will take them into consideration when I sit down with the clerk.

Mr. Dane Lloyd: You know that when we don't feel as though we're being consulted or listened to, we have the penchant to act in certain ways.

The Chair: That's your prerogative, Mr. Lloyd.

Mr. Ron McKinnon: Mr. Chair, one thing we need to consider in our deliberations is that the legislative clerk will need time to go through the amendments. I think he'll need probably a couple of days.

The Chair: Mr. Shipley, go ahead, please.

Mr. Doug Shipley: Thank you, Chair.

Just quickly, since we're talking a little bit about the auto theft, we hadn't discussed which ministers would be attending for those hearings. We would like to suggest that the justice minister, the public safety minister and the transportation minister could all be invited if everybody on the committee agreed that those three ministers would be important to hear from on this important issue.

I think everybody would probably agree with that, Chair.

Mr. Ron McKinnon: We can invite ministers, but we don't necessarily know if they're available, right?

The Chair: Ms. O'Connell, go ahead.

Ms. Jennifer O'Connell: Thanks.

I think it's best not to make decisions on the fly. There was a motion that the committee agreed to, and we should stick to the details of that motion, and then, coming from that, if there are additional witnesses to be invited, the committee can do that. Just suggesting it here on the fly is not adhering to the motion that was passed unanimously by this committee.

I think that's the appropriate mechanism rather than just adding witnesses as members see fit when we've already gone over the time for committee. There's a process for this.

The Chair: Mr. Motz, go ahead.

Mr. Glen Motz: Thank you, Chair.

Just so we're clear, amendments are due on February 26. For February 26 and 29, the recommendation is to have the auto theft study. That is what the majority of the opposition side has come up with. Then on Monday, March 18 we would begin clause-by-clause of Bill C-26 with the idea that on that particular day, Monday the 18th if possible, we would extend those hours for a reasonable time depending on resources. I think that would be very reasonable, to begin Bill C-26 on that date.

The Chair: Thank you, Mr. Motz.

Mr. Julian, go ahead, please.

Mr. Peter Julian: I'm presuming that we have a deadline of Monday for auto theft witnesses?

The Chair: I think you've already submitted them.

Mr. Peter Julian: Thank you. I would suggest that if there were additional witnesses, they could be submitted by Monday.

The Chair: Thank you.

Okay. So leave that with the chair, please.

For Bill C-26, on Monday the clerk distributed the draft budget in the amount of $14,500.

Are there any questions or comments?

Mr. Chris Bittle: So moved.

The Chair: That is so moved. Perfect.

Now we'll get into a new travel budget regarding the study of the growing problem of car thefts.

As requested by the committee members, the clerk has prepared new travel budgets for the Port of Montreal regarding our upcoming study on the growing problem of car thefts in Canada. The request from the members was to reduce to a minimum the costs of the site visit. Two options were distributed by the clerk.

The first one involved a chartered bus in the amount of $8,199. The second one involved a chartered bus and a train in the amount of $9,399.

The clerk can provide additional context and information if it is required.

Go ahead.

● (1025)

Mr. Ron McKinnon: Mr. Chair, as a matter of form, the project was so moved, but we didn't vote on the budget.

That's all approved. Okay.

The Chair: As discussed with the clerk, I recommend that we adopt both budget options in order to provide flexibility in the next approval step before the Subcommittee on Committee Budgets of the Liaison Committee.

Are we good?

Some hon. members: Agreed.

The Chair: Is the committee in agreement to adjourn?

Some hon. members: Agreed.

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