HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

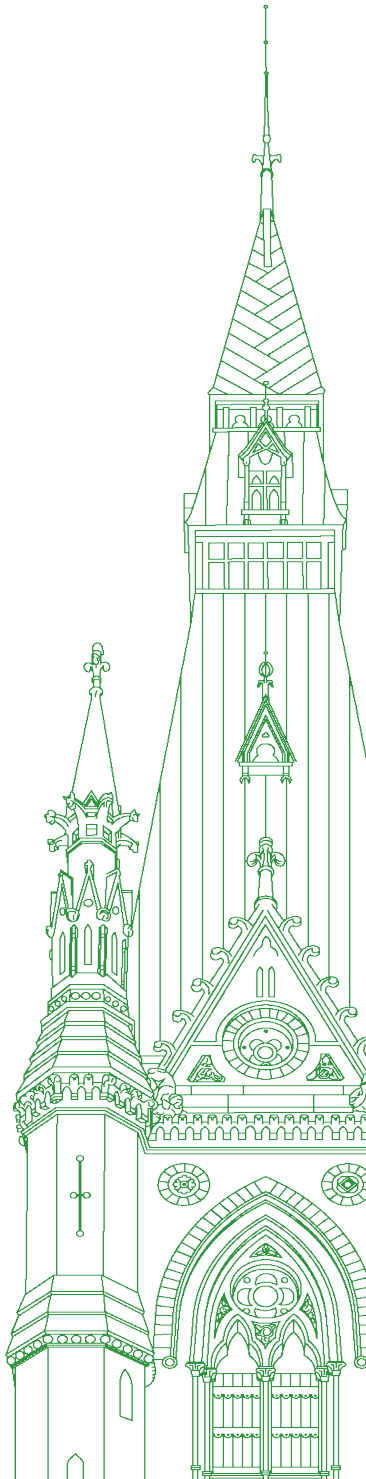
45th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 021

Tuesday, February 3, 2026



Chair: Jean-Yves Duclos

Standing Committee on Public Safety and National Security

Tuesday, February 3, 2026

● (1535)

[*Translation*]

The Chair (Hon. Jean-Yves Duclos (Québec Centre, Lib.)): I call this meeting to order.

Welcome to meeting number 21 of the House of Commons Standing Committee on Public Safety and National Security.

Before we begin clause-by-clause consideration, I would like to ask the committee to consider the two budgets members received from the clerk, distributed just a few hours ago and last Friday. The first budget in the amount of $31,500 is for the study of Canada's capacity to remove nationals with criminal records, and the second budget in the amount of $6,500 is for the study on the purpose of clause 371 (division 19) and clauses 380 to 385 (division 21) of Bill C-15, an act to implement certain provisions of the budget tabled in Parliament on November 4, 2025.

Please note that those are estimated amounts and that the committee may spend less than expected on these studies. Any unspent funds will be returned to the Liaison Committee. If there are any questions, we can put them to the clerk, who can answer them.

Is it the will of the committee to adopt these budgets?

Some hon. members: Agreed.

The Chair: We'll move on to the next item.

Pursuant to the House order of October 3, 2025, the committee is now meeting on its study of Bill C-8, an act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other acts. I would like to provide committee members with a few opening remarks on how we'll proceed with the clause-by-clause consideration of this bill.

As the name suggests, this is a consideration of all Bill C-8 clauses in the order in which they appear. I will call each clause successively, and each is subject to debate before moving to a vote.

If an amendment to the clause in question is proposed, I will recognize the member proposing the amendment so they can explain it, if they wish to. Amendments will be considered in the order in which they appear on the list committee members received from the clerk. Amendments have been given a number, indicated in the top right corner, to show which party submitted them. During debate on an amendment, members can move subamendments. Amendments and subamendments must be properly drafted in a legal sense, but they must also be procedurally admissible. The chair, that would be me, may be called upon to rule amendments inadmissible if they go against the principle of the bill, beyond the scope of the bill—both the principle and the scope were adopted at the same time as the bill at second reading in the House—or if they infringe the financial prerogatives of the Crown.

I thank the members for their attention, and I wish the committee and all its members a productive clause-by-clause consideration of Bill C-8.

I would now like to welcome the witnesses, who are here to answer questions, if necessary.

From the Department of Public Safety and Emergency Preparedness, we welcome Mr. Colin MacSween, director general, national cybersecurity directorate; and Ms. Kelly-Anne Gibson, director, national cybersecurity directorate. From the Department of Industry, we welcome Mr. Andre Arbour, director general, telecommunications and Internet policy branch; and Mr. Wen Kwan, director general, spectrum and telecommunications sector.

We will now move to clause-by-clause consideration of the bill. First, we're going to proceed more slowly to make sure we establish a dynamic and a pace that suits everyone. We'll begin, then, by calling clause 1.

Is it the will of the committee to adopt clause 1?

Mr. Ramsay, you have the floor.

Jacques Ramsay (La Prairie—Atateken, Lib.): We agree on the second part of the clause. It doesn't cover the impacts of lawful expression of opinion, persuasion or political debate, so we're fine with that.

What we don't like as much is the first paragraph—

● (1540)

The Chair: Mr. Ramsay, we are talking about clause 1. Soon, we'll get to the amendment you're probably talking about, the CPC-1 amendment, for which a notice has been filed and which deals with clause 2.

Jacques Ramsay: I apologize.

The Chair: It's confusing, because they both have the number 1. In this case, we're talking about clause 1.

Is it the will of the committee to adopt clause 1?

(Motion agreed to)

(On clause 2)

The Chair: Let's move on to clause 2.

Is there a proposed amendment for clause 2?

Mr. Caputo, you have the floor.

Frank Caputo (Kamloops—Thompson—Nicola, CPC): Thank you, Mr. Chair.

Thank you to the officials and my colleagues Ms. May and Ms. Kwan.

[*English*]

I am moving CPC-1, please, and I'd like to explain why. I'm mindful of the fact that we may not have agreement, but this is quite important to me.

The language in this bill carries not only a lot of responsibility but also an ability for the government to do a great deal of things. The language, in my view, is somewhat ambiguous in places. I know sometimes we get legislation that's drafted to catch everything and then our job, as legislators, is to bring it together.

We've heard all sorts of testimony, but I think when the courts go to interpret this, they will interpret the plain meaning. That's the basis of statutory interpretation. That's the start.

I'm greatly concerned that if we do not include that certain things are excluded—namely, appropriate speech, lawful expression, debate, persuasion—from the definition of interference and explicitly exclude the content of the communication from the definition of "telecommunications system".... It's my view that we need to narrow this down in order to clarify that we are only attempting to catch material threats to a telecommunications system. With the language we have now, we are casting too broad of a net.

I will listen with intent to what my colleagues from the Bloc and the Liberals say, because my hope is that we can come to an agreement, if they're not agreeable to this section, to carry out our intent.

Thank you.

The Chair: Thank you, MP Caputo.

Does anyone else want to intervene?

Madame Acan, go ahead.

Sima Acan (Oakville West, Lib.): Unfortunately, I am against that amendment.

One reason is that this amendment, to my understanding, attempts to clarify that "telecommunications system" does not include the actual content of information being sent and that secret orders cannot interfere with lawful expression. The experts are here as well. There's a technical danger behind this amendment if it goes through. This is highly problematic, because the definition of "content" is technically ambiguous. In a cybersecurity context, the technical signalling information, which is vital for monitoring system health, could be legally interpreted as content.

Furthermore, malicious code, such as malware or computer worms, is technically part of the data content and we cannot separate these two. If the government is prohibited from regulating anything classified as content, it will be legally powerless to stop these technical threats from moving through the systems.

The Chair: Thank you, MP Acan.

[*Translation*]

Mr. Ramsay, you have the floor.

Jacques Ramsay: I would agree with Ms. Acan. I would just like to move a subamendment to remove the first paragraph of Mr. Caputo's proposed amendment.

The Chair: Since this is a subamendment, we'll have to suspend the meeting for a few moments to make sure that everyone has the right information, including the clerks and legislative clerks.

I will therefore suspend the meeting for a few moments to make sure everyone gets a copy of the proposed subamendment.

● (1545)

_____(Pause)_____

● (1545)

The Chair: We are resuming the meeting.

Mr. Ramsay, just to make sure everyone clearly understands, do you want to explain again the nature of your subamendment?

Jacques Ramsay: The amendment proposed by Mr. Caputo has two paragraphs. We're proposing to completely remove the first paragraph and simply keep the second paragraph.

The Chair: Okay.

[*English*]

I think it's fairly clearly stated. The subamendment is to remove the first paragraph of the amendment.

I'll now turn to MP Caputo, and then to MP Lloyd.

Frank Caputo: I'll let MP Lloyd go first, please.

Dane Lloyd (Parkland, CPC): Thank you.

The claim was made by my colleague, Ms. Acan, that it would create a technical risk if proposed section 15.01 were included, because we would be saying that we can't deal with any of the content.

I just want to ask the officials, can you provide some background for that?

Andre Arbour (Director General, Telecommunications and Internet Policy Branch, Department of Industry): Thank you for the question.

The language refers to "the content of the intelligence that is emitted, transmitted or received", so it's not referring just to content in a generalized, colloquial sense.

The other thing is that it further.... I don't think this is the intent of the amendment, to be clear, but in conjunction with proposed section 15.02, which is very clearly about speech issues.... Normally, you don't have text added unless it's there for a purpose. Proposed section 15.01 has, very much, the risk of communicating that it's actually not about speech, because that's what proposed section 15.02 is about, so proposed section 15.01 is about something different, presumably.

When we get into the content of the intelligence, in terms of what is actually being transmitted, in a technical sense it's all zeros and ones, ultimately, with how it gets converted into signalling. When we're talking about the actual intelligence that's being transmitted, some zeros and ones could be malware, and some zeros and ones could be expressive speech. The telecom act already does not allow for government control of expressive speech. That has no bearing on the telecom act, so it's already not captured.

I totally appreciate the concern for greater certainty, but that is the reason why.... Proposed section 15.02 is just consistent with the overall scheme.

Dane Lloyd: Thanks.

The Chair: Thank you for that.

Do you have any other questions or input, MP Caputo?

Frank Caputo: Thank you very much for that.

Now, I think I understand your concern. Is there any way that proposed section 15.01 could be tweaked—to use the colloquial term—in order to not run afoul of the issues you just mentioned?

● (1550)

Andre Arbour: We struggled, and part of the issue is that it's in conjunction with proposed section 15.02, which already gets into the issues of speech. We couldn't think of an alternative formulation that wasn't already captured by proposed section 15.02 in some shape or form.

Frank Caputo: To be clear, proposed section 15.01 is nugatory, unnecessary, in your view. Just to be very clear, proposed section 15.01 is unnecessary, given proposed section 15.02, and proposed section 15.02 gets us to the point that we are trying to get to, given my prior intervention. Is that accurate?

Andre Arbour: Yes. The telecom act doesn't allow for regulation of speech. However, to provide for the greater certainty that you're seeking, proposed section 15.02 absolutely spells that out in plain language. It's just that, when you add proposed section 15.01 on top of that and the specific wording of proposed section 15.01, then you have issues.

Frank Caputo: Could I just have one moment, please?

The Chair: We'll suspend for just a second to give the MP the time needed.

● (1550)

(Pause)

● (1550)

[*Translation*]

The Chair: We are resuming the meeting.

Is there any further debate?

[*English*]

Are there any other questions, input or arguments?

MP Caputo, go ahead.

Frank Caputo: We may be able to deal with the amendment. I don't know if we need a recorded vote, or on division, and then to move to the main amendment.

The Chair: Okay.

Is there any other input? I see none.

(Subamendment agreed to on division [*See Minutes of Proceedings*])

The Chair: This brings us back to the amendment.

Is there any other input on the amendment as amended?

[*Translation*]

We will systematically do recorded votes to make sure the vote count is in the record.

We'll take the recorded vote on the amended version of amendment CPC-1.

Is it the will of the committee to adopt the amended version of amendment CPC-1?

(Amendment as amended agreed to: yeas 9; nays 0) [*See Minutes of Proceedings*])

● (1555)

The Chair: This brings us to another amendment.

Is there a mover for amendment CPC-2?

Mr. Caputo, you have the floor.

Frank Caputo: I move amendment CPC-2.

[*English*]

I will speak to this amendment, which is really critical, in my view.

Before I begin, I think we can agree that the act provides substantial power to the minister. At the end of the day, though, that power has to be checked, and there really are a couple of ways to check it.

What the act does now is an *ex post facto*, or after the fact, review. In other words, there is a method to judicially review the act and when that happens, a judge says that, yes, the exercise of authority under the act was appropriate or, no, it wasn't, but that happens after.

My position, our position, is that the review, where possible, should occur beforehand. In other words, when there is time to get judicial authorization, then judicial authorization should occur, so that the exercise of considerable power is not just reviewed; it is at the outset conferred upon the court, which is independence. In that case, when there is an opportunity to do so, we will have an assurance that an independent body has reviewed the ministerial proposal and what is proposed to be done pursuant to the act, and they can give a thumbs-up or a thumbs-down. I think that is actually much more prudent than reviewing it after the fact.

We review things after the fact in this country all the time. As we have recently seen.... Sometimes we do see it and sometimes we don't, but sometimes we see that mistakes are made. I think we should actually be trying to address those mistakes before they are made.

There is one thing I would like to ask the officials, and I hope I spoke clearly on this. Could a clause like this work in conjunction, perhaps, with some sort of *ex parte* requirement wherein if it isn't practicable, if time is of the essence...but where it is practicable, we could address it through this sort of judicial authorization?

I'd love to get the officials' input on that, please.

[*Translation*]

The Chair: I have to cut you off, Mr. Caputo.

[*English*]

I have a ruling to make before we open up the debate on CPC-2.

[*Translation*]

As you know, Bill C-8 amends the Telecommunications Act by giving new powers to the Governor in Council and the minister to issue orders under subsections 15(1) and 15(2).

The purpose of amendment CPC-2 is to amend the bill by requiring that the Governor in Council and the minister obtain legal authorization before issuing these orders, which could be subject to court-imposed conditions.

As stated in section 16.74 of the *House of Commons Procedure and Practice*, fourth edition: “An amendment to a bill that was referred to a committee after second reading is out of order if it is beyond the scope and principle of the bill.”

It is the chair's opinion that the introduction of judicial authorization prior to the issuance of orders is a new concept that goes beyond the scope of the bill. Therefore, I rule this amendment inadmissible.

Mr. Caputo.

[*English*]

Frank Caputo: With the greatest of respect, Chair, I would like to challenge your decision.

Thank you.

The Chair: Thank you, Mr. Caputo.

There is a challenge to the decision of the chair, which brings us to an immediate vote.

(Ruling of the chair overturned: nays 5; yeas 4)

● (1600)

[*Translation*]

The Chair: The chair's ruling has been overturned, so we'll begin the debate on amendment CPC-2. Are there any members who wish to speak?

Ms. Acan, you have the floor.

[*English*]

Sima Acan: Thank you, Mr. Chair.

Yes, I do have some comments.

As we all know, during the committee's studies we have heard several times from the experts in this field that cyber-threats move at digital speed, often requiring immediate mitigation. Requiring a judge to sign off on every technical order would definitely cause major delays in the government's ability to respond, especially to an active attack. By the time a court application was processed, damage to telecommunications systems could be irreversible.

The Chair: Do you have a point of order, MP Caputo?

Frank Caputo: Yes. Are we dealing with an amendment here?

The Chair: Yes.

Frank Caputo: Which amendment was moved?

The Chair: It was CPC-2.

Frank Caputo: I thought you just ruled it out of order.

The Chair: Yes, except that my decision wasn't sustained.

Frank Caputo: Oh, it was not sustained. Oh, my gosh. I am so sorry.

The Chair: Do you regret voting against me?

Frank Caputo: I thought Madame DeBellefeuille voted yes. I am sorry.

I'm sorry, Ms. Acan. I apologize for interrupting you.

Sima Acan: No problem, Mr. Caputo.

That gives me the chance to repeat my sentence.

Again, cyber-attacks move very fast, and in most cases when there's an active attack, the government will not have the chance to move forward while waiting for the court's decision. At that point, by the time a court application was processed, the damage to telecommunications systems could be irreversible.

Additionally, it would also create significant new burdens on the Federal Court. That's the legal side, but I'm more concerned with the technical side. That's my point.

Thank you.

The Chair: Thank you, Madame Acan.

Let me turn to MP Caputo.

[*Translation*]

Frank Caputo: Thank you, Mr. Chair.

[*English*]

To the officials, I think I had asked a question, and then we did a vote. Are you in a position to answer that question? I think it's very important, given what Ms. Acan said.

I understand that things move quickly. We are not talking about criminal law, but in criminal law we have the principle of exigency, which is a term that means it's impracticable to get an authorization. Is it possible to have this amendment with something that would go along with exigency? Does that make sense, the principle of it?

I invite officials to comment on that, please.

Andre Arbour: Under criminal law, there's a very substantial body of law and practice and procedure for specifically how to involve the courts, and involve them for a very good reason, because fundamental human rights are involved in searches, invasion of privacy, search and seizure or arresting someone. We're talking about very serious issues. There's a huge body of law that makes it very easy for a judge.... Well, “very easy” is too simple, but specific, defined criteria make it much more straightforward for a judge to rule yea or nay.

In the current context, we are talking much more about either policy issues or technical issues, as opposed to legal issues. The courts do not have that kind of expertise. They do not have a staff of engineers, like my colleague here, who can advise them on these issues. We are talking about new issues. We are talking about activities that the court is not used to dealing with.

For instance, the Minister of Industry is currently the spectrum regulator. They administer the Radiocommunication Act. This includes authorizing all wireless services within Canada for use, managing 150,000 spectrum licences and 35,000 different entities across Canada. That's just the spectrum management piece, and that's under the minister's authority, but ISED is fundamentally supporting that work.

We're talking about something much more similar when we're talking about the provisions of Bill C-8. We're talking about technical management of network infrastructure. Here, there are going to be a whole bunch of novel issues for a court. They're going to be non-legal issues in most cases, and the court will not have the expertise to deal with them. Maybe as a basis of comparison, the Goldtv case before the Federal Court in 2019 might give an indication. That had some novel issues. It was a copyright infringement case that involved a network management site-blocking issue. It was uncontested by the site that was being blocked, but it still took five months for the court to come to a decision.

That was over copyright infringement, which is much more well defined. Injunctions around copyright infringement are a more common activity before the court, but this is going to be much more novel, much more far-ranging and much more outside the court's normal remit.

● (1605)

Frank Caputo: I'm going to push back a little bit, and here's why.

Judges often aren't experts. I know a lot of judges. I taught with a judge. They frequently rely on submissions of counsel or information in an affidavit. What this would do is require somebody, on oath or affirmation—which is serious, since you could commit perjury if you stated something falsely—to say that the test is met, and why the test is met in section 15.

I'm not trying to be combative here with you. I'm just trying to express myself to say that a lot of times judges have to deal with complicated material. When somebody under oath or affirmation says, “These are the requirements under the act. This is the threat. This is the action we propose to take, and this is why”, I don't think a judge has to be an expert. They have to say, “Is the definition of threat or material threat met? Is this information reliable?”, and things like that.

Just because we haven't done it before and this is new, I don't find it persuasive, to be very candid, to say that we shouldn't be entertaining this, and here's why. This is new legislation. These are sweeping powers, and I'm mindful of the fact that in the G7, this is a requirement. Nobody, I think, wants to say that we invite threats to our telecommunications. Of course not. We just want to get the best legislation, legislation that balances the privacy rights of people and the safety of our critical infrastructure, and anything in between.

Given that, I guess I just don't see why a judge would have to be an expert on this, when they're simply evaluating whether the law is met, and somebody under oath or affirmation would be stating why.

Am I making any sense here?

Andre Arbour: When a court is reviewing the reasonableness of a decision, in my experience and in various aspects of judicial review of decisions, they do not take the government's word as a given. They will want to evaluate the facts of the matter. It's a very lengthy process for them to come to a decision when they want to make sure they understand the contested facts of the issue. It's in the order of 12 to 18 months for those types of things.

I would also flag that given that this is at heart a regulatory process, there is already a set of guardrails to allow for the scrutiny through the development of the order-making process. For stakeholders to provide their views, there is guidance within the act in terms of how to scope and what's an appropriate use of those powers. There's a requirement that orders must be reasonable in relation to the gravity of the threat. You can't do something excessive in response to a minor issue.

Then again, to evaluate the reasonableness, you need to get into some analysis of facts, typically, and that means understanding the subject matter. Certainly, judges will absolutely get up to speed when they have a matter before them in their court, but it typically takes quite some time to do so.

Frank Caputo: Thank you.

I guess where you and I part company on this issue is on the necessity of a judge reading something that ideally would be provided in plain language to them and that would say: “This is what we're doing, this is why we're doing it, and I swear or affirm these are the facts.” In the analysis you just provided, Mr. Arbour, where you talk about the checks and balances, those are all after the fact. What I'm looking at is something that occurs before the fact. I know that you take no position. I'm not trying to put words in your mouth as to the position you're taking. I'm simply commenting on what you've just advised.

We may be at a standstill at this point. I'll let others intervene.

Thank you.

● (1610)

The Chair: Thank you, MP Caputo.

MP Ehsassi.

Hon. Ali Ehsassi (Willowdale, Lib.): Thank you, Mr. Chair.

I genuinely find this very fascinating. I have to say I agree with Mr. Caputo that it could very well be that someone sitting on the bench is not familiar and does not have the expertise, but there's always a way around it, as Mr. Caputo has rightly pointed out. That's not the source of my concern.

The source of my concern is the issue that MP Acan has actually identified, which is that, on occasion, given the speed of these challenges, you need to act with alacrity. You need to do it as expeditiously as possible. On that specific issue, I would say that I wholeheartedly agree with Mr. Arbour, because, practically speaking, it would take quite some time for this process to play out. There's no doubt in my mind that this would be the case.

The other issue is that in the event that any minister does overstep their authority or does not act on a legitimate basis, the remedy, as Mr. Caputo does know, is that you can bring a claim later, but let's not get into this process of handcuffing the hands of our authorities when there is something imminent that is about to occur.

It's a very interesting debate that's going on, but I would say that practical considerations lead me to believe that perhaps we would be ill-advised to go with Mr. Caputo's amendment. I'm not quite sure how Mr. Caputo sees that.

[*Translation*]

The Chair: Thank you, Mr. Ehsassi.

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ): Thank you, Mr. Chair.

I can already tell you that I support amendment CPC-2. I've been thinking a lot about the implications, given all the witnesses we've heard from. One of them, the Honourable Simon Noël, the intelligence commissioner, made a presentation that really resonated with me. He also made two recommendations to the committee, one of which was to use warrants to limit ministers' powers. That stuck with me, because I have a great deal of respect for Mr. Noël's career, and I thought his judgment was very sound.

I continued to ponder this knowing that numerous bills adopted by the new Liberal government give a lot of powers to ministers, and I have a problem with that.

Yes, we are studying Bill C-8, but when I look at the powers Bill C-15 will give ministers and the laws it'll suspend, I wonder about the whole basis of granting power to ministers without specific restrictions.

What bothers me in this case is that I know the Royal Canadian Mounted Police, the Canadian Security Intelligence Service and police forces think the requirement of a warrant would hinder intelligence sharing. We also wonder how to strike a balance between intelligence sharing and privacy protection. Perhaps requiring a warrant would provide some safeguard.

The reason I agree with this amendment is that we proposed amendment BQ-15, which would allow for a reassessment of the legislation in five years to see if we were right to insist that a warrant be obtained and whether we should revise the legislation. If it turns out to be a disaster, I think the government could quickly react with legislative amendments.

The fact that the National Security and Intelligence Review Agency's budget, the only body that monitors agencies, the government and ministers to ensure their compliance with the law, was dramatically cut isn't really reassuring. On the one hand, the government decides to give more power to ministers, but on the other hand, it takes powers away from those who have the authority to investigate. Those decisions are incompatible and inconsistent.

It might have been more convincing if the government had said it was increasing the agency's budget and giving it the means to investigate. Instead, it's imposing significant budget cuts on the agency, limiting its ability to investigate.

I would also say that I followed the entire trial on the government's decision to invoke the Emergencies Act. As you saw, two courts later ruled that it was a bad decision.

Taking all that into consideration, since this is a new bill, I think it would be wise to rein in the ministers' powers by requiring warrants be obtained. If it's a disaster, I trust the government to call us back to make legislative amendments or corrections, since it can do that at any time. For now, I'd be more careful. If it doesn't work, we'll consider amendments or corrections, or the government can table another bill.

That would be my motivation. I don't trust the current government, because in many instances, it has given a lot of power to ministers and suspended legislation, and even citizens' rights. Bill C-15 suspends the rights of Mirabel residents who will be expropriated. They won't have the right to challenge or negotiate their expropriation. It's as if we're dealing with an authoritarian government that suspends laws as well as citizens' rights. I don't trust this government. I can't give it carte blanche on Bill C-8.

I've shared my thoughts with you on the matter and I hope amendment CPC-2 will be adopted. If the process doesn't work, I trust the government will call us back so we can make amendments by providing very clear examples and reconsider our decision.

● (1615)

That said, for the time being, I'd prefer to keep that part.

The Chair: Thank you, Mrs. DeBellefeuille.

Mr. Lloyd, the floor is yours.

[*English*]

Dane Lloyd: Thank you.

Thank you to my colleague for her excellent intervention.

To the officials, are you aware that the "Communications Security Establishment Canada Annual Report 2024-2025" states that the CSE disrupted ransomware groups targeting Canadian critical infrastructure within 48 hours using the existing tools at their disposal?

Andre Arbour: I didn't have that specific example in mind, but that is a very different set of circumstances from anything that is contemplated under part 1.

Dane Lloyd: I just find it interesting. My colleague Ms. Acan raised a very good point. If we bring in this judicial authorization, there's a concern that it might delay the government's ability to take action to stop malware, yet in 2024, the Communications Security Establishment of the Canadian government was able to disrupt malware within 48 hours. It didn't require judicial authorization. They already had the capability of intercepting threats to our critical communication systems.

If this legislation was not in place in 2024, I wonder how the Communications Security Establishment could have been able to take that action to prevent that from happening, as has been claimed by the government.

Andre Arbour: I'm going to start, and my colleague may supplement.

First, part 1 involves regulatory obligations on the private sector. If CSE says that there's a problem and that they recommend we patch our system, then that can be done incredibly quickly, and it's voluntary.

If we are talking about a legal obligation on the private sector, it has to go through an existing set of procedural requirements to come to that. Judicial review of those types of decisions takes 12 to 18 months, so there is a very high risk that, if this amendment were to be adopted, the powers under this act would be inoperable—not practical to be implemented—to a degree that makes me very concerned.

● (1620)

Dane Lloyd: Just to follow up on that, it's been referenced in testimony that stakeholders involved with this would be consulted if these powers were going to be used on them. In the case of a serious imminent threat to our telecommunications system, as Ms. Acan brought up, how quickly would you be able to go through the entire process of consulting all of the stakeholders and making a regulatory order? That doesn't seem like a very quick process. It seems to me that the process could be carried out alongside seeking a judicial authorization, if it was an urgent case.

What are your thoughts on that?

Andre Arbour: It's true that any consultation will have to be over an appropriate period of time for us to solicit feedback, and—

Dane Lloyd: Can you give an example of an appropriate period of time?

Andre Arbour: It will depend on the circumstance. If we go through, for instance, something that's quite broad in scope, such as the use of a particular high-risk vendor's equipment that's broadly used throughout the industry, we will publish either a draft order or a public consultation paper on our website.

[*Translation*]

The Chair: I apologize Mr. Arbour.

Mrs. DeBellefeuille, are there issues with interpretation?

Claude DeBellefeuille: Mr. Ehsassi is a bit loud, so I'm having a hard time hearing the interpretation.

The Chair: Okay. That's because of the noise in the room.

[*English*]

I'm sorry, colleagues. I hate to do this, but I have to call everyone to order, in a noise manner.

I'll go back to you, Mr. Arbour.

Andre Arbour: Just reverting back to the example, there's a broad range of stakeholders implicated. Our default consultation, in basically all circumstances when we're talking about this type of thing, is just to publish something publicly on our website, just in case we miss someone, and to consult that way. Generally, that's carried out over a period of months. It will depend on the precise set of circumstances and the exigency.

Dane Lloyd: It won't be the same amount of time in an extreme circumstance, as Ms. Acan brought up.

Andre Arbour: If we're talking about something simple—for instance, one operator has a vulnerability in one piece of their network, but it's a serious one—it could be a question of a day or a couple of days.

[*Translation*]

The Chair: Thank you, Mr. Arbour and Mr. Lloyd.

Mr. Ramsay, you have the floor.

Jacques Ramsay: It's important to take a step back and look at the initial reason for this amendment. It was written with a particular focus on privacy and charter rights issues, issues that usually warrant judicial review and authorization. Now that it's been clearly established that this is not the case here, we are talking about orders relating to the security and technical operation of communications networks.

Given that cyber-attacks can happen at any time, even in the middle of the night, as in Mr. Lloyd's example, 48 hours is a very long time. Moreover, rarely is a judicial authorization mechanism used to regulate private sector businesses. I'd like to hear the experts on this: Why would we need such a process when there is normally no such process to regulate private enterprise?

Andre Arbour: Part 1 of this massive bill is about regulating the private sector. This means it affects Bell's network operations and the way Bell, Rogers and Telus manage their network.

● (1625)

[*English*]

I cannot think of a comparable example of having courts substitute for a regulatory authority as a matter of daily course. It is just extremely unusual and outside the norm of how regulations are made in Canada or in any OECD country that I am aware of.

The existing regulation of the telecommunications sector via the Telecommunications Act or the Radiocommunication Act is done via regulatory means and not via the court. All other federally regulated sectors in Canada, including energy, banking and transportation, are regulated through a regulatory process and not through a court process. You involve the courts in an *ex ante* fashion when you're dealing with charter rights, which is fundamentally not the scope and substance of what part 1 is dealing with.

[*Translation*]

Jacques Ramsay: Mr. Caputo says a quick process is possible. You just named Telus and Bell, among others, and as far as I know, they're dealing with major contentious issues and have some of the best lawyers.

Hypothetically, is it possible they won't agree in this case and choose to wage a long legal battle?

Andre Arbour: Telecommunications service providers such as Bell, Telus and Rogers have considerable resources and teams of lawyers. The telecommunications sector is already very contentious and players use the judicial process, because that's an available tool in a regulated sector. They're well positioned to challenge any government regulatory proposal. In the vast majority of cases, difficulties and issues are identified during the consultation process. If the government and Bell, for example, disagree, Bell can certainly challenge the proposed regulation.

Jacques Ramsay: Does the legislation of any other Five Eyes nation give this power to get consent from the court? Is Bill C-8 aligned with what we see in other countries?

Andre Arbour: In every case I can think of, a regulatory process was adopted rather than a judicial process. Honestly, I've never had to consider such a huge measure. I apologize if I wasn't clear, but it's really through a regulatory process that OECD countries deal with private sector regulatory issues.

At the beginning of the Telecomunications Act and in the specific powers described in part 1, there are measures to require consultations, as well as guidelines for the government, to frame the powers provided by the act. Also, there are oversight measures for parliamentary agencies and committees, as well as the possibility of launching a legal process later on.

However, the use of a judicial process to regulate the private sector on a daily basis would be exceptional compared to OECD standards.

● (1630)

Jacques Ramsay: So, if I understand you correctly, we would be going it alone and would be completely different from other countries.

I don't want to get ahead of myself. However, other amendments will be moved later to regulate the powers of the Governor in Council and the minister. These amendments would limit the powers and would allow for proper regulatory control. Do you agree with this and with the inclusion of the concept of proportionality and necessity in the legislation?

Andre Arbour: Yes. There are already measures to regulate the powers stemming from the bill. However, amendments are also being moved to add criteria for issuing confidential orders, for example, as well as measures to further regulate the power to disconnect a company in the event of a cyber-attack. So, the committee could consider other measures to better regulate the powers.

The Chair: Thank you, Mr. Ramsay.

I'll suspend the meeting for a few minutes. I believe that discussions are taking place around the table and in other areas. After the suspension, if the members don't mind, we'll get back to the speaking order before me. The order is as follows: Mr. Au, Mr. Strauss, Ms. Acan and Mr. Powlowski.

● (1630)

_____(Pause)_____

● (1645)

The Chair: I call the meeting back to order.

I'll make an exception to the rule. Normally, Mr. Au should speak. However, Mr. Caputo asked me for a few moments to summarize some of the discussions.

Mr. Caputo, the floor is yours.

[*English*]

Frank Caputo: Thank you, Mr. Chair.

This is what we have discussed. I want to be abundantly transparent. I invite any of my colleagues, from other parties or my own party, to chime in if I misstate anything. This is what I would propose. I propose that we vote on CPC-2. If CPC-2 passes, the officials have advised us that there will be situations of exigency, which is the term I've used, when judicial authorization is impracticable to obtain. In other words, there's no time to obtain that. That is my understanding of their recommendation. What we would then do is that I would ask that the drafters draft an amendment to that effect. We would then consider that amendment as part of new proposed section 15.201—perhaps new proposed subsections 15.201(3) and 15.201(4), if necessary—and vote on that amendment in the future.

Right now, though, we are voting on CPC-2. If it passes, we would give instruction for a draft on what I call exigency. Then everybody can deal with what they need.

Am I clear? In other words, I think we should vote on CPC-2 now and then give the instructions.

● (1650)

[*Translation*]

The Chair: I'll suspend the meeting again for a few moments.

● (1650)

(Pause)

● (1650)

[*English*]

The Chair: This is what I was suspecting: It wouldn't be possible to go back to an amendment that was adopted unless there was unanimous consent to revert to that amendment. It's the decision of the committee later on, when it comes to a vote on CPC-2, to consider that option.

Having said that, MP Caputo, is there something more you want to add on that?

Frank Caputo: I want to clarify it.

The Chair: Go ahead, please.

Frank Caputo: What I'm saying is that we vote on CPC-2 as is. It is closed. Then the drafters draft an amendment about exigency. That might be CPC-38. It would be a new amendment. We wouldn't be reopening CPC-2. We would be considering a different amendment, but that amendment would be about new proposed section 15.201.

Am I being clear here?

The Chair: Yes, except it depends on where we will be at that time. We will probably be later on in the process. Being later on in the process, it's impossible to revert back to an amendment that would have been voted on.

Frank Caputo: I see. Okay. You're talking about the clause, not the amendment. We will already have gone past clause 2.

In that case, yes, I can say that we would give consent to come back to that in good faith.

The Chair: Okay. That's for MPs to decide in terms of the usefulness and validity.

Having heard that, let me follow the suggestion of MP Caputo to continue the debate on CPC-2.

I have MP Au, MP Strauss, MP Acan and MP Powlowski.

MP Au.

Chak Au (Richmond Centre—Marpole, CPC): I just want to ask, in practical terms, how difficult or how easy it is to get the authorization. As a layperson, I can see that there's a difference between authorization and the application for a warrant. For a warrant, perhaps it could take more steps or a higher threshold. Authorization can be much easier and simpler, perhaps just a certification saying that the minister has considered the need for this kind of action. Then it could be approved. I can also draw reference to when a police officer is trying to get into a home to search. I think they can get a warrant quite fast. It doesn't take days and hours for them to get it.

Practically, then, how difficult is it to get this authorization?

Andre Arbour: In the context of the Criminal Code, there are considerable, very detailed criteria for the different types of circumstances in which law enforcement might be engaged with that. There are many decades of precedent about how the charter is applied in those circumstances. Today, yes, it's relatively straightforward, but it's based on decades of hashing out the details and lots of detailed practice. It's an activity that the court is designed for.

What we are talking about here involves, generally, determinations of fact and not law. What that means is this: What is the nature of the threat? How much equipment is it implicating? How easy is it to remedy that issue?

This is fundamentally a policy or a regulatory process. There are no criteria to instruct the court on how to consider this matter. It is completely unique. There is no precedent for it that I can think of—not just in Canada, but in any country—to guide the court in terms of how to apply it. It involves fundamental questions of fact, which means the court would need to be briefed, get up to speed and understand the technical details, which they certainly can do, but it's why, typically, these judicial processes take six to 18 months.

The other thing I will say is that I know there's been a focus on exigency, but to some degree, I'm almost as concerned about all of the routine activities we need to do when we think about how we regulate the telecom sector as it is. When the service providers end up in court, which happens from time to time—again, it's very rare in the grand scheme of the total number of regulatory actions we take; we have around 150,000 licences out in the field on just the spectrum part alone—we are talking about a year or a year and a half.

● (1655)

Chak Au: Thanks for the answer.

The Chair: Thank you, MP Au.

MP Strauss.

Matt Strauss (Kitchener South—Hespeler, CPC): It's fine.

The Chair: Okay.

Let me turn to MP Acan.

Sima Acan: Thank you, Mr. Chair.

We all respect the role of the judiciary. However, I still see this amendment as detrimental. It prioritizes red tape over national resiliency, especially when we look at the global situation now. We talked about how cyber-threats move in milliseconds, and we repeated that several times. We also know, especially because we have lawyers sitting here, that court applications can take days or hours. They may be too late to stop the attack in the moment.

This amendment would also place a massive administrative burden on our Federal Court—I keep repeating that—by forcing our judges to act as technical clearing houses for every instance and every security order. I believe we do not need to create a new hurdle that slows down our national security processes, because as we heard again and again, the status quo already provides judicial oversight. That's one point that we spoke about today.

Again, with the amendment as is, I see it effectively handcuffing our ability to defend our country. To me, in my heart, it's very important, and it is against instant attacks. I would ask my colleagues to consider the security of our provinces and our country when we think about this amendment.

I want all of us to understand the situation from the technical perspective as well. We mentioned several times at the industry committee, as well as here, that the damage to our companies is in the millions of dollars. Overall, it's billions of dollars. That's our future money.

I would like to ask the experts to help us understand this better. Could you please give us some concrete examples of the malware and worms we are discussing here that are threats not only to our telecom infrastructure, but to our critical infrastructure? What are the potential implications that we can face as a country, especially if we go through really difficult times in the future?

Andre Arbour: Thank you for the question.

Salt Typhoon is a threat actor affiliated with a foreign jurisdiction that infiltrated and subverted American telecommunications infrastructure for several years. The risks of surveillance and the risks to privacy were quite substantial.

SolarWinds refers to an IT management system that is used throughout critical infrastructure. In 2020, we saw a supply chain attack where 18,000 of their customers had malicious updates installed that went undetected.

In terms of manipulation, we had a circumstance in 2016 where, for six months, Internet traffic between Canada and Korea was rerouted through China.

Volt Typhoon was an instance whereby multiple IT environments for critical infrastructure organizations, mainly in the U.S., were compromised. There is a high likelihood that this is a form of prepositioning, so that should there be kinetic warfare, that would then be a vector to attack the United States in relation to that.

We also see a high degree of hybridization—that's the term used—in relation to the war in Ukraine. There have been cyber-attacks associated with that in relation to supporters of Ukraine.

The Colonial Pipeline ransomware attack in 2021 shut down this critical infrastructure in the northeast United States.

We also have had a ransomware attack that affected AT&T: the ShinyHunters attack.

That's the tip of the iceberg, but with the set of hostile foreign adversary countries that are routinely attacking critical infrastructure, with the growth of ransomware, which is more profitable due to the use of cryptocurrency, and with the rapid increase in damages due to extreme weather events such as forest fires or hurricanes, or issues around even just human error, which happens with the growing complexity of the system, such as what we saw with the Rogers outage in 2022, this is a set of issues that touch our work and Canadians every day, frankly.

The scope of the issues is what really keeps us up at night. Certainly, one can imagine extreme examples where there is an emergency, and that is very much a real thing as well, but it's dwarfed by all of the ongoing management that goes into telecommunications regulation and oversight. It's quite substantial and it's quite routine, and people don't notice it until there's an issue. Then they notice it and then they really care.

I'm a policy wonk who does the legislative part, and it's my colleagues in the engineering part who really have to operationalize this stuff. I see what they have to do every day, and it's really something. The range of threats—cyber, natural disaster and human error—is substantial and ever-present in terms of an ongoing management context.

● (1700)

Sima Acan: Just as a small add-on, we already spoke about how we are the only country in the Five Eyes that doesn't have the authority the bill is asking for. Am I correct?

Andre Arbour: Yes, that is correct.

Sima Acan: Thank you.

The Chair: Thank you, MP Acan.

MP Powlowski.

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): I just want to speak to it a bit, because although the *realpolitik* at the moment may mean that we have to accept part of this, I don't think it's a good idea.

Overall, when Frank first brought up the requirement for a warrant, it seemed to me like a good idea. However, especially with regard to cybersecurity, I think time is of the essence, and time is of the essence most of the time. There are other instances in life—I'm thinking of Matt Strauss, as well as myself—when you have to act quickly, and I think this is an area where, generally speaking, you have to act quickly. Therefore, the fallback position should not be that a warrant is required, because that's going to stall the process.

Cyber-attacks are part of modern warfare. We've seen Russia repeatedly attack Ukraine and its vital infrastructure. It seems to happen—and they want it to happen—quickly, in a matter of seconds. Certainly, we've been talking about why we need this law. It's in order to protect our power grids, nuclear power stations and communications, such as from air traffic controllers to airplanes. All that is controlled by computers, and all that could be shut down.

It seems to me that putting an extra layer of protection, a requirement for a warrant, just further stalls things. This is letting down the gates of the fort, and we're surrounded by enemies on all sides right now. I would say that this is not the time to let down the gates. If I were Putin and the Russians, I'd be applauding this amendment and saying, “Absolutely, put a requirement that they have to have a warrant beforehand. Let's add other protections to stall the process.” As I said, that's letting down our guard, and this isn't the time to let down our guard.

● (1705)

The Chair: Thank you, MP Powlowski.

MP Ehsassi.

Hon. Ali Ehsassi: Thank you Mr. Chair.

I'll just follow up on the question MP Acan had, because I wasn't quite clear on that. She did ask about the Five Eyes, about what powers and prerogatives existed in those jurisdictions. However, I'm not quite sure whether you were talking about the minister's powers or about the fact that they do have legislation in place. If you could kindly clarify and bifurcate those two distinct issues, I would be very grateful.

Also, I want to thank you for sobering us all up and listing all of those issues that you did. I think we should all recognize that this is a big responsibility and that we have to act in a responsible fashion. Thank you.

[*Translation*]

The Chair: Mr. Arbour, would you like to respond?

[*English*]

Andre Arbour: Different countries have different institutional arrangements in terms of how this is set up. It is not necessarily a minister. It depends on the context.

As for the reasons, I would first and foremost flag that some of the powers that would be captured by this amendment are for the Governor in Council as opposed to a minister. However, one might then also ask why the authority is under a minister. What started with that proposition? There are two main regulators of telecommunications in Canada. There's the CRTC, and there's ISED under the Minister of Industry. That's been the case since at least the 1980s.

Right now, the minister can revoke someone's licence to provide wireless services and can turn off their wireless services. Certainly, the degree of exigency associated with justifying that decision would have to be very, very considerable. I cannot think of a single case where that, in fact, happened. However, that is an authority that has existed with either the Minister of Industry or the Minister of Communications since, I think, the 1970s at least.

There is a wide range of ongoing regulation of these private sector companies that is material to these companies and has to do with their ongoing network management. With regard to issues with respect to human rights, such as speech, those are not within the scope of the Telecommunications Act, and the committee also adopted a “for greater certainty” amendment that further scoped out those considerations.

This approach is consistent with many decades of how the telecommunications sector has been regulated.

[*Translation*]

The Chair: Thank you.

[*English*]

Are there any other interventions?

[*Translation*]

We'll now proceed with a recorded vote on amendment CPC-2.

Is it the pleasure of the committee to adopt amendment CPC-2?

[*English*]

Hon. Ali Ehsassi: Can I do a follow-up question, Mr. Chair?

The Chair: Unfortunately, it's now too late, MP Ehsassi.

● (1710)

Hon. Ali Ehsassi: Okay.

The Chair: We'll hear you later, hopefully.

Hon. Ali Ehsassi: No, no. I didn't realize that you'd called the vote.

The Chair: Yes, we'll do a roll call.

(Amendment agreed to: yeas 5; nays 4 [*See Minutes of Proceedings*])

[*Translation*]

The Chair: We'll now turn to amendment CPC-3.

[*English*]

Is CPC-3 moved?

Frank Caputo: I will move CPC-3.

The Chair: You have the floor.

Frank Caputo: Thank you.

Colleagues, I spoke at length earlier, so I won't speak at length about what I call some of the vague language that I think concerns us all. In fact, some of the government amendments do deal with this. I will say that it's actually rare to see the NDP, Bloc, Green and Conservative MPs all raising the same issues. I take it that it came from the Privacy Commissioner.

One of the consistent themes that I think we can all agree with is that some of the language, based on what we heard from testimony, is vague. Here we're asking for the word “threat” to essentially go from “any threat” to “material threat”. I think “any threat” is too broad. Sometimes in law we talk about a de minimis standard. That could be just about anything. To me, a material threat is something important. Everybody around this table has spoken about the charter. We all know about its import. When you say “material threat”, that suggests that there has to be something worthy of intervention.

I believe this is a fairly reasonable amendment. It's just to say that if the government or a judge orders that somebody may intervene, they're intervening for a good reason. I think “any threat” can be quite subjective, while “material threat” is a much higher threshold.

That is my argument in favour of CPC-3.

Thank you.

[*Translation*]

The Chair: Thank you, Mr. Caputo.

Before discussing this amendment, I would like to make a comment.

If amendment CPC-3 were adopted, the subsequent amendment BQ-1 could no longer be moved because of what we call a line conflict. In *House of Commons Procedure and Practice*, Fourth Edition, which we know well, section 16.71 states that "the committee Chair calls the proposed amendments in the order in which they would appear in the bill", meaning based on the lines. "Once a line of a clause has been amended by the committee, it cannot be further amended by a subsequent amendment as a given line may be amended only once."

In other words, remember that the adoption of this amendment would mean that a subsequent amendment, BQ-1, could no longer be moved because of a line conflict.

Mr. Ramsay, you have the floor.

Jacques Ramsay: Would Mr. Caputo like to clarify the content of his motion?

The Chair: I understand that people would like to—

[*English*]

Frank Caputo: Thank you, Mr. Ramsay.

I was just going to ask if, based on what you have mentioned, Mr. Chair.... I believe it was amendment BQ-1. Was BQ-1 the one you referenced?

If we were to amend BQ-1 by stating, "the gravity of that material threat", would the amendment then accord with CPC-3? I don't want to scuttle Madame DeBellefeuille's amendment when it's just one word that would be changed.

● (1715)

The Chair: We can check on that. It will require a little time.

Again, what we know now is that if we adopt CPC-3, which we may do, BQ-1 cannot be voted on.

Let me suspend for a couple of minutes to check on your question, MP Caputo.

● (1715)

_____(Pause)_____

● (1720)

[*Translation*]

The Chair: I call the meeting back to order.

As you know, we're debating amendment CPC-3. I already said that the adoption of this amendment would mean that amendment BQ-1 couldn't be moved because of a line conflict. I don't think that this decision has been challenged. It's more of a warning than a decision.

I'll now open the floor to debate.

Mr. Ramsay, you have the floor.

Jacques Ramsay: Mr. Chair, we're debating amendment CPC-3.

In our view, this amendment is largely unnecessary. It raises the risk of limiting the scope of threats that the proposed orders could address. This could limit the government's flexibility to deal with what we might call new technological advances or cyber-threats that would be defined later and that are currently unknown.

In our view, the bill is already narrowly focused on the security of telecommunications systems alone. The legislation doesn't allow the Governor in Council or the minister to use the proposed powers to address broader national security threats or challenges. This legislation isn't meant to focus on national security issues.

In addition, the proposed amendment includes the addition of the qualifier "*importante*" to the word "*menace*". It isn't clear how this could be interpreted. Some threats are potential, but they nevertheless warrant mitigation. So we won't be supporting this choice of the word "*important*", which remains difficult to interpret.

The Chair: Thank you, Mr. Ramsay.

I'll give the floor to Mr. Caputo. Then it's Ms. Kirkland's turn.

[*English*]

Then it's Madame DeBellefeuille.

You can start, MP Caputo.

Frank Caputo: Okay. I'll be quite brief here. I would like to answer Mr. Ramsay's points about materiality. I respectfully disagree, and here's why.

We talked about potential threats. Right now, the bill says "any threat". That would probably include a potential threat. What we're saying—and I think we would all agree around this table—is that a threat must be substantial enough that the government can act. The concern we have is that, in order to prevent any abuse of power.... I'm not trying to impute nefarious motives to anybody. The whole point is to say that, when the government is going to act, it must have reason to act.

I think that's a sentiment we all share around this table. Now, we may disagree on whether the word "material" encapsulates this. Usually, the word "material" in law means "important", "substantial" or something like that. If the government is only going to act when it should be acting, the word "material" is quite important. When we get to "any threat", it's much more confusing because "any threat" is so subjective. Who sees what as a threat?

That's why I prefer the term "material", but I'll allow any of my other colleagues to intervene.

Thank you.

[*Translation*]

The Chair: Thank you, Mr. Caputo.

Mrs. DeBellefeuille, you have the floor.

Claude DeBellefeuille: Mr. Chair, I would like a clarification.

When we compare the English and French versions of the amendment, the French version clearly states “*menace importante*”, but the English version says “material threat”. I don't see the word “important”. I'm wondering whether there was a translation error. That's my first question. I want to try to determine whether this English phrase means the same thing as it does in French. We know that words matter in a bill. I just want to check so that Mr. Caputo can say that we're talking about the same thing.

That said, I think that amendment BQ-1 is more complete. I'll be voting for amendment CPC-3. I believe that amendment BQ-1 is more relevant and complete. However, I would appreciate an answer to my question about the translation.

● (1725)

The Chair: I'll invite the officials to respond.

I may have misunderstood you, Mrs. DeBellefeuille, but if amendment CPC-3 were adopted, we couldn't—

Claude DeBellefeuille: I wanted to give Mr. Caputo a chance, because the English and French don't match. However, I'll definitely be voting against amendment CPC-3.

The Chair: I thought that I heard you say the opposite.

Claude DeBellefeuille: That may be. Thank you for paying attention.

The Chair: I don't want to do your job, because you do it very well. However, I wanted to make sure that we all understood.

Would the officials like to answer Mrs. DeBellefeuille's question?

Andre Arbour: The word “*important*” in French could be compared to the word “material” in English. Both words aren't necessarily very precise in context. They remain vague, especially in view of the other provision stating that an order must be reasonable in relation to the threat in question.

The Chair: Thank you.

Mr. Strauss, you have the floor.

[*English*]

Matt Strauss: Thank you, Chair.

It seems that we're struggling for the right word, but I have perceived, over the last couple of meetings I've attended, that there's some amount of consensus, including with Minister Joly when she attended, that the intent—I take it on good faith—of the legislation is to regulate the structure of the telecommunications system. The words “any threat”, to me, would include the content. When I proposed to Minister Joly that an amendment be made to use words like “physical” or “structural” or “infrastructural”, she expressed agreement with that proposition at that time.

If you don't like the word “material”, I guess I would put it to all of the members here to come up with some sort of word that drives at the civil liberties concern. My fear is that, as it's written right now, a leftist government could view conservatism online as a threat, and a conservative government could view leftism online as a threat.

I would ask members to look at it from that perspective. I just want some safeguard in place. I'm not a lawyer and I'm not a telecommunications regulator, but if on team Canada here we could find some word to allay this concern, which the minister said she shared with me, I would appreciate that.

Mr. Arbour, do you have any suggestions for words that way?

Andre Arbour: Part of my hesitation, given the existing language in the bill, is just, again, trying to think through what would be useful to add without being confusing. I'm at a bit of a loss at the moment, to be perfectly clear.

Matt Strauss: That's fine. I did spring it on you at the last minute.

Andre Arbour: In terms of the comments you made about the way the telecom act is scoped for targeting infrastructure, it doesn't get into the same detail in this, because we're talking about amendments as opposed to the act as a whole. That is indeed already the scope of the act. You can read the Supreme Court's Capital Cities case from 2003 or the ISP reference case from 2012.

Telecommunications in the modern world touches pretty much any activity that exists in Canada. If someone is engaged in online commerce, like Rogers, which has a banking activity, that is subject to the Bank Act. It's not subject to the Telecommunications Act just because it happens to be online. The Telecommunications Act is specifically about the physical transmission between equipment. That is the definition of “telecommunications” in the Telecommunications Act. That's what it speaks to.

In the ISP reference case I mentioned, the Supreme Court got into what it means, for instance, to be a broadcaster engaging in expressive speech versus what it means to be a telecommunications operator. There, the ruling was quite clear: When you're just providing the raw transmission, you're acting as a neutral conduit. That's just the focus of the bill and the infrastructure there. Certainly, the amendment that was adopted this evening added for greater certainty that expressive speech cannot be controlled.

Thank you.

● (1730)

[*Translation*]

The Chair: Thank you.

[*English*]

I have other MPs on the list, but if they withdraw their names.... I see Madame Acan specifically.

If there are no more interventions, we can vote on CPC-3. Otherwise, we will adjourn.

Sima Acan: Before we vote, can I make my point, Mr. Chair?

The Chair: Yes. With such a nice smile, you can do that.

Sima Acan: Thank you.

In the technical field of cybersecurity, I think this amendment could be considered dangerous for some reasons. One reason is that it would prevent proactive defence. I would be very happy if the experts could speak to that briefly before we move on.

Effective cybersecurity relies on identifying and mitigating near misses and the smaller technical threats before they escalate into a national crisis. If the law is restricted to only material threats, which I read as significant, the government could be legally barred from acting against early-stage vulnerabilities. I think it's important. We need to act against early-stage vulnerabilities that have not yet caused immeasurable harm. A material threshold might even prevent the government from addressing a major attack targeting a single service provider if the attack is not yet considered material to the entire Canadian telecommunications system. By forcing the government to wait until the threat is significant, in using the word "material", this amendment effectively prioritizes reactive measures over proactive protection.

Could you please briefly talk about near misses and how important it is to detect them before they become material threats? Thank you.

Andre Arbour: Yes, a lot of the regulatory activities that would be considered are very routine. It's about good hygiene, so it's about, for instance, how frequently you're patching your systems and that type of thing.

In that context, it's just unclear how "material" would be interpreted. I would say it's possible that it ends up being interpreted in an expansive way, but it's unclear to me, at least, if that would be the case.

The Chair: Okay. Thank you for that.

We'll go to a recorded vote.

(Amendment negatived: nays 5; yeas 4 [*See Minutes of Proceedings*])

● (1735)

[*Translation*]

Before adjourning, I would like to inform you that we'll be continuing our clause-by-clause consideration this Thursday, February 5, and probably also on Tuesday, February 10.

On February 12, we'll be meeting with the Minister of Public Safety and the National Police Federation as part of our study on Bill C-15.

On February 17 and 19, the House of Commons won't be sitting and the committee won't be sitting either.

Thank you.

This meeting is adjourned.