



HOUSE OF COMMONS  
CHAMBRE DES COMMUNES  
CANADA

44th PARLIAMENT, 1st SESSION

---

# House of Commons Debates

Official Report  
(Hansard)

**Volume 151 No. 139**  
Thursday, December 1, 2022

---

Speaker: The Honourable Anthony Rota



## **CONTENTS**

(Table of Contents appears at back of this issue.)

# HOUSE OF COMMONS

Thursday, December 1, 2022

The House met at 10 a.m.

---

*Prayer*

---

## ROUTINE PROCEEDINGS

• (1000)  
[*English*]

### GOVERNMENT RESPONSE TO PETITIONS

**Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.):** Mr. Speaker, pursuant to Standing Order 36(8)(a), I have the honour to table, in both official languages, the government's response to eight petitions. These returns will be tabled in an electronic format.

\* \* \*

### COMMITTEES OF THE HOUSE

#### CANADA–PEOPLE'S REPUBLIC OF CHINA RELATIONSHIP

**Mr. Ken Hardie (Fleetwood—Port Kells, Lib.):** Mr. Speaker, I have the honour to present, in both official languages, the first report of the Special Committee on the Canada–People's Republic of China Relationship in relation to the motion adopted on Tuesday, November 29, regarding Canada and the People's Republic of China.

The motion is as follows:

That the committee express its support for the brave and courageous Chinese protesters who are fighting for their fundamental human rights and freedoms of association and expression, and call on Beijing to respect the right to peaceful assembly and avoid a repeat of the Tiananmen Square massacre of June 5, 1989

#### FINANCE

**Mr. Peter Fonseca (Mississauga East—Cooksville, Lib.):** Mr. Speaker, I have the honour to present, in both official languages, the eighth report of the Standing Committee on Finance in relation to Bill C-32, an act to implement certain provisions of the fall economic statement tabled in Parliament on November 3, 2022 and certain provisions of the budget tabled in Parliament on April 7, 2022.

I would like to thank our finance committee clerks, Alexandre Roger and Carine Grand-Jean; our legislative clerks, Philippe Méla and Jean-François Pagé; our analysts, Joëlle Malo and Michaël Lambert-Racine; our committee assistant, Lynda Gaudreault; all

committee staff, interpreters and services, and all members of the finance committee for their dedication and hard work.

\* \* \*

• (1005)

### BANKRUPTCY AND INSOLVENCY ACT

**Mr. Charlie Angus (Timmins—James Bay, NDP)** moved for leave to introduce Bill C-309, An Act to amend the Bankruptcy and Insolvency Act and the Companies' Creditors Arrangement Act (public institutions).

He said: Mr. Speaker, I am certain anyone who read the Ontario auditor general's report on the financial disaster at Laurentian University understands the importance of protecting public institutions from ever being exploited through the bankruptcy protection act.

What happened at Laurentian was a debacle. We now know that this was not an accident. The administration and lawyers deliberately chose bankruptcy protection. In doing so, they trashed the careers of numerous academics, destroyed programs that took years to build up, and damaged the career trajectory of over 1,000 students. It will take years to restore the confidence there once was.

We need to ensure that the bankruptcy protection act is never used against institutions that receive public funding, whether it is hospitals, universities or health care centres. This cannot be a tactic used by right-wing governments at the provincial level to undermine public investment in key institutions, like what happened at Laurentian University.

(Motion deemed adopted, bill read the first time and printed)

\* \* \*

### PETITIONS

#### TAXATION

**Mr. Tom Kmiec (Calgary Shepard, CPC):** Mr. Speaker, I have a petition to table on behalf of my constituents. They are asking for the Minister of Finance to suspend the federal excise tax and carbon tax for Canadians until the cost of living crisis has been resolved. They are reminding the government that we are currently at triple the Bank of Canada's targeted 2% inflation rate, and it is destroying their ability to purchase groceries and fuel and pay for home heating. They are asking for this tax to be axed.

*Routine Proceedings*

## THE ENVIRONMENT

**Ms. Rachel Blaney (North Island—Powell River, NDP):** Mr. Speaker, I am here to present a petition on behalf of many constituents in my riding of North Island—Powell River who are very concerned about the foam from marine infrastructure and its increasing pollution of Canadian beaches.

Expanded polystyrene, commonly known as styrofoam, in the marine environment is very hazardous. They are concerned that it will cause significant harm to marine life, seafood resources and ecosystems. It is incredibly difficult to clean this debris from the shores. As members know, it breaks up into very small pieces, enters the system and is very hard to get out. The petitioners are calling for action to prohibit the use of expanded polystyrene in the marine environment.

## CLIMATE CHANGE

**Mr. Gord Johns (Courtenay—Alberni, NDP):** Mr. Speaker, it is an honour to table this petition on behalf of constituents from my riding of Courtenay—Alberni. The petitioners are calling on the Government of Canada to enact just transition legislation that reduces emissions by at least 60% below 2005 levels by 2030, to make significant contributions to emissions reductions in countries in the global south, and to create new public economic institutions that expand public ownership of services and utilities across the economy to implement this transition; that create good, green jobs, driving inclusive workforce development led by and including affected workers in communities and ensuring decent low-carbon work for all workers; that protect and strengthen human rights and workers' rights; that respect indigenous rights, sovereignty and knowledge by including them in the creation and implementation of this legislation; and that pay for the transition by increasing taxes on the wealthiest corporations and financing through a public national bank.

## PERSONS WITH DISABILITIES

**Ms. Bonita Zarrillo (Port Moody—Coquitlam, NDP):** Mr. Speaker, as we head into December 3, the International Day of Persons with Disabilities, I find myself again in the House advocating for the reduction of poverty among persons who live with disabilities.

Today I am tabling a petition on behalf of the constituents of Port Moody—Coquitlam, Anmore and Belcarra, to ask the government to finally lift people with disabilities out of poverty. Over a million people in Canada with disabilities live in poverty, and that needs to end. The petitioners are asking the government to end the current practice of legislated poverty of Canadians living with disabilities and establish a federal disability benefit that upholds human rights, the Convention on the Rights of Persons with Disabilities and sustainable development goal number one: no poverty under the Canada disability benefit act. I close by saying that this is possible immediately.

● (1010)

## HOUSING

**Mr. Mike Morrice (Kitchener Centre, GP):** Mr. Speaker, I am proud this morning to rise on behalf of over 2,000 petitioners who recognize that housing affordability and homelessness are twin national crises. They note that private corporations and real estate in-

vestment trusts are rapidly buying up affordable units across the country and raising rents, and that this financialization of the housing market is inflating real estate prices. They are calling on the Government of Canada to implement a suite of eight different measures that would address this root cause of the housing crisis that we are in, including creating regulations for real estate investment trusts, putting in place a national standard for rent control and providing funding for non-profit and co-op housing.

## SENIORS

**Mr. Churence Rogers (Bonavista—Burin—Trinity, Lib.):** Mr. Speaker, I want to present this petition on behalf of single seniors in Bonavista—Burin—Trinity and across the country. They are asking for an adjustment to Canada's tax laws that would allow them the same opportunities and advantages as senior couples. Many opportunities in the tax laws, such as splitting income, for example, give senior couples a major advantage over single seniors. The petitioners are asking for fairness in the tax system.

## CHARITABLE ORGANIZATIONS

**Mr. Arnold Viersen (Peace River—Westlock, CPC):** Mr. Speaker, the first petition I am presenting is from Canadians from across the country who are concerned about the Liberal Party of Canada's promise in their last election platform to revoke the charitable status of pro-life organizations, such as pregnancy care centres, which counsel women and save countless lives every year.

Revoking the charitable status of pro-life organizations is the first step to the politicization of charitable status in Canada. This would mean that churches, summer camps and other great organizations, like the Mustard Seed in Calgary, may have their charitable status put at risk. Therefore, the folks who have signed this petition are calling on the Government of Canada and this Parliament to protect the charitable status of pro-life organizations and to ensure that charitable status is not politicized.

● (1015)

## FIREARMS

**Mr. Arnold Viersen (Peace River—Westlock, CPC):** Mr. Speaker, the next petition I have to present is from Canadians from across Canada. They are concerned about the fact that Canada is the only G6 nation that prohibits the use of a health and safety device.

Given the highly damaging noise levels that come from firearm use, these folks are calling on the Government of Canada to allow these sound moderators. These are universally recognized health and safety devices that are criminally prohibited in Canada. The petitioners would note that sound moderators reduce noise pollution near shooting ranges in rural and farming communities and in areas used for recreational activities. The use of sound moderators facilitate increased humane husbandry of game animals, livestock and pets that are hunting companions. The hearing damage that does happen from these firearms is significant for many and is a public health issue costing Canadian taxpayers millions of dollars annually.

The petitioners are calling on the Government of Canada to empower Canadians to be responsible for their own health and safety by removing the prohibition on sound moderators here in Canada, and allowing the legal acquisition and possession of sound moderators in Canada. They call on the provinces and territories to amend provincial and territorial prohibitions as well.

#### COVID-19 MANDATES

**Mr. Arnold Viersen (Peace River—Westlock, CPC):** Mr. Speaker, the next petition I have to present comes from Canadians from across the country who are still concerned about the imposition of COVID-19 mandates.

They continue to talk about the restrictions that they have at the border. They are calling on the Government of Canada to work with the United States to increase cross-border travel. They are also calling on the Prime Minister to quit politicizing the use of vaccines and insulting Canadians who disagree with him. They are also calling on the government to protect the sacred duty of the Government of Canada to guard against discrimination and guarantee the freedoms of all Canadians.

Therefore, the folks who have signed this petition are calling on the Government of Canada to immediately end all vaccine mandates for truckers and travellers, and they call for a complete and total end, not just a suspension, of these mandates.

#### MILITARY CHAPLAINCY

**Mr. Arnold Viersen (Peace River—Westlock, CPC):** Mr. Speaker, the final petition I have to present today is from Canadians from across the country who are concerned about the recent announcements around changes to the chaplaincy service in the Canadian Armed Forces.

Folks note that there have been reports of slander even in the mainstream Canadian media against religious communities. The folks who have signed these petitions are calling on the Canadian Armed Forces to reject the recommendations in the final report of the Minister of National Defence's advisory panel, and they are calling on the Canadian government to affirm the rights of all Canadians, including Canadians in the armed forces, to chaplaincy and to freedom of religion.

#### PERSONS WITH DISABILITIES

**Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC):** Mr. Speaker, it is a pleasure to rise today. I have a number of petitions to present to the House.

#### *Routine Proceedings*

The first petition comes from Canadians living with disabilities who have a number of asks regarding policies within the ambit of the federal government and Parliament that relate to Canadians with disabilities.

The petitioners note that inflation has increased the cost of living and is having the greatest impact on Canadians with fixed incomes, including Canadians living with disabilities. They note disturbing reports of people accessing euthanasia in Canada due to a lack of access to care and support. They also note that Canada's leading disability advocacy organizations had warned that Bill C-7 would threaten the lives and security of Canadians living with disabilities and that a choice to access euthanasia can never be truly free if those who suffer do not have access to the support they require.

The petitioners urge the House of Commons to pass Bill C-22, ensuring that the new Canada disability benefit is accessible to all Canadians who live with disabilities and does not take away existing benefits. They also ask for us to repeal Bill C-7 so that Canadians who live with disabilities are not coerced into accepting euthanasia because they do not have access to adequate support.

#### FREEDOM OF SPEECH

**Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC):** Mr. Speaker, the next petition is about Bill C-11, a bill currently before the Senate. The government has now admitted that it is seeking to give itself the power to regulate social media algorithms. The petitioners are opposed to that bill. They call on the Government of Canada to respect Canadians' fundamental right to freedom of expression and call on the government to prevent Internet censorship in Canada.

#### CONSULAR AFFAIRS

**Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC):** Mr. Speaker, the next petition I am tabling deals with the case of the ongoing arbitrary detention in China of Huseyin Celil, a Canadian citizen of Uighur origin. Mr. Celil is a Canadian Uighur rights activist. He was originally detained in Uzbekistan for supporting the political and religious rights of Uighurs and was then illegally rendered to China. The Chinese government continues to deny his Canadian citizenship.

The petitioners note that they were pleased to see the release of the two Michaels, and they want to see the government as actively engaged on the case for Huseyin Celil as it was on those two previous cases.

The petitioners ask the Government of Canada to demand that the Chinese government recognize Mr. Celil's Canadian citizenship and provide him with consular and legal services in accordance with international law; to formally state that the release of Mr. Celil from Chinese detainment and his return to Canada is a priority of equal concern as the release of Michael Kovrig and Michael Spavor from unjust detention; to appoint a special envoy to work on securing Mr. Celil's release; and to seek the assistance of the Biden administration and other allies around the world in obtaining Mr. Celil's release, as done with the two Michaels.

*Speaker's Ruling*

## CHARITABLE ORGANIZATIONS

**Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC):** Mr. Speaker, the next petition deals with a proposal in the Liberals' 2021 election platform to politicize charitable status and make charitable status determinations not on the basis of the work that organizations do but on the basis of what their convictions happen to be with respect to the pro-life question. The proposal to exclude organizations with pro-life convictions from accessing charitable status could put at risk the charitable status of worthy organizations such as hospitals, houses of worship, schools, homeless shelters and other charitable organizations that happen not to agree with the Liberals on that particular issue.

The petitioners note that the imposition of a values test associated with charitable status, similar to the one imposed on the Canada summer jobs program, would effectively involve meting out charitable status on the basis of the political or private religious convictions of different organizations, which goes against the core principles of the Charter of Rights.

The petitioners therefore call on the House of Commons to protect and preserve the application of charitable status rules on a politically and ideologically neutral basis, without discrimination on the basis of those opinions and without the imposition of another values test. They also ask us to affirm the right of all Canadians to freedom of expression.

## HUMAN ORGAN TRAFFICKING

**Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC):** Mr. Speaker, I would like to table a petition in support of Bill S-223, a bill that would make it a criminal offence for a person to go abroad and receive an organ taken without consent. This bill also has a provision whereby someone could be deemed inadmissible to Canada if they are involved in forced organ harvesting and trafficking.

This bill has been before Parliament in various forms for the last 15 years, and the petitioners call on the Parliament of Canada to move quickly on this proposed legislation to support it. They are hopeful that this Parliament will be the one that finally gets it passed into law.

• (1020)

**The Speaker:** I am afraid the member only has 20 seconds left. That is not enough to go through another petition, so we will stop here. I am sure the hon. member will have his petition ready for tomorrow, or the next time we have petitions. We look forward to it.

The hon. parliamentary secretary to the government House leader.

\* \* \*

## QUESTIONS ON THE ORDER PAPER

**Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.):** Mr. Speaker, I ask that all questions be allowed to stand.

**The Speaker:** Is that agreed?

**Some hon. members:** Agreed.

## POINTS OF ORDER

REQUIREMENT OF ROYAL RECOMMENDATIONS FOR BILL C-285—  
SPEAKER'S RULING

**The Speaker:** I am now ready to rule on the point of order raised on October 4, 2022, by the parliamentary secretary to the government House leader regarding Bill C-285, an act to amend the Canadian Human Rights Act, the Canada Labour Code and the Employment Insurance Act.

[Translation]

In my statement of September 26, 2022, concerning Private Members' Business, I expressed concern about Bill C-285, which stands in the name of the member for Niagara West. At the time, I encouraged members who wished to present their views on the need for the bill to be accompanied by a royal recommendation to do so.

[English]

When he rose in the House, the parliamentary secretary to the government House leader explained that Bill C-285 would provide an exception for claimants to receive employment insurance benefits if they lose their job for the sole reason that they made certain decisions about their health. In his view, this amendment to the act would therefore authorize employment insurance benefits in a manner and for purposes not currently permitted by the act.

As noted in *House of Commons Procedure and Practice*, third edition, on page 838, "Without a royal recommendation, a bill that either increases the amount of an appropriation or extends its objects, purposes, conditions and qualifications is inadmissible on the grounds that it infringes on the Crown's financial initiative."

[Translation]

Clause 7 of the bill adds section 35.1 to the Employment Insurance Act. It creates an exemption to the grounds for disqualifying or disentitling a claimant from receiving employment insurance benefits that are listed in sections 30 to 33 of the act by providing that no claimant is disqualified or disentitled from receiving benefits if they lost their employment for the sole reason that they made certain decisions about their health.

[English]

The Chair is of the view that the bill imposes a new charge on the public treasury and infringes on the financial prerogative of the Crown. As a result, the Chair finds that the bill must be accompanied by a royal recommendation if it is to receive a final vote in the House at third reading.

• (1025)

[Translation]

For now, the next time the House takes up the bill, it will begin debate on the second reading motion, and this motion can be put to a vote at the conclusion of that debate.

I thank the members for their attention.

## GOVERNMENT ORDERS

[English]

### TELECOMMUNICATIONS ACT

**Hon. Marco Mendicino (Minister of Public Safety, Lib.)** moved that Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, be read the second time and referred to a committee.

He said: Mr. Speaker, it is an honour to help kick off second reading debate of Bill C-26, an act respecting cybersecurity. I know this chamber has been anxiously awaiting the chance to advance discourse on this important legislation.

I will begin by saying that cybersecurity is national security. We need to make sure that our defences meet all of the challenges that are reflected today, and we need to make sure that both the public sector and the private sector are able to better protect themselves against malicious cyber-activity, including cyber-attacks. It is about defending Canada and the critical infrastructure we rely on, and we know that this will not be the last we hear of this issue.

What we decide now in the cybersecurity realm will help us form a launching pad for the way forward, because we know that our actions in the cybersphere are always a work in progress. We know that meeting the moment means that our actions must continually, effectively and safely provide a foundation for the way Canadians thrive in the 21st century.

Being online and connected is essential to all Canadians. Now, more than ever, Canadians rely on the Internet for their daily lives. It is about more than just conducting business and paying bills. It is also about staying in touch and connected with loved one from coast to coast and indeed around the world. Our critical infrastructure is becoming increasingly interconnected, interdependent and integrated with cyber systems, particularly with the emergency of new technologies such as 5G, which will operate at significantly higher speeds and will provide greater versatility, capability and complexity than previous generations.

[Translation]

These technologies certainly create significant economic benefits and opportunities, but they also bring with them new security vulnerabilities that some may be tempted to prey on.

The COVID-19 pandemic showed how important it is for Canadians to have secure and reliable connectivity. The government is determined to boost security for Canada's cyberfuture.

[English]

We also know about the inherent threats to our safety and security. Cyber-threats remain a significant national and economic security issue that can threaten that safety. The Canadian centre for cybersecurity's "National Cyber Threat Assessment 2023-2024" found this:

State-sponsored and financially motivated cyber threat activity is increasingly likely to affect Canadians...

Cybercriminals exploit critical infrastructure because downtime can be harmful to their industrial processes and the customers they serve. State-sponsored actors

### Government Orders

target critical infrastructure to collect information through espionage, to pre-position in case of future hostilities, and as a form of power projection and intimidation.

These activities will not cease. Malicious actors could take advantage of increased connectivity to trigger malicious events that could also potentially have severe effects on our public safety and national security.

[Translation]

Large corporations and critical infrastructure providers are targeted by actors probing for vulnerabilities and opportunities for penetration, theft and ransomware attacks.

Like its allies, Canada has made efforts to address these vulnerabilities and to ensure the security of Canadians and Canadian businesses.

• (1030)

[English]

Canada has long recognized the importance of securing our cyber systems. In 2013, Canada established a collaborative risk mitigation framework, the Communications Security Establishment's security review program. This program has helped to mitigate risks stemming from designated equipment and services under consideration for use in Canadian 3G, 4G and LTE telecommunications networks.

Furthermore, consultations with Canadians in 2016 informed the 2018 national cybersecurity strategy. This strategy established a framework to guide the Government of Canada in helping to protect citizens and businesses from cyber-threats and to take advantage of the economic opportunities afforded by digital technology.

[Translation]

In 2019, the government paid \$144.9 million to develop a framework for the protection of critical cyber systems.

In 2021, the government completed its interdepartmental review of 5G telecommunications security. The findings included a recommendation to work with the industry on moving forward with the current risk mitigation framework for the products and services intended for Canadian telecommunications networks.

All this work done over many years to address these known problems and to improve Canada's cybersecurity posture, including with 5G technology, brings us to the bill before us today.

[English]

The objectives of Bill C-26 are twofold. One, it proposes to amend the Telecommunications Act to add security, expressly as a policy objective. This would bring the telecommunications sector in line with other critical infrastructure sectors.

*Government Orders**[Translation]*

The changes to the legislation would authorize the Governor in Council and the Minister of Innovation, Science and Industry to establish and implement, after consulting with the stakeholders, the policy statement entitled “Securing Canada’s Telecommunications System”, which I announced on May 19, 2022, together with my colleague, the Minister of Innovation, Science and Industry.

*[English]*

As we announced at the time, the intent is to prohibit the use of products and services by two high-risk suppliers and their affiliates. This would allow the government, when necessary, to prohibit Canadian telecommunications service providers from using products or services from high-risk suppliers, meaning these risks would not be passed on to users. It would allow the government to take security-related measures, much like other federal regulators do in their respective critical infrastructure sectors.

The second part of Bill C-26 introduces the new critical cyber systems protection act, or CCSPA. This new act would require designated operators in the federally regulated sectors of finance, telecommunications, energy and transportation to protect their critical cyber systems. To this end, designated operators would be obligated to establish a cybersecurity program, mitigate supply chain third party services or product risks, report cybersecurity incidents to the cyber centre and, finally, implement cybersecurity directions.

It would include the ability to take action on other vulnerabilities, such as human error or storms that can cause a risk of outages to these critical services. Once implemented, it would support organizations' abilities to prevent and recover from a wide range of malicious cyber-activities, including cyber-attacks, electronic espionage and ransomware.

The rollout of 5G technology in Canada is well under way. This technology will allow Canadians to move more data faster. It will bring benefits for Canadians and our economy, but with these benefits comes increased risk. Canada's updated framework, established in part 1, aligns with actions taken by our Five Eyes partners, particularly in the United Kingdom. I will add that I recently met with our counterparts in Washington, D.C., not too long ago.

It would allow Canada to take action against threats to the security of our telecommunications sector if necessary. Legislative measures would provide the government with a clear and explicit legal authority to prohibit Canadian telecommunications service providers from using products and services from high-risk suppliers, such as Huawei and ZTE, if required and after consultation.

*[Translation]*

Once these amendments receive royal assent, the government will be in a position to apply these new order-making powers to the Telecommunications Act.

• (1035)

*[English]*

The CCSPA established in part 2 is also consistent with critical infrastructure cybersecurity legislation established by our Five Eyes partners and would provide a consistent cross-sectoral approach to cybersecurity for Canadian critical infrastructure.

Designated operators would be required to protect their critical cyber systems through the establishment of a cybersecurity program and to mitigate any cybersecurity risks associated with supply chain or third party products and services.

Cyber-incidents involve a certain threshold that would be required to be reported, and legislation would give the government a new tool to compel action, if necessary, in response to cybersecurity threats or vulnerabilities. Both parts 1 and 2 of Bill C-26 are required to ensure the cybersecurity of Canada's federally regulated critical infrastructure and, in turn, protect Canadians and Canadian businesses.

Overall, Bill C-26 demonstrates the government's commitment to increasing the cybersecurity baseline across Canada and to help ensure the national security and public safety of all Canadians.

*[Translation]*

Cybersecurity is also essential in the context of our economic recovery after the COVID-19 pandemic. In our increasingly connected world, we must implement the measures required to guarantee the security of our data and ensure that data is not exploited by actors, state-sponsored or not, who constantly seek to exploit our systems.

*[English]*

Recovery from cybersecurity incidents is both costly and time-consuming. Accordingly, when it comes to improving cybersecurity, the interests of government and private industry are aligned. Nevertheless, an administrative monetary penalty scheme and offence provisions would be established within both parts of the bill to promote compliance with orders and regulations, where necessary.

All of the actions I highlighted today form a key part of our ongoing commitment to invest in cybersecurity, including to protect Canadians from cybercrime and to help defend critical private sector systems. Like our allies, Canada has been working to address these vulnerabilities to keep Canadians and Canadian businesses safe. However, we have to be sure that we are ready for the threats that lie on the landscape.

*[Translation]*

For example, unlike laws governing other critical infrastructure sectors, the Telecommunications Act does not include any official legislative authority to advance the security of Canada's telecommunications system. Despite the existence of multiple programs and platforms enabling public and private collaboration in the telecommunications sector, participation is voluntary.



*Government Orders**[English]*

In addition, across Canada's highly interconnected and interdependent critical infrastructure sectors, there are varying levels of cybersecurity preparedness and no requirement to share information on cyber-incidents currently. Moreover, the government has no legal mechanism to compel action to protect these systems at this time. These are important gaps that the legislation introduced today seeks to address. That is why the government is establishing a strong and modern cybersecurity framework to keep pace with the evolving threats in our environment.

In short, the legislation would form the foundation for securing Canada's critical infrastructure against fast-evolving cyber-threats while spurring growth and innovation to support our economy. Cyber systems are understandably complex and increasingly interdependent with other critical infrastructure. This means the consequences of security breaches are far-reaching. It is also the reason that a consistent, cross-sectoral approach to cybersecurity is built into this legislation.

Bill C-21, which we have tabled and are now debating, would protect Canadians and the cyber systems they depend on well into the future. Significantly, this legislation can serve as a model for provinces, territories and municipalities to help secure critical infrastructure outside of federal jurisdiction. It is an essential addition to Canada's already robust arsenal, which is there to protect us and our economy against cyber-threats. It would allow us to continue taking even stronger action against threats to the security of our telecommunications sector and ensure Canada remains secure, competitive and connected.

I encourage all members to join me in supporting this landmark cybersecurity legislation, Bill C-26, today.

*[Translation]*

**Ms. Raquel Dancho (Kildonan—St. Paul, CPC):** Mr. Speaker, I thank the Minister of Public Safety for his speech.

I have a question about the impact of this bill on Crown corporations that are considered to be critical infrastructure companies. What impact will this bill have on Crown corporations?

- (1040)

*[English]*

What are the impacts of this bill on provincial Crown corporations?

*[Translation]*

I am referring to Hydro-Québec and Manitoba Hydro, for example. What impact will this bill have on Crown corporations?

**Hon. Marco Mendicino:** Mr. Speaker, I would like to thank my colleague for her very important question.

The goal of Bill C-21 is to build a bridge, a collaborative effort between the government, critical infrastructure sectors and the private sector. We developed an approach that includes excellent lines of communication in order to effectively identify the cyber-threats to critical infrastructure that might jeopardize national security and the economy.

In answer to my colleague's question, we will work with all federal regulators to create a system to protect all critical infrastructure sectors against all cyber-threats.

**Mr. Simon-Pierre Savard-Tremblay (Saint-Hyacinthe—Bagot, BQ):** Mr. Speaker, I think we are happy to see the government finally tackle the issue of cybersecurity. I am not necessarily saying that it is too little, too late, but I can say that we have waited a long time. We applaud the idea of forcing Internet providers to adopt better practices, and to that we say kudos. We all agree on that.

However, why does the federal government always have to react rather than be proactive?

We have been talking about 5G and Huawei for years. Hydro-Québec has been fending off daily computer attacks for years. We have known for years that China has been gaining power and interfering more and more. In short, we have known for years that Canada is extremely vulnerable in terms of cybersecurity.

How is it that, in this postnational system, everything always happens reactively, not proactively?

**Hon. Marco Mendicino:** Mr. Speaker, with all due respect for my colleague, I would like to point out that the government is always vigilant when it comes to any type of threat, including cyber-threats.

For example, in 2018, we created the national cyber security strategy. That is what I was talking about in my speech. The pillars of this strategy, which is used to respond to all risks, include resilient security systems, an innovative cyber ecosystem and Canadian leadership here and around the world.

We have taken concrete action to protect against the risks posed by certain actors that are not aligned with Canadian interests. We are now prepared to take the next step by introducing this bill to better protect our critical infrastructure. This excellent and effective measure will be implemented in collaboration with all federal regulators and the private sector.

*[English]*

**Mr. Daniel Blaikie (Elmwood—Transcona, NDP):** Mr. Speaker, folks would find that it is pretty easy to get agreement here on the idea that there is more to do in respect of cybersecurity. Where some of us may part ways is on the extent to which the government, while increasing its power to act, has not built into the bill corresponding checks and balances on its authority. Indeed, many of the orders it would give itself the power to issue under this act are secret orders. It has exempted itself from some of the normal reporting requirements.

*Government Orders*

I want to test the minister today on his openness to amending the bill at committee to ensure that there are appropriate checks and balances commensurate with the new and quite wide-ranging powers the government is proposing to grant itself in Bill C-26.

**Hon. Marco Mendicino:** Mr. Speaker, I look forward to collaborating with the hon. member and other parliamentarians on the debate of this important bill, including at committee stage. Without question, whenever the government takes decisive action to meet the threats posed in the realm of cybersecurity, there does need to be corresponding transparency and an articulation of the reasons we are taking that action.

He is quite right to underline that there would be new authorities contained in this bill. However, those new authorities we would propose to create are in direct response to the gaps that currently exist, as I outlined in my speech. We need to do both in lockstep: address the gaps posed on the landscape of national security in the context of cybersecurity but also be transparent about that.

I point out that there are independent bodies, for example NSI-COP and NSIRA, so that where the government is taking steps that implicate national security, there can be accountability. This is the way we can achieve both objectives. It would ensure the confidence of all Canadians that this is an appropriate measure to seize the opportunities there, as well as to manage the risks manifested in our landscape.

• (1045)

**Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.):** Mr. Speaker, I wonder if the minister can provide additional comments on the importance of the Five Eyes nations, the countries we work closely with, and give a different perspective on what he believes and why he believes it is important that we walk in step with those Five Eyes nations.

**Hon. Marco Mendicino:** Mr. Speaker, this question allows me to highlight how Canada is co-operating with like-minded democracies around the world, both in the context of the Five Eyes relationship as well as the G7. I had a chance to meet with both counterparts very recently, one in Washington, D.C., and then, about two weeks ago, in Germany. It is without doubt that all the democracies within these multilateral forums are thinking very hard about how to manage threats in cyber, including ransomware, including the spread of disinformation and including the efforts of hostile actors to engage in cyber-espionage and the like.

The way we are advancing that collaboration is through information and intelligence sharing as much as possible, so that we can push back against efforts to attack our economies and to attack Canadian interests, etc.

Even as we present Bill C-26 for debate, to take decisive action here at home domestically by addressing the current gaps within our cyber-realm, we are also collaborating very robustly with partners around the world who are like-minded in managing these threats.

**Mr. Alex Ruff (Bruce—Grey—Owen Sound, CPC):** Mr. Speaker, I just have a couple of quick points.

First, I would correct the minister. He referred to it as Bill C-21 a couple of times earlier in his speech. I think that maybe it is on his mind. He knows that there are great changes that need to be made or scrapped out of that bill.

As for the references he talked about in his speech, to Huawei and 5G, obviously the government finally decided to ban Huawei from our 5G network just in May.

Why did it take the government so long? It was tabled here. A motion was passed in the House a year and a half prior to its making that decision.

I am just interested to know why it took the government so long to make such a critical national security decision.

**Hon. Marco Mendicino:** Mr. Speaker, I embrace the urgency of my hon. colleague's question. I also want to thank him for the legislative title correction. Obviously, I am managing a number of priorities, as he well knows.

There is no dispute that we need to advance this debate and to do so thoughtfully and deliberately and urgently. As he will know, we took very decisive action against the risks posed by Huawei and ZTE as they relate to 5G, 4G and 3G networks, and we are going to continue to be vigilant about them.

If he shares that sense of urgency in moving forward, he really ought to study the bill along with his colleagues in the Conservative Party and support it.

At the end of the day, this bill would address those gaps and potential vulnerabilities so that we can manage the risks and, at the same time, leverage the innovative opportunities that lie in wait when it comes to technology.

**Ms. Raquel Dancho (Kildonan—St. Paul, CPC):** Mr. Speaker, it is an honour to speak today in the House about Bill C-26, an act respecting cyber security, amending the Telecommunications Act and making other consequential amendments.

This is a critical bill, and I am very happy to see the debate being undertaken today in the House. I do know that cybersecurity is important to the Minister of Public Safety, so I will give him credit for bringing this bill forward. It should be something that is important to all government ministers of every level of government. It is very important that we are having this debate today.

I was provided a briefing from cybersecurity experts from the minister's department just under a year ago. It was very informative about the risk Canada faces in terms of cybersecurity. Just to speak simply, I asked them what would be, in the worst case scenario, sort of a Pearl Harbor moment for Canada. They responded that it would be a cybersecurity attack on our electrical infrastructure or our pipeline infrastructure in the middle of winter. If there were a cyber-attack or a ransomware attack on the infrastructure that keeps Canadians warm in the middle of winter, that would be absolutely devastating, specifically in our coldest provinces, regions and territories in Canada.

*Government Orders*

Just to give Canadians an idea of the gravity of what we are talking about today and how important it is, not only that we bring forward cybersecurity legislation that builds capacity, but also that it be done right. There was a series of questions before my remarks that outlined a number of the issues in this bill.

I will just outline a number of recent cybersecurity attacks in Canada and also in the United States of late. We know that the Canada Revenue Agency was attacked in August 2020, impacting nearly 13,000 Canadians who were victims of that. There was also a hospital in Newfoundland, in October 2020, where the cybersecurity hackers stole personal information from health care employees and patients in all four health regions, as well as social insurance numbers belonging to over 2,500 patients. Very deeply personal and private data from these hospitals was stolen by cybersecurity hackers.

Global Affairs also most recently was attacked in January 2022, right around the time that Russia engaged in the illegal invasion of Ukraine. It was reported that it may have been Russian, or Russian state-sponsored, actors who were responsible for the cyber-attack on Global Affairs.

That was a very serious attack on another government department. The government is certainly not immune to these types of cybersecurity attacks.

Most famously, I would say, there was a ransomware attack on critical infrastructure in the United States back in May 2021. Pipeline infrastructure was attacked. President Biden issued a state of emergency. Seventeen states issued these states of emergency. It was very serious, and it just shows the capabilities of some of these cyber-threat actors, and the threat they pose to Canadians in their everyday lives and to Canada as a whole, as well as the threat to our allies.

This bill is coming forward in light of the government announcing most recently, in the past year, that it would ban Huawei from our 5G infrastructure. Conservatives and the House of Commons, in fact, have been calling on the government to do that for quite for some time. This legislation would help enable the practical implications of that ban. Again, it is certainly a very long time coming. Had this been done years ago, it would have saved our telecommunications and thereby the everyday users of our telecommunications companies, a lot of pain and a lot of money. I am concerned about the financial impact, although this is critical, that waiting so long to bring it forward would have on everyday Canadians and their cell-phone bills, just as an example.

I am the vice-chair of the public safety and national security committee. I championed a study we are undertaking, which is in the process of being finalized right now, of Canada's security posture in relation to Russian aggression. A large part of that study was about cybersecurity. The experts we brought in repeatedly sounded the alarm that cybersecurity is of the utmost importance. It is something that the Government of Canada, the private sector, provincial governments and, frankly, municipal governments must take extremely seriously. It is rapidly evolving. I am going to give some quotes from a few of the experts to lay the stage of what we are facing as Canadians.

Professor Robert Huebert of the University of Calgary said:

With regard to other cyber threats, we also know the Russians have shown an increasing capability of being able to interfere in various electronic systems and cyber systems of other states. We've seen this with their ability to influence the Ukrainian electrical system prior to the onset of the war in 2014.

• (1050)

This is the other war it engaged in over the last number of years. He also said that we are seeing this in other locations across the globe.

He went on to state:

Once again, it's hard to know exactly how well-defended [Canada has] become in being able to harden that part of cyberwarfare. There's no question, whatsoever, that the attention the Russians and the Chinese are giving this is increasing....

He compared that to the reports we are hearing from our American and British friends and allies who are saying the Chinese and Russians are extremely active on the issue of cybersecurity and involving state-sponsored actors launching attacks against countries like Canada and the United States.

We also had a woman named Jennifer Quaid, who is the executive director of the Canadian Cyber Threat Exchange, which is a private company that supports various companies to help boost their cybersecurity. She talked a lot about cybercriminals. This is an important piece. Even the minister talked about this as well.

First and foremost, she flagged that the Minister of National Defence of the current government said, "Cyber security is one of the most serious economic and national security challenges we face." Therefore, it is quite a serious issue we are talking about today.

Ms. Quaid went on to say, "cyber-threats are becoming more sophisticated and are increasingly pervasive. Driven by the growth and global adoption of innovative technologies, cybercrime pays."

She meant that cyber-threat actors can be grouped roughly into two categories, nation states conducting espionage and statecraft through the Internet, and criminals engaging in cybercrime for financial gain.

She went on to say, "It's this criminal element that has commercialized cybercrime", meaning that cybercriminals and cybercrime have now become a thriving industry. She pointed out that the barriers to entry, the technical expertise needed to be a hacker, so to speak, is increasingly low. She said that several countries now are allowing cybercriminal groups to operate within their borders.

She also named something called a "hacktivist", an activist hacker, of all things. We may have someone, in the name of social justice, hacking into a fossil fuel company, for example. Imagine if that happened in Canada in the middle of winter to our gas pipeline infrastructure. It would be devastating and deadly, so we have to keep an eye out for hacktivists, as she said.

*Government Orders*

She also pointed out that 25% of organizations in Canada have reported a cyber-breach. One in four. That is pretty significant. She said that the small and medium-sized enterprises that make up 98% of our economy are also being impacted. Almost 100% of our economy is being attacked in some form or another.

This is really important when we think of big banks and big, wealthy corporations that have pretty good cybersecurity infrastructure and have the money to do so. What feeds them is third party suppliers that may provide the various components or various mechanisms to undertake their important parts of the industry that company is engaged in. They are also at risk. Therefore, if a lower third-party provider of a major telecom is attacked, for example, that may seriously impact the ability of that telecom to deliver its services adequately to Canadians.

She mentioned that 44% of SMEs, small and medium-sized enterprises, do not have any defence. Almost half of our small and medium-sized enterprises, which dominate our economy, do not have any sort of defence and are not even thinking about cybersecurity. That is why today's discussion and this bill are important to be debated and have experts weigh in.

I will also quote Dr. Ken Barker, who is a professor at the Institute for Security, Privacy and Information Assurance at the University of Calgary. He talked a lot about the impact of cybersecurity on critical infrastructure. He mentioned that, in general, it is very vulnerable because it is built on legacy systems that, in essence, pre-date the Internet. As our legacy systems are getting online, this creates, as he explained, some gaps that hackers can take advantage of, which again puts our critical infrastructure at risk. That came up over and over at committee. He pointed out that our large private companies and our banks are investing a lot in cybersecurity, but again, as he and Ms. Quaid pointed out, it is their SMEs that are the most vulnerable.

I will conclude my quotations here with Caroline Xavier, who is the director of the Communications Security Establishment, which falls under the Department of National Defence. It is the part of government responsible for cybersecurity. Therefore, that she is the head of government cybersecurity is a simple way to look at it.

● (1055)

She said, “cybercrime is the most prevalent and most pervasive threat to Canadians and Canadian businesses. Cybercriminals trying to probe Canadian systems have been found in Russia, Iran and China, among others. [They] use various techniques such as ransomware”. They are specifically focusing on our critical infrastructure, and they certainly pose, as she said, “the greatest strategic threat to Canada.”

The bill before us would do a number of things. It is quite a large bill, so I will not go into every detail of what it would do, but in essence there are two parts. One would amend our existing Telecommunications Act. Of particular importance, it would give very broad and sweeping powers to the minister of industry to do a number of things. What has been criticized by a number of organizations is a specific part of the bill, which is in the summary, that says it would allow the minister and the Governor in Council to “direct telecommunications service providers to do anything, or refrain from doing anything”.

Those are very broad powers to be given to one minister, so that should immediately put up red flags for all of us. No one should have such vast sweeping powers over our telecoms. Again, I have built the case that we need better cybersecurity, but there is a big question mark here of whether we are giving too much power to one minister, one person, in all of Canada.

The bill also has a whole financial issue involved in it. To do anything, as it said, could have massive financial implications. Big companies such as Telus may be able to afford that, but our small telecoms may not be able to do so much. It might bankrupt them. That is not great news, and there would be no financial component, in terms of compensation, for any of these losses, so there is a big question mark there as well.

Also, something of importance I find quite concerning is the way the bill is structured would result in a significant exchange of a lot of information from telecoms to the minister, which he could pass on to various ministers and government agencies. Is that very confidential information? It is certainly the cybersecurity plans. Does that include state secrets? Is it safe that we would be asking our telecoms this?

The second part of the bill involves all critical infrastructure companies in Canada, as was outlined by the minister, including provincial and Crown corporations, and the like, so the bill would really establish the process that all of these companies would have to provide their cybersecurity plans, and there would be a very strict reporting mechanism. We are talking about days, if not a few weeks, to get together these plans and provide them to the minister. There would be annual updates required. If a big company were to change a third-party provider, it would have to, in essence, immediately report that to the minister of industry.

There is a whole host of very cumbersome reporting mechanisms, and I do believe we need some of these, but a question remains, as I have outlined earlier, and the government is not immune to being hacked by cybercriminals. I just outlined three or four incidents when that happened. The bill would take all of our critical infrastructure, and all of companies' cyber-defence plans, along with countless other pieces of personal data of Canadians and others, and we would give that to the government. An argument could be made that this is needed, but where are the protections for that? Where is the defence of government to ensure that this would not end up in the wrong hands or that information is not hacked by cyber-actors?

That is a significant threat that needs to be addressed by the minister, and I was not assured from his remarks that this is something that is front and centre in his objective through the bill.

*Government Orders*

I would also say that there is a number of civil liberty organizations that have raised serious alarm as well. There was an open letter written to the minister from the Canadian Civil Liberties Association, the Canadian Constitution Foundation, the International Civil Liberties Monitoring Group, Leadnow, Ligue des droits et libertés, OpenMedia, and the Privacy and Access Council of Canada. All of the leaders of research and discussion of our civil liberties, all such major organizations in Canada, were quite alarmed by the bill in many ways and wrote an open letter to the minister that outlined a number of things.

In essence, they said the bill would grant the government sweeping new powers, not only over vast swathes of the Canadian economy, but also in intruding on the private lives of Canadians. To sum it up, and I think they said really quite well, “with great power must come great accountability.” There is great power in the bill, but the accountability side is lacking.

Before I go on to detail some of their concerns, I do want to outline what some other countries are doing. If we look at the U.S. and the EU, they have established similar bills in the past year or so. The EU actually has greater and more significant fines in many ways, and the U.S. provides more prescriptive and strict reporting mechanisms, such as, if a U.S. critical infrastructure company has a ransomware attack, the legislation outlines the company must report it to the government within 24 hours.

• (1100)

That actually might be something we may want to consider for the bill. If we are going to go there, we might as well have it in line with our American allies and make it tight. I do think that a reporting mechanism is one of the most important parts of this bill.

I want to go back to the civil liberties issue. With the government's track record on Internet regulation bills, such as Bill C-11 and others, a lot of people have their backs up about their personal freedoms online and their data, rightfully so. The civil liberties associations are raising some of the concerns that have not been assuaged thus far by the government or the Minister of Public Safety.

In the open letter, they mention that this, “Opens the door to new surveillance obligations”, which is quite concerning. In their view, and this has not been proven, “Bill C-26 empowers the government to secretly order telecom providers ‘to do anything or refrain from doing anything’”, as I mentioned. They believe that, if there was an abuse of this extreme power, it could be utilized by a government with ill intent, not to say that is the Liberal government's intent, but it could be utilized to survey Canadian citizens. It is quite concerning.

They go on in that realm to outline that the powers in this bill allow the administrative industry to terminate who telecoms work for, for example. They believe that could also be applied to individual citizens. They are looking at this and thinking, if a government wanted to punish a group of people, it could call up Telus, and this is very blunt and not overly academic in the way I am explaining it, to direct Telus it cannot do business with these people, cut off their access to the Internet and cut off their cell phones.

It is an extreme worst-case scenario, but it is worth flagging that there may be a bit of a backdoor in this bill that would allow that,

should an evil government ever come along that is looking to abuse the civil liberties of Canadians. I would like to see that addressed and have safeguards put in place to prevent that type of abuse, should it ever happen in an extreme circumstance.

They also talk about how it “Undermines privacy” and that there are “No guardrails to constraint abuse”. Again, I think this is an area where opposition parties, in particular, and hopefully government members on the committee, can come together to ensure that there is an ombudsman put in place or an oversight body. We need something where the rights of companies, and more importantly of citizens, are protected from the abuses I have outlined, and there are many others.

There were also a lot of concerns from the Business Council of Canada. It wrote an open letter to the minister on behalf of large companies, and also small and medium-sized enterprises. In essence, what we are seeing is the red tape is extremely high, so we are worried that will impact our small and medium enterprises.

The business community, in general, has said that it seems that this bill, to sum it up bluntly, is all stick and no carrot. It is all hard-hitting. It is going to be super hard on us, and we better comply. I can hopefully go into more details about that in the question part of this debate, but there is no incentive structure built in.

There is no incentive to have companies share best practices with each other. I think the government should be a leader in encouraging the open sharing of best practices and experiences that protect the confidentiality of companies but allow them to share information, so other companies can be better equipped, and we can all work together as one big happy, cyber-secure family.

The Conservative Party of Canada is, first and foremost, concerned about national security and ensuring the federal government takes that leadership role in ensuring that Canada, as a whole, is secure against any possible threat, every eventuality, as the Minister of National Defence likes to say.

We are seeing serious gaps in our military. We can have stronger alliances in our Five Eyes intelligence sharing and other agreements. Certainly, that involves cybersecurity. Canada is vulnerable, like many countries in the world. In fact, most countries are dealing with these problems. The Conservative Party of Canada wants to see a more robust framework to incentivize and enforce reporting mechanisms to ensure our cybersecurity is protected, and to make sure there is not a ransomware attack on our pipelines in the middle of winter, which could kill thousands of Canadians from the cold, for example.

*Government Orders*

We will be looking to support this bill in going to committee, but I want to make it very clear that, if the issues in this bill, and I have outlined a few of them concerning privacy and impacts to business, are not addressed, the Conservative Party is ready to pull its support immediately and put up a very strong defence to stop this bill from going beyond committee. I want to make that very clear to the minister and the Liberal government.

We will get this to committee to hear from experts because we believe that is important, but it must be fixed. There are serious issues that need to be addressed and amendments that need to be made. I would ask Liberal members on the committee to get to work with us, so we can make this bill what it needs to be and make it better to ensure cybersecurity is protected in Canada today and for years to come.

• (1105)

**Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.):** Mr. Speaker, I do not think there is anyone in society who does not recognize the potential harm of cybersecurity. The issue is how do we ensure we are well positioned to address vital threats to our critical infrastructure. The member opposite says her concern is that we are giving too much power to one individual.

Does the Conservative Party have an alternative to ensure that particular issue is addressed in the form of an amendment? Does the member have any suggestions on that point?

• (1110)

**Ms. Raquel Dancho:** Mr. Speaker, the member is also from Winnipeg, so he is a fellow Manitoban.

As I outlined it in my remarks, it is not just the Conservative Party. We were alerted to this by every major civil liberties organization in the country. They wrote quite an in-depth open letter with over two dozen different concerns that they had, give or take, so we are using the information we are getting from the organizations specifically tasked with protecting civil liberties and privacy and freedoms of Canadians. That is who alerted us to it.

We would like to bring them before committee to make their recommendations. They have made recommendations in open letters. Various organizations with technical expertise have also recommended various amendments to this bill. Again, I am not an expert in cybersecurity, but I do understand Canadians' need to protect their privacy. Therefore, at the committee stage, we will be bringing forward these experts to help us craft amendments. I mentioned in my remarks that perhaps there could be an ombudsman or a specific oversight committee that is built into this.

One last thing is that there is no annual reporting mechanism in this bill, where government would be responsible for tabling a report to Parliament that would outline and give Canadians an idea of what the government has been doing with this bill and what the threat assessment of Canada in the impacts of what the bill has done and what it has seen in the reporting mechanisms from companies. I would say it needs annual reports to Parliament, and we have to craft those amendments with expert witnesses' testimony at committee. I look forward to those discussions.

[*Translation*]

**Mrs. Julie Vignola (Beauport—Limoilou, BQ):** Mr. Speaker, I have so many questions.

We agree on the principle of the bill, but I do have to wonder about the precautionary principle. Since 2017, the Chinese government has required Chinese companies to hand over any information they collect to its intelligence service. Despite this, the federal government continues to award contracts to Chinese companies like Nuctech, for example.

That was a very important contract, I might add. Nuctech was being asked to install x-ray machines in embassies, precisely where our information must be protected. Information from the embassy could have easily been passed on.

My question for my colleague is this. We currently have an interesting bill before us, although it needs improvement. Should the precautionary principle not be applied more systematically, along with the recommendations made by the Standing Committee on Government Operations and Estimates in its June 2021 report?

[*English*]

**Ms. Raquel Dancho:** Mr. Speaker, the member's question is quite a technical one. The member does mention China and what it has done. I am deeply concerned about Chinese state-sponsored actors who are conducting espionage and looking to steal data and very important national security information from various government departments and individual citizens. That is the reason that all of our Five Eyes allies, with Canada being last, banned Huawei from our 5G infrastructure, because of any possible back-door element.

Because, with all companies that are owned by China, there is, to put it bluntly, an ability for them to direct, for example, Huawei to take all their information. That is why Five Eyes allies, put quite simply, called on Huawei to be banned. They did that before us, and we took a very long time.

I will look more into the specifics. The member was not too familiar with what she talking about. Suffice it to say, the Conservative Party of Canada has been very clear: We need to be very clear-eyed on China, in particular when crafting this bill. It needs to be crafted in a way that offers the most defence for Canadian critical infrastructure against Chinese sponsors, state actors or others.

**Mr. Daniel Blaikie (Elmwood—Transcona, NDP):** Mr. Speaker, there is a lot to think about in what the member for Kildonan—St. Paul had to say, and I agree with many things she said, including her concern about the oversharing of Canadians' personal information between government departments. I know that was a significant issue in the 41st Parliament with Bill C-51, when the government of the day introduced security legislation at that time.

I wonder if the Conservative Party today is in a mood to actually protect Canadians against the oversharing of information between government departments and if we might try to find an opportunity in the course of this bill's passage through the House to correct, as we go, some of the defects in that legislation from many years ago.

• (1115)

**Ms. Raquel Dancho:** Mr. Speaker, I appreciate the question from my colleague, who is also from Winnipeg and a fellow Manitoban.

I take the member's point regarding former pieces of legislation that need work. The leader of the official opposition, the member for Carleton, has been very clear in his desire to protect data and the rights of Canadians, especially if we are looking at Bill C-11, which is the Liberal government's attempt to control and regulate the Internet, so to speak. He put forward the very first, very public and very well executed defence of Bill C-11, so I would say that the capability for data sharing between departments and between ministers, which is a large part of this bill, raises a lot of significant privacy concerns of the data of individual Canadians.

We have been very clear that our intentions with this bill and others are to protect those freedoms and that privacy of Canadians. Therefore, that will be the underlying theme of our approach, certainly to this bill during the committee process and in the days and weeks to come.

**Mr. Larry Maguire (Brandon—Souris, CPC):** Mr. Speaker, I want to thank my colleague for Kildonan—St. Paul for taking part in the Manitoba debate that is going on here.

The member commented on SMEs, noting that half of them had no defence and were the most vulnerable. As with the bill I was able to get through last year on SMEs and small businesses, it is very important they have the abilities and rights to protect themselves on this as well. In response to the last question, the member also talked about transparency, which is so important.

Could the member expand on those two areas?

**Ms. Raquel Dancho:** Mr. Speaker, I am enjoying this Manitoba debate. There are a couple of things I would say.

The government, in the last budget of 2021-22, announced about \$700 million for cybersecurity. It seems that it is all going to the Communications Security Establishment, which, as I mentioned in my speech, is the government's sort of cybersecurity agency under the Minister of National Defence. It is great. We do need more resources at the government level for CSE. However, I asked the minister if any of that funding was being provided for our small and medium-sized enterprises so they could boost their cybersecurity. The minister never did get a response to my email.

Again, when we are looking at small companies, it is easy for Telus, big banks and others to afford some of these things. However, if we are looking at small telecom providers, like a small Internet provider in northern B.C., the cost to meet the red tape in the bill might put them out of business. Why not take a little of that funding the government has announced and provide it to our SMEs to help them get to the level we need them to be to protect our critical infrastructure? Perhaps we can get a bit creative and look at our tax system to see if there is some sort of capital expense tax write-

### *Government Orders*

off or something we can provide our SMEs to help them get there, because we really need to, as I made the case in my remarks, as I am sure others will as well.

I have not heard a response to that. The government is spending the money anyway. It is spending more money than any government in history. Why not provide a little of that to our SMEs to ensure that critical infrastructure is up to par?

[*Translation*]

**Mr. Alexis Brunelle-Duceppe (Lac-Saint-Jean, BQ):** Mr. Speaker, we are talking about cybersecurity. This means that there is a lot of foreign interference conducted through cyber-attacks.

Speaking of foreign interference, is my colleague not concerned that, in 2016, after giving a Chinese bank a business licence, the Prime Minister received \$70,000 in donations to his riding of Papineau within 48 hours? Is that not interference? In 48 hours, he received donations from outside his riding, specifically from Toronto and British Columbia. Is that not evidence of foreign interference?

[*English*]

**Ms. Raquel Dancho:** Mr. Speaker, I appreciate the investigative work done by the Bloc Québécois on this issue.

We are just learning about the details of this. I am very concerned about the allegations being made, as everyone should be if there is proven to be a connection and it is proven to be true. We are monitoring this quite closely.

I imagine the Parliamentary press gallery and other media sources across the country are digging into this very quickly and as closely, as they should. It is something we are closely monitoring as we learn the details of any possible payoff to the Prime Minister from the Chinese government or other actors from China.

• (1120)

**Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.):** Mr. Speaker, an interesting debate is under way thus far on such an important issue with which we all have to come to grips. As changes in technology take place, we have to take that into consideration. I suspect that legislation dealing with privacy or cyber-attacks will be ongoing. Once the bill goes to committee, I am sure there will be a great deal of dialogue. I anticipate a great diversity of witnesses will come forward with ideas on the legislation.

I will pick up on the point I raised with the member opposite about the concern that the minister had too much power under this legislation. Often, when government brings forward legislation, opposition members bring forward concerns about how power is enhanced through the minister's office.

*Government Orders*

I have had the opportunity to briefly go through the legislation and I genuinely believe there is the right amount of balance. That is why I posed the question for the member. She suggested of reporting mechanisms, whether through an annual report or a report to a standing committee, and that has merit. I say that because I know there has been a great deal of effort in formulating this legislation. If there are ideas that would enhance or make it that much stronger, we should be looking at that. I do believe the ministry is open to that.

When the member was quoting, I wondered where those quotes were from. She used those to amplify fears that one might be challenged to justify. For example, the member referred to an “evil government” based on quotes she had received. I am not saying it is her opinion, but she has raised it, saying this is a quote from some third-party organization and if we believe in that quote, it could lead to an evil government. We have witnessed that a great deal from the Conservative opposition on a variety of different issues, as if there is some sort of conspiracy. There is no conspiracy, contrary to what the member said, at least in one part of her speech. The government is not out to spy on Canadians.

The government takes the issue of the privacy of Canadians very seriously. We have brought forward legislation to that effect. This government has spent tens of millions of dollars on cyber threats. The government has had working groups and advisory groups dealing with cyber threats. We recognize the changes in technology and the impact they have had on society. I have said in the past that if we were to look at technological advancements, we would be challenged to find an area that has been as advanced as computer Internet technology. Just the other day, I was speaking to a private member's bill, saying that 10 or 20 years ago there were no such things as iPhones.

• (1125)

I note the member for Winnipeg South Centre is listening. He will recall that when we were first elected back in 1988, there was a big computer purchase of \$5,000 made through Reg Alcock. We had a wonderful computer with a laser printer, which came with a keyboard and a mouse. At the time, when logging into the Internet with that wonderful and beautiful computer, the first thing we would hear was a dial tone. Then we would hear that stupid clicking sound, which meant we were actually connected to the Internet. We were all fairly impressed with that computer, and there were about 20 of us at the time.

We can compare that to where we are today. People can buy a laptop for \$500 that has abilities and technological advancements more than tenfold of what we paid \$5,000 for, with that long dial-up connection. In fact, people can purchase something brand new for \$250 that is hooked into the Internet and running at a rapid speed. It is not even comparable to what it was.

There is so much advantage to technological change, but with that change comes risk, which is the essence of what we are debating through Bill C-26. Even though society has benefited immensely, we need to recognize there is a significant risk factor. That risk factor not only applies for the individual who might be surfing the net today, but it also applies to military operations taking place in Ukraine today.

Computers today are not optional. The Internet is not optional. They are essential services. That is why the Prime Minister, or one of the other ministers, just the other day made reference to the percentage of Canadians who were hooked up with high-speed connections and how we had literally invested billions to ensure that Canadians continued to get that access, with a special focus on rural Canada. We recognize that because it is no longer optional; it is an essential service.

The digital economy varies significantly. If we want to get a sense of this, we can turn to Hollywood and like-minded productions found on Netflix, CBC or the more traditional media outlets. We can look at some of the movies and TV shows out there. The other day I was watching an episode of a show called *The Blacklist*, which is all about cyber-attacks. I suspect a number of my colleagues might be familiar with that show.

One member talked about hydro. Manitoba, in fact all of Canada, should be concerned about our utilities. Through Hollywood productions, we are better able to envision the potential harm of cyber-attacks. A well focused cyber-attack can deny electricity to communities. It can shut down things that should never be shut down.

We talk about the sense of urgency. One would expect there will be mischievous lone individuals working in their basements, or wherever it might be in society, challenging systems. However, we also have state-sponsored cyber-attacks, and we should all be concerned about that.

• (1130)

In fact, that is why it was comforting when the minister made reference to the Five Eyes. I caught on right away that there are like-minded nations. Canada is not alone. There are like-minded nations that understand the importance of cyber-attacks and the potential damage that can be caused.

I will get back to the international side of things later, but when we think of what is at risk, think of digital data. Digital data comes in many different forms. One of the greatest collectors of data is Statistics Canada, an organization that invests a great deal in computers and technology to protect the data it collects from Canadians. Statistics Canada is actually respected around the world for its systems. It has absolutely critical data, and that data is provided to a wide spectrum of stakeholders, obviously including the national government.

Let us think of health organizations, the provinces and the collection of health records, or motor vehicle branches and passport offices. All of these government agencies have, at the very least, huge footprints in data collection.



*Government Orders*

Those are government agencies. We could also talk about our banking industries or financial industries. We can think of those industries and the information that is collected from a financial perspective when people put in an application for a loan. All of the information they have to provide to the lender, such as their history, is going into a data bank.

There is also the private sector. The other day we were talking about apps. One example is Tim Hortons. We were talking about it, as members might recall. The Tim Hortons app is fairly widely downloaded, and there is a lot of critical information within it. Canadians need to know, whether it is a government agency or private agency, that governments at all levels, in particular the national government, have their backs. That is the reason I started off by giving a very clear indication that even though Bill C-26 is before us today, we have been investing substantial financial resources through other types of legislation to provide assurances to Canadians so they know their information is in fact being protected.

There are actions on the Internet today related to our small businesses. The member opposite made reference to this and asked how the government is supporting small businesses. If a person has a small business today, chances are they are on the net. More and more consumers turn to the net for widgets and a multitude of different services.

● (1135)

As a result of that, there has been a great demand on small businesses. That is why we have a Minister of Small Business who looks at ways to not only provide tax relief but provide support. Sometimes it is done directly through financial measures and sometimes it is done indirectly by providing resources. However, let there be no doubt that there is support coming from the government. Whether it be a small, medium or large business, the government has a vested interest. We will do what we can. A good example of that is the individual who uses an ATM card when they make a small or large purchase at a small business.

The attacks we are talking about today can take many different forms. The digital economic side is definitely one of them, but there is also a social component to the Internet. When I think of the social component, I think about issues of privacy and of communications through, for example, social media. Again, Canadians have an expectation that the government is going to be there for them. Cyber-attacks take place in areas we all need to be concerned about. As I said, the more advanced we become, the more risk there is.

There are a lot of things that take place on the net that we need to be aware of and take action on. The exploitation of children is an example. That needs to be taken into consideration.

In the legislation, there is a very strong compliance component. As I raised, the minister would have the authority to make some things happen with our telecommunications companies and tell them to stop. I think that sort of action is necessary at times.

There is also a financial component so we can ensure a penalty is put in place as an incentive for people to abide by the legislation and the regulations, which are all there for one purpose and one purpose alone: to protect Canadians and institutions from risk. That

is why we are investing in cybersecurity, ensuring respect for the privacy of Canadians and supporting responsible innovation.

We will continue to protect Canadians from cyber-threats in an increasingly digital world. This legislation is one aspect of what the government is doing to accomplish that. I believe that state-sponsored cyber-threats are one of the greatest concerns and one of the reasons we need to work with allied countries. I made reference to the Five Eyes. There are democratic, free, allied countries that recognize the potential harm of cyber-threats sponsored through governments. This legislation really sinks its teeth into that.

I hope that all members will get behind this legislation so we can ultimately see its passage to the committee stage. An official opposition member has indicated there is a great deal of interest in reviewing the legislation, the idea being to come up with ways to ultimately make the legislation better.

● (1140)

**Mr. Arnold Viersen (Peace River—Westlock, CPC):** Mr. Speaker, I am frustrated with this bill given the fact that it does not lay out a lot of specifics. It states that there is a problem, and I think we all agree with that, but the government's solution to that problem is to hand the minister a lot of power so the minister can do amazing things. Is the member not concerned that the bill does not have the details we need to prevent some of the very things he was talking about?

I think about Ski-Doos and Bombardier, which is an iconic Canadian company. It has been the victim of one of these targeted cyber-attacks. I do not think there is anything in the bill that would have prevented that or held the people who perpetrated it to account.

**Mr. Kevin Lamoureux:** Mr. Speaker, I do not necessarily know the details of the case the member has referenced, but what I can say is that even the Conservative critic acknowledged that certain aspects of the legislation would ensure there are financial penalties and opportunities for the minister to virtually stop an action from taking place. Am I concerned that there is overreach? I do not personally believe there is, but I think there is some merit in having that discussion at the committee stage.

I posed a question to the member: If the concern is that there is too much power for the minister, what would the Conservatives do differently? I recognize the fact that in a cyber-attack, often it is necessary to take fairly strong action in an immediate fashion. I think all members recognize that fact. The issue is whether there is something the Conservatives would like to see to provide an additional sense of security.

[*Translation*]

**Mr. Simon-Pierre Savard-Tremblay (Saint-Hyacinthe—Bagot, BQ):** Mr. Speaker, I thank our colleague for his speech, which was a real voyage of discovery. One moment we were in Hollywood, and the next we were at Tim Hortons.

I will do him one better. I will take us on a journey across the Pacific all the way from China to the riding of Papineau. I worry about interference, as does our colleague, I am sure, because he supports a cybersecurity bill to reduce digital vulnerability.

*Government Orders*

Is my colleague concerned about the fact that, within the same time period, the federal Liberal association for the Prime Minister's riding of Papineau received donations from China and a Chinese bank got permission to set up shop in Canada?

I have a second question. Does the member believe in chance and coincidence?

[*English*]

**Mr. Kevin Lamoureux:** Mr. Speaker, I think Bloc members are hanging around the Conservatives too much. It is usually the Conservatives who go under all the rocks and have conspiracy theories.

I, for one, see the legislation for what it is. It is an attempt by the government to ensure that we can effectively deal with the threat of cyber-activities, whether they are state-sponsored or from individuals. That is a very strong positive and is absolutely not unique, as other countries around the world are doing likewise in bringing forward legislation of this nature.

In terms of the member's conspiracy theory, I will leave that for another member on another day.

**Mr. Gord Johns (Courtenay—Alberni, NDP):** Mr. Speaker, I think we all agree that Canada is ill-prepared to deal with cybersecurity threats. I am comforted to hear that we are all on the same page. However, we are falling far behind other similar jurisdictions, such as France and the U.K. Their ability to intercept and respond to cybersecurity threats is much more enhanced to protect their countries.

Again, we are glad to see this moving forward, but I am a bit concerned about the government granting ministers so much broad power, especially the Minister of Public Safety and the Minister of Industry. I just want an assurance for Canadians that these powers would not be applied unjustly to them. Also, would the member and his party be willing to work with the NDP to bring forward amendments at committee to make sure there are protections for everyday Canadians?

• (1145)

**Mr. Kevin Lamoureux:** Mr. Speaker, I suspect there would be a great deal of will to continue working with the New Democrats in the House in a minority situation. The NDP has taken a very responsible approach to dealing with the government-sponsored legislation. Where there are changes that make sense, I suspect the ministry would be open to how we could address concerns.

Having said that, it does not mean we are looking for NDP amendments. As it has been pointed out, whether it is the official opposition or the Bloc, this is legislation that we brought in today at second reading. We hope it will pass at some point so it can go to committee stage, where I expect there will be a great deal of interest from coast to coast on this legislation.

I look forward to the contributions of others and their ideas and thoughts going into it, like the member for Kildonan—St. Paul had regarding an annual report that comes from the minister and how that might be incorporated into the legislation. The sooner we can make the ministry aware of some of those ideas, the better it is.

Ultimately, it will go to committee, and there will be representatives from the minister's office there. It will be a wonderful oppor-

tunity to get the feedback we are all looking for. If there are chances to make it a healthier and stronger legislation, I am sure the government would act on that.

[*Translation*]

**The Deputy Speaker:** The hon. member for Saint-Hyacinthe—Bagot on a point of order.

**Mr. Simon-Pierre Savard-Tremblay:** Mr. Speaker, that is twice now that my colleague has accused me of subscribing to conspiracy theories. With all due respect, I would ask that he withdraw his remarks.

**The Deputy Speaker:** I understand the member for Saint-Hyacinthe—Bagot's request.

The hon. parliamentary secretary.

[*English*]

**Mr. Kevin Lamoureux:** Mr. Speaker, I will withdraw the comment.

**Mrs. Élisabeth Brière (Parliamentary Secretary to the Minister of Mental Health and Addictions and Associate Minister of Health, Lib.):** Mr. Speaker, 85% of Canada's critical infrastructure is owned by the private sector, provinces and non-governmental agencies.

Does my colleague think Bill C-26 will help standardize cybersecurity practices to better protect systems and services pertinent to Canada's cybersecurity?

**Mr. Kevin Lamoureux:** Mr. Speaker, as the member highlights, when we talk about infrastructure, the whole digital economy and what government does, it would be negligent not to recognize the significance of the private sector and how the private sector feeds into it. In fact, it is a major player of 80% plus. That is why, when we talk about the government's role, ensuring that the national infrastructure is safeguarded against cyber-threats is of the utmost importance. That is the essence of the legislation, along with ensuring that Canadians', business's and governments' interests are well served.

**Mr. Larry Maguire (Brandon—Souris, CPC):** Mr. Speaker, in regard to my colleague from Kildonan—St. Paul's speech, she talked about how the government has brought this bill forward with a lot of sticks in it and no carrots. I am looking for incentives that would improve it.

Is the government open to amendments on this particular bill? If so, what would be its theme to bring forward some issues to improve the bill's transparency?

• (1150)

**Mr. Kevin Lamoureux:** Mr. Speaker, I have made reference to the idea, and I hope it will be discussed at committee stage in terms of a reporting mechanism. I get the sense, based on questions for both me and the minister, that there is some concern related to that. We will have to wait and see if that comes forward through committee.

At the end of the day, I think it would be nice to see the legislation pass at some point, where the committee is given the opportunity to provide its recommendations and thoughts on the legislation.

**Mr. Daniel Blaikie (Elmwood—Transcona, NDP):** Mr. Speaker, before I begin my remarks, I request that you seek unanimous consent for me to split my time with the member for Windsor West.

**The Deputy Speaker:** Is there agreement for the member to split his time?

**Some hon. members:** Agreed.

**Mr. Daniel Blaikie:** Mr. Speaker, with thanks to the chamber, I am pleased to rise today to speak to Bill C-26.

Cybersecurity is a topic that is very much on the minds of many Canadians. It is something that many of us have had experience with in our personal lives, or we know somebody who has. Certainly, as MPs, we hear from folks who have fallen prey to various kinds of cyber-attacks online. We know it is a burgeoning criminal industry to take advantage of people online, grab their information and impersonate their identities. Canadians deserve to be protected from this kind of crime.

We also heard about the impact that cybersecurity attacks have had on our commercial industries. One of the examples that stands out in my mind of particular concern was the 2017 cyber-attack on Equifax, where the personal and financial information of thousands of Canadians was obtained illegally. It is an obvious concern for folks when they find out that a company they trusted with their personal information has been subject to this kind of attack.

We also know that our government has not been immune from these kinds of attacks. Hospitals and Global Affairs Canada have been the object of successful cyber-attacks. Earlier this fall, the House of Commons had a cyber-attack. MPs were warned about changing their email passwords for fear of information in their work accounts being exposed to outside eyes and ears that would find out what was going on in those accounts.

There is no question that it is a real issue. There is also no question, when we talk to experts on the file, that Canada is a laggard in respect to cybersecurity. There have been many debates in this place about the role of Huawei, for instance, in our 5G infrastructure. The government did finally take a decision on Huawei, I think the right decision, although late in the game with respect to our other Five Eyes allies. The idea with this legislation is that the government needs more legal authority in order to implement that decision. Of course, there are a number of ways it can do that.

The bill, as it stands, is not ready to go, but New Democrats are happy to send it to committee where we can hear from experts and try to improve it. When I say it is not ready to go, in my view, it is that for as long as it took for the government to reach a decision on Huawei, it clearly was not doing any work alongside its deliberations on Huawei to prepare for banning it. This legislation would largely give a broad, sweeping power to the Minister of Industry to decide later what exactly the government will have to do in order to ban Huawei and respond to other kinds of cyber-threats.

There is not a lot of detail in the legislation, and that is something we have seen from the government on other fronts. We have

### *Government Orders*

seen it on unrelated items, like the Canada disability benefit. It drafted a bill that had no content on the program. The attitude is “trust us and we will get it right later”. However, we also see a litany of problems with the way the government manages its business, whether we go all the way back to the SNC-Lavalin affair and the question of deferred prosecution agreements or other ethical issues that have come up in the context of this government.

I think Canadians are right to have a certain distrust of the government. The answer lies in mechanisms that impose accountability on the government, and those are very clearly absent from this legislation. In fact, not only are they absent from the legislation but the government also very explicitly exempts itself from some of the current types of accountability that do exist.

For instance, it exempts itself from the Statutory Instruments Act, which would make it possible for the parliamentary regulations committee to review orders that the minister may issue under the new authority granted to him in this act.

● (1155)

Therefore, not only would there be no new accountability measures commensurate with the new powers the government would be giving itself, but it would also be exempting itself from some of the accountability mechanisms already there. The government is also explicitly letting Canadians know its intention in the legislation to give itself the legal authority to keep those orders secret. Therefore, we have to contemplate the idea that there will be a whole branch of secret orders and laws that govern the telecommunications industry that Canadians will not know about, and the telecommunications companies may not have an adequate awareness of them.

Where I would like to go with this is to talk a bit more broadly about the Internet and about privacy rights on the Internet. When the new Canada-U.S.-Mexico trade agreement was signed, there was a number of provisions in that agreement that went too far in shoring up the rights of companies to keep their algorithms secret, for instance. There are other kinds of IP protections, or protections that are sold as IP but really mean that it is harder to get a transparent accounting of how companies operate on the Internet and of the artificial intelligence they use to navigate the Internet.

There is a way of dealing with the Internet that prioritizes secrecy for commercial purposes, but that same secrecy also breeds more opportunity for malignant actors on the web to go about their business and not have to worry they will have to expose what it is they are doing. Whereas, if we look to the European Union as another model, for privacy and conducting business on the Internet, there are a lot more robust protections there for the private information of consumers on the Internet, and there are a lot more reporting requirements for actors on the Internet.

*Government Orders*

The problem with the bill as it is written here is that it would be trying to fight secrecy with secrecy. When firefighters show up to a house that is on fire, they do not usually show up with a flamethrower. They show up with something else that can fight the fire instead of accelerating it.

I do not think Canadians, who are concerned about malignant actors on the Internet and the ways that they are able to exploit the dark corners of the Internet and the back doors of software, also think that the way to fight that is to let the government do it in secret without any reporting. Canadians are not thinking that, with less information available about actors within the digital space or government actions against cybersecurity threats, they are better off if they do not know what the actors on the Internet are doing, and they do not know what the government is doing about it.

The problem with the bill as written is that it would double down on the approach that we saw in CUSMA. It was about privacy for actors on the Internet and privacy for the government in how it deals with it. Instead, it could take a more open-source approach to say that the way forward on the Internet has to be that digital actors have to be upfront about the kind of business they are conducting on the Internet, the ways they do it and the algorithms they use. Governments, likewise, could then be pretty transparent about how they would deal with people who were non-compliant or who were breaking the rules.

New Democrats are concerned to see, along those broad lines, an approach to the Internet that says transparency and accountability, both for private actors and for public actors, is the way forward. Digital consumers deserve to have this information at their fingertips, so they understand what people are going to be doing with the information they enter on their computer, whether that is to purchase a book, get a loan or whatever kind of business they are doing on the Internet. They should have more rights to know how that information is handled, and the role of the government in keeping that information secure, rather than being told not to worry about it, because commercial interests have their best interest at heart, the government has their best interest at heart, and they do not need to know what is going on.

That is why the bill should go to committee, to be sure, because Canada does need its government to have the authority to implement the decision on Huawei and to do better in respect of cybersecurity. There is a lot of good work for committee members to do there, and a lot of amendments that ought to be made to the bill in order for it to pass in subsequent readings.

• (1200)

**Mr. Arnold Viersen (Peace River—Westlock, CPC):** Mr. Speaker, I share a number of the hon. member's concerns, but I want to ask him about some of the major threats we have seen in cybersecurity. I am frustrated because the government has a lot of the tools already at its disposal to go after people who are threatening our cybersecurity. We have seen the shutdown of pipelines and major companies across this country. Rogers Communications was shut down.

Is the member not at all concerned about the lack of ability of law enforcement to chase down the bad actors that are pursuing some of this stuff?

**Mr. Daniel Blaikie:** Mr. Speaker, there are only so many things that can be fixed with legislation. Legislation is a necessary component of the solution, but it is not sufficient on its own. We see that in many areas. Despite the fact that we have made good laws in this place against certain kinds of crime, nevertheless, those kinds of crimes persist, so of course enforcement is an important part of that question and requires the attention of and resources from government. When those resources are not made available, it matters very little the kinds of laws we pass in this place, because the other necessary component is on the enforcement side.

I share the member's concern for proper enforcement of the laws we pass in this place.

[*Translation*]

**Mr. Xavier Barsalou-Duval (Pierre-Boucher—Les Patriotes—Verchères, BQ):** Mr. Speaker, we are talking about Bill C-26, which deals with national security, and discussions about national security inevitably include the issue of interference from elsewhere, from other countries. Security threats can be internal as well as external.

With respect to external threats, there is a lot of talk right now about the possibility that China interfered in our elections. Earlier, some of our colleagues mentioned that, a few years ago, the Prime Minister received nearly \$70,000 in donations immediately after a bank that offers services specifically to Chinese Canadians set up shop in Canada. The donations, which were mostly from people with Chinese names, were made on the same day and within hours of the bank being authorized to open.

Does my colleague find that strange? Is he concerned that there might have been some kind of interference? It is hard to believe that this happened by accident and that it was all just a fluke.

**Mr. Daniel Blaikie:** Mr. Speaker, I thank my colleague for his question.

I think that type of coincidence is always a concern. We have mechanisms in place to launch investigations when warranted. I would encourage my colleague to submit his evidence to the authorities who could look into this, because that is the most appropriate way to ensure that the wrongdoing that the member mentioned in his comments has not taken place.

• (1205)

[*English*]

**Ms. Leah Gazan (Winnipeg Centre, NDP):** Mr. Speaker, my hon. colleague spoke during his intervention about the need for greater government accountability in the bill, and I am wondering if he could provide the House with an example.

**Mr. Daniel Blaikie:** Mr. Speaker, at the very least there has to be some kind of accounting for and public disclosure of the number of orders the government is making under these new powers. That is just one example, a very minimum reporting threshold.

The idea that any number of these orders could be made and Canadians would not even know they have been made or how many have been made is not acceptable. There has to be some reporting of the extent to which these powers are used, or there will be no factual basis upon which to evaluate whether the powers have been appropriate or adequate, or whether they need to change in the future.

**Mr. Brian Masse (Windsor West, NDP):** Mr. Speaker, I am please to speak today to Bill C-26, an act respecting cybersecurity, amending the Telecommunications Act and making consequential amendments to other acts.

It is really important to acknowledge that we are severely behind with regard to our protections in this matter. I am going to quote from myself, from when I once engaged the government and asked them this. "I am very concerned that we are not doing enough in Canada to protect the digital privacy of Canadians and am calling on the government to develop stronger frameworks and guidelines to improve cyber security in Canada. These are critical issues that must be addressed". They must be addressed for the benefit of Canada, as our economy and commerce are currently under threat, as is our personal privacy.

When did I do that? That was in 2016. From 2016 to today, with the digital changes we have had, is a lifetime of change.

I got a response from the government at that time, basically saying it would refer matters and let them play themselves out in court.

One of the most famous cases that came forward at the time involved the University of Calgary, which had reportedly paid \$20,000 in compensation to a group of organizations we do not know to protect the breach they had.

What has taken place over several different cases and also in our current laws has shown that it is okay to pay out crime and it is okay to pay out these types of requests for extortion and not even refer that matter back to the people whose privacy has been breached. We do not even have to report it as a crime to law enforcement agencies. It is very disturbing, to say the least. Getting this legislation is something, but it is still a long way off.

As New Democrats, we recognize very much that there needs to be balance in this. This is why I also wrote at that time to the then privacy commissioner of Canada, Jennifer Stoddart, about the cyber-attacks and data breaches.

There is concern about the amount of data and one's rights and one's protections and the knowledge one should have as an individual in a democracy. I do not think it is a conspiracy theory to have those kinds of concerns.

I would point to a simple famous case. As New Democrats are well aware, and I think other Canadians are as well, our number one Canadian champion of health care, Tommy Douglas, was spied upon by his own RCMP at that same time. That was in relation to bringing in Medicare. This is very well documented. We still do not have all the records. We still do not have all the information, and it is a very famous case.

Bringing in our number one treasured jewel, health care, led to a case where our own system was spying on an elected representative

### *Government Orders*

who was actually declared Canada's greatest Canadian by the public. We do not want to forget about those things because, when we are introducing laws like this, there is a real concern about one's ability to protect oneself and one's privacy, as well as the expansive conditions that are going to change, often with regard to personal privacy.

What also took place after that was that I was very pleased, in 2020, to put a motion forward at the House of Commons industry committee, where we studied, for the first time in Canadian history, fraud calls in Canada.

There are a lot of cyber-attacks through this type of operating system, and we need to remind ourselves that using this type of system, being our Internet service providers and the telecoms sector, is something that is done by giving up the public infrastructure and a regulated system of industry.

We have built a beast, in many ways, that has a low degree of accountability, and we are finally getting some of that restored. There are also some new programs coming in, like STIR/SHAKEN and other types of reporting that is required.

I want to point out that since we have done that, we have another report that will be tabled, or at least a letter. We have not decided yet, and there is still work going on, but we have had a couple more meetings in the industry committee about it and we have really heard lots of testimony that showed that there is more work that can and should be done.

A good example from the previous report that we did was recommendation number five, which went through sharing information between the RCMP and the CRTC. We have not seen the government act on it.

#### • (1210)

It is important to note that with this bill there has been a lot of talk about the types of things we can do internationally, as well. One of the things I would point out that I have been very vocal on, because I have had Ukrainian interns in my office for a number of years, is that we could use a lot of our leverage in terms of cybersecurity and training to help them to deal with the Russian hacking and other nefarious international players. That would not only help Ukraine right now in the war with Russia. It would also help with the other activity that comes out of this subsequently, which would help the world economies by having trained, solid professionals who are able to use their expertise and battle this with regard to the current state of affairs and also the future. This would be helpful, not only for the Ukrainian population but also for the European Union, Canada, North America and others, who will continue to battle more complex artificial intelligence and other cyber-attacks that take place.

One of the things I want to note is that in the bill, a proposed new section 15.2 of the act would give the Minister of Industry and the Minister of Public Safety the authority to make several types of orders. It relates to guiding TSPs to stop providing services if necessary. This is a strong power that we are pleased to see in this type of legislation.

*Government Orders*

What we are really concerned about, as the member for Elmwood—Transcona noted, is that there is no general oversight of the type that we would normally see on other types of legislation. Scrutiny of regulations was the one referred to. For those who are not familiar with the back halls and dark corners of Parliament, there is a committee that I was one of the vice-chairs of at one point in time. The scrutiny of regulations committee oversees all legislation passed in the House of Commons and ensures that the bureaucratic and governmental arms, including that of ministers, whatever political colour they will be of at that time, follow through with the laws of the legislation that is passed. Making this bill not have to go through that type of a process is wrong. I would actually say it is reckless, because the committee has to do a lot of work just to get regulatory things followed on a regular basis. It can be quite a long period, but there is that check and balance that takes place, and it is a joint Senate and House of Commons committee. It is unfortunate that the legislation tries to leave that out.

The legislation also does not have the requirement to gazette information in terms of making it public for the different types of institutions. That is an issue, and it also has a lot of holes when it comes to information that can be withheld and shared.

Why is that important with regard to confidence in the bill? It all comes down to the fact that many of the institutions at risk of being targeted involve not only the private sector, where we have seen not only abuse of customers themselves, or businesses with lax policies that do not protect privacy very well, but also others that have used abusive techniques and processes. Even right now, it is amazing when we think about the information in the process that is going on in the United States. The U.S. Senate is going to oversee the issue with regard to Taylor Swift tickets and Ticketmaster again. That is another one that has had a nefarious past with regard to privacy, information and how it runs its business. People can go back to look at that one, with Live Nation and so forth. At any rate, the U.S. is also involved in this.

I raised those things because it also comes from the soft things like that, which are very serious with respect to credit cards and to people's personal information that is shared. However, across the world and in Canada we also have municipal infrastructure and government institutions that are constantly under attack. That is very important, because it is not just the external elements with regard to consumer protection and business losses, which are quite significant and into the billions of dollars. It is also everything from water treatment facilities to health care facilities in terms of hospitals and utilities for power and hydro. All those elements can be used as targets to undermine a civilian population as well, and one of the things we would like to see is more accountability when it comes to those elements. There is definitely more to do.

One of the things I do not quite understand, and which I am pleased to see the government at least bring to committee, is what we could do to educate the population.

Our first intervention on this bill as New Democrats was several years ago, and it is sad that it is just coming to fruition now.

● (1215)

**Ms. Marilyn Gladu (Sarnia—Lambton, CPC):** Madam Speaker, I am a little concerned with some of the elements in Bill C-26

that seem overly broad. They give the government powers to secretly order providers to do things or refrain from doing things, without any transparency. Does the member share my concern?

**Mr. Brian Masse:** Madam Speaker, I do. For us to get fully engaged in this, we want full accountability, clarity and a playbook so everybody understands the rules. We want to deal with some of the stuff and provide some leverage for law enforcement and investigations to take place, but there has to be a set of rules and that needs to be backstopped by parliamentary oversight. Where it stands right now, it is not backstopped by parliamentary oversight.

**Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.):** Madam Speaker, I would like to follow up on that question. When the minister is called upon to instruct a provider to take a specific action, that would often be required because something has happened in the environment. If the minister does not have that authority, then the opposition might be somewhat critical of the minister not taking action.

I wonder if the member feels that it is necessary in the legislation, or does he believe we should have it, but we need to amend it in some fashion to ensure it is not abused. Is that what I am hearing from the member?

**Mr. Brian Masse:** Madam Speaker, absolutely, but if we are going to give some flexibility in power for the minister to act, it has to be responsibly met with oversight, and that has to be heavy oversight. That will provide the confidence.

That is why I wrote to the Privacy Commissioner right after I challenged the government back in 2016 to act on this. We have seen how long it has taken for it to act on this now, so we need to have that confidence. It is a two-way street. If we have the confidence of privacy and protection for people, with oversight, then I think people will be more willing to accept that there could be some changes with respect to how investigations take place.

**Mr. Mike Morrice (Kitchener Centre, GP):** Madam Speaker, a group of organizations, including the Canadian Civil Liberties Association, OpenMedia and Leadnow, have written an open letter calling for improvements to Bill C-26. One of the items they call out is that secrecy undermines accountability and due process.

The member for Windsor West spoke a bit about this in his speech. Could he share more about the suggested improvements that would ensure better public reporting as part of Bill C-26?

*Government Orders*

**Mr. Brian Masse:** Madam Speaker, I have a book that we use for privacy protection and it is available to everybody. It was written by Kevin Cosgrove. It is a playbook for people on how to protect themselves and their families from a whole bunch of different issues, whether it be WiFi, online banking, shopping, social media, a whole series of things. The reason I use that as a specific example is that a ton of education has to be done. That has to be done for this bill as well. There needs to be a defined playbook of accountability, like going to the Standing Joint Committee for the Scrutiny of Regulations and ensuring there is oversight for the minister. All those things have to be really enhanced to build the confidence so we all buy into this.

• (1220)

**Ms. Bonita Zarrillo (Port Moody—Coquitlam, NDP):** Madam Speaker, I want to thank the member for Windsor West for all his hard work on this. Definitely, when it comes to protecting Canadians, he is the right person to do it.

I wonder if he would expand on clause 15.2 with respect to no general oversight and what the risk is to Canadians if that is not in place.

**Mr. Brian Masse:** Madam Speaker, It has been fun to work with my colleague on some of these issues. We need a lot of public education related to this going forward.

That section again is just too weak. It provides too many holes. There should be a way to get back to a process of ensuring the minister is held to account. That is one of the things where we are looking to expand powers, but, again, we really need a lot more public education with respect to cybersecurity.

I know it is one of those issues that when we hear it, our eyes fog up, or they roll back in our heads and we think it is just too complicated for us, that there is always something happening, but we really need to engage Canadians on this. That includes engaging the government to ensure it understands that it has to teach residents about the bill and its repercussions as it goes forward.

**Ms. Julie Dzerowicz (Davenport, Lib.):** Madam Speaker, I will be sharing my time with the hon. member for Vaughan—Woodbridge.

It is a true privilege for me to add my voice to the debate on Bill C-26, an act respecting cybersecurity, on behalf of the residents of my riding of Davenport, many of whom have written to me through the years about their concern around cybersecurity and the need for additional protections at all levels of government.

This bill represents the latest step in the government's constant work to ensure our systems, rules and regulations are strong and as up-to-date as possible. That is especially important when dealing with a topic as fluid and rapidly evolving as cyber-technology. We have known for quite some time we would need to be constantly vigilant on this issue.

In 2013, the government established the security review program operated by the Communications Security Establishment. In 2016, we conducted public consultations on cybersecurity. In 2018, we released the national cybersecurity strategy. In 2019, we allocated \$144.9 million through budget 2019 to develop a critical cyber systems framework. In 2021, we completed an interdepartmental

5G security examination, which recommended an updated security framework to safeguard Canada's telecommunications system.

A cornerstone of the updated framework is an evolution of the security review program. It would allow for continued engagement with Canadian telecommunications service providers and equipment suppliers to ensure the security of Canadian telecommunications networks, including 5G. As a result of this multi-year work, to address these identified concerns and improve Canada's cybersecurity posture, including in 5G technology, we introduced Bill C-26.

The bill is intended to promote cybersecurity across four federally regulated critical infrastructure sectors: finance, telecommunications, energy and transportation.

Bill C-26 consists of two very distinct parts. Part 1 introduces amendments to the Telecommunications Act that would add security as a policy objective and create a framework that would allow the federal government to take measures to secure the telecommunications system. Part 2 introduces the critical cyber systems protection act, which would create a regulatory regime requiring designated operators in the finance, telecommunications, energy and transportation sectors to protect their critical cyber systems.

As I mentioned, 5G has the potential to be a transformative technology for Canadians. It promises to bring lightning-fast Internet speeds that are unlike anything we have experienced so far. The benefits of instant and real-time connectivity will be immediate and far-reaching for Canadians and Canadian businesses.

The COVID-19 global pandemic has underlined the importance of this connectivity, whether it is for virtual classrooms, work from home or keeping in touch with loved ones, but we need to be absolutely sure this technology is safe and secure as the technology is rolled out in Canada.

Canada already has a system in place to mitigate cybersecurity risks in our existing 3G and 4G LTE wireless telecommunications network. Since 2013, the Communications Security Establishment's security review program has helped mitigate risks stemming from designated equipment and services under consideration for use in Canadian 3G, 4G LTE telecommunications networks from cyber-threats.

*Government Orders*

Like previous generations, 5G technology will have new risks and vulnerabilities that will need to be addressed so Canadians can realize its full potential. 5G is considered more sensitive than 4G because it will be deeply integrated into Canada's critical infrastructure and economy, and will connect many more devices through a complex architecture. The deep integration, greater interconnection and complexity increase both the likelihood and potential impact of threats. That is why an examination of emerging 5G technology and the associated security and economic considerations continues to be very important.

The technical agencies of the Government of Canada, within the Department of Innovation, Science and Economic Development, and the safety and security agencies that fall within the Public Safety portfolio, Global Affairs Canada, National Defence and others, are all involved in the federal government's efforts to develop a made-in-Canada approach to ensuring the secure rollout of 5G wireless technology. Moving this bill forward will further that vital work.

In the meantime, our world-class national security and intelligence agencies continue to protect our country from a wide range of threats. As we know, those threats include a growing number of targeted attacks from state and non-state actors, including cybercriminals.

• (1225)

Canada's two main national security organizations, CSIS and CSE, which is short for Communications Security Establishment, are working tirelessly to mitigate these threats.

CSIS provides analysis to assist the federal government in understanding cyber-threats and the intentions and capabilities of cyber actors operating in Canada and abroad who pose a threat to our security. This intelligence helps the government to improve its overall situational awareness, better identify cyber vulnerabilities, prevent cyber espionage or other cyber-threat activity and take action to secure critical infrastructure.

For its part, the CSE is always monitoring for threats that may be directed against Canada and Canadians. The CSE is home to the Canadian centre for cybersecurity, which was established as a flagship initiative of the 2018 national cybersecurity strategy. With the cyber centre, Canadians have a clear and trusted place to turn to for cybersecurity issues. It is Canada's authority on technical and operational cybersecurity issues, a single, unified source of expert advice, guidance, services and support for the federal government, critical infrastructure for owners and operations, the private sector and the Canadian public. It helps to protect and defend Canada's valuable cyber assets and works side by side with the private and public sectors to solve Canada's most complex cyber issues.

For example, the cyber centre has partnered with the Canadian Internet Registration Authority on the CIRA Canadian Shield. The shield is a free protected DNS service that prevents users from connecting to malicious websites that might infect their devices or steal personal information. With the passage of the National Security Act in 2019, Canada's national security and intelligence laws have been modernized and enhanced.

As a result, CSIS and the Communications Security Establishment now have authorities they need to address emerging national security threats, while ensuring that the charter rights of Canadians are protected.

These updates are in line with CSIS's mandate of collecting and analyzing threat-related information concerning the security of Canada in areas including terrorism, espionage, weapons of mass destruction, cybersecurity and critical infrastructure protection.

The passage of the National Security Act also established stand-alone legislation for the CSE for the first time ever. With the Communications Security Establishment Act, the CSE retained its previous authorities and received permission to perform additional activities.

For example, the CSE is now permitted to use more advanced methods and techniques to gather intelligence from foreign targets. Under the CSE Act, CSE is mandated to degrade, disrupt, influence, respond to and interfere with the capabilities of those who aspire to exploit our systems and to take action online to defend Canadian networks and proactively stop cyber-threats before they reach our systems. It is also permitted to assist DND and the Canadian Armed Forces with cyber operations.

As Canada's national police force, the RCMP also plays a very important cybersecurity role. It leads the investigative response to suspected criminal cyber incidents, including those related to national security.

Cybercrime investigations are complex and technical in nature. They require specialized investigative skills and a coordinated effort. That is why, as part of Canada's 2018 national cybersecurity strategy and as a second flagship initiative, the RCMP has established the national cybercrime coordination centre, or NC3.

The NC3 has been up and running for over a year now. It serves all Canadian law enforcement agencies, and its staff includes RCMP officers and civilians from many backgrounds. Working with law enforcement agencies, government and private sector partners, the NC3 performs a number of roles, including coordinating cybercrime investigations in Canada.



*Government Orders*

All of this is backed up by significant new investments in the two most recent budgets. In budget 2019, we provided \$144.9 million to support the protection of critical cyber systems and we later invested almost \$400 million in creating the Canadian centre for cybersecurity, the national cybercrime coordination unit and increased RCMP enforcement capacity.

Whether it is nationally or internationally, I have full confidence in the abilities of all those in our national security and intelligence agencies who are working hard day and night to safeguard our cybersecurity and protect us from harm online. I am confident that Bill C-26 will go a long way to continue doing that.

● (1230)

**Mr. Eric Melillo (Kenora, CPC):** Madam Speaker, I appreciate the comments from the government member across the way.

In the debate today, a number of concerns have been brought forward around some of the ministerial powers included in Bill C-26, as well as the lack of accountability mechanisms. I think we have heard from all parties about the desire to bring forward amendments and improvements at the committee stage.

Does the member opposite have a willingness to work with members of the House to ensure that we improve this bill and make sure it achieves the results it intends to?

**Ms. Julie Dzerowicz:** Madam Speaker, I think our Minister of Public Safety was very clear this morning. Without question, every time the government takes additional, decisive action and puts additional measures in place, there has to be corresponding transparency and accountability. We absolutely need to make sure there is enough of that in Bill C-26 so we have the confidence not only of the House but of Canadians with regard to having the proper accountability and transparency in place.

[*Translation*]

**Ms. Louise Chabot (Thérèse-De Blainville, BQ):** Madam Speaker, I thank my colleague for her speech.

This bill still raises some serious concerns. The Bloc Québécois is prepared to support it so that we can examine and improve it in committee.

In 2021, in Canada alone, one in four businesses reported being the victim of a cyber-attack. We are the G7 country that has done the least in this regard. We spent \$80 million over four years for research and development, which is not much. Canada is lagging behind in that department. Cyber-attacks on businesses can be sudden and unexpected, and not every business has the money to invest in cybersecurity or protection mechanisms.

What will this bill actually do to help with and improve cybersecurity?

[*English*]

**Ms. Julie Dzerowicz:** Madam Speaker, I want to point out that we have been providing significant investment in critical cyber systems and cybersecurity. We did this in budget 2019 by providing \$144.9 million for the protection of our critical cyber systems in the areas of finance, telecommunications, energy and transport. We also invested almost \$400 million in the Canadian centre for cyber-

security, in the creation of the national cybercrime coordination unit and to increase our RCMP enforcement capacity.

The hon. member did a wonderful job in asking how we are going to make sure we work with the public and private sectors. The Minister of Public Safety was very clear this morning: This legislation is about filling in the gaps and providing a bridge for all of the different actors, both in the private sector and in the public sector, so we can work together to create more resiliency against any cyber-attacks in the future.

● (1235)

**Mr. Gord Johns (Courtenay—Alberni, NDP):** Madam Speaker, I think we all agree that the protection of Canada's cybersecurity needs to be improved. However, as we are hearing from the opposition, there are concerns around the broad powers the minister would have through this bill and concerns about everyday Canadians possibly being surveilled by their own government.

We have not heard assurances from the government as to how it will address that to ensure Canadians do not feel they will be victims of government overreach through powers given to the minister.

**Ms. Julie Dzerowicz:** Madam Speaker, this question has come up all morning. I think it is a very big concern, not only for the opposition but for this side of the House.

We want to make sure we get this right. We must ensure that we have very strong protections against cyber-attacks and have cyber-attack resiliency in this country. We also have to be very transparent about the additional powers and how they will be used.

**Mr. Francesco Sorbara (Vaughan—Woodbridge, Lib.):** Madam Speaker, I say good morning to all of my hon. colleagues, and I thank the hon. member for Davenport for her insightful discussion of this bill.

I am thankful for the opportunity to weigh in on Bill C-26, an act respecting cybersecurity, as we continue debate at second reading. Bill C-26 will take great strides to enhance the safety of our cyber systems and will make changes to allow for measures to be taken within our telecommunications system.

There are two parts to this act. Part 1 amends the Telecommunications Act to “promote the security of the Canadian telecommunications system” as a policy objective. An order-making power tied to that objective would be created for the Governor In Council, or GIC, and the Minister of Industry. That power could be used to compel action by Canadian telecommunications service providers if deemed necessary. With these authorities, the government would have the ability to take security-related measures, much like other federal regulators can do in their respective critical infrastructure sectors.

### *Government Orders*

The bill would enable action against a range of vulnerabilities to these critical systems, including natural disasters and human error. The Department of Innovation, Science and Economic Development would exercise regulatory responsibilities, and an administrative monetary penalty scheme would be established to promote compliance with orders and regulations made by the GIC or Minister of Industry. Once amendments to the Telecommunications Act receive royal assent, GIC or ministerial orders could be issued to service providers.

Part 2 of the act would create the critical cyber systems protection act, or the CCSPA. The CCSPA would be implemented collaboratively by six departments and agencies: the departments of Public Safety; Innovation, Science and Economic Development; Transport; Natural Resources; and Finance, as well as the Communications Security Establishment. They will all play a key role. Indeed, across the Government of Canada, there is a recognition that cybersecurity is a horizontal issue, and it should be addressed through a streamlined government response across sectors, all rowing in the same direction.

Schedule 1 of the act would designate services and systems that are vital to the national security or public safety of Canadians. Currently, schedule 1 includes telecommunications service and transportation systems. It also includes, in the finance sector, banking systems and clearing and settlement systems, and, in the energy sector, interprovincial or international pipeline and power line systems and nuclear energy systems.

Schedule 2 of the act would define classes of operators of the vital services and systems identified in schedule 1, as well as the regulator responsible for those classes. Operators captured in a class are designated operators subject to the act.

In line with the responsibility to exercise leadership in matters related to national security and public safety, the Minister of Public Safety would have overall responsibility for the legislation and would lead a number of CCSPA-related processes.

Decision-making by GIC under the CCSPA would ensure that a broad range of relevant factors, including national security, economic priorities, trade, competitiveness and international agreements and commitments, are considered when making decisions that have an impact across sectors. The CCSPA would also leverage regulators' expertise and relationships with entities they already regulate under existing legislation.

The Canadian centre for cybersecurity, or the cyber centre, is responsible for technical cybersecurity advice and guidance within Canada, and that would be no different under the CCSPA. It would receive resources to provide advice, guidance and services to designated operators in order to help them protect their critical cyber systems; regulators in support of their duties and functions to monitor and assess compliance; and public safety and lead departments and their ministers, as required, to support them in exercising their powers and duties under the act.

The CCSPA would require designated operators to establish a cybersecurity program that documents how the protection and resilience of their critical cyber systems will be ensured. CSPs must be established by designated operators within 90 days of them be-

coming subject to the act, that is, when they fall into a class of designated operators published in schedule 2 of the act.

• (1240)

Once established, the CSP must be implemented and maintained by the designated operator in order to keep it up to date and responsive to changing threats and evolving technology. CSPs must include reasonable steps to identify and manage organizational cybersecurity risks, including risks associated with an operator's supply chain, and the use of third party products and services. They must also protect their critical cyber systems from compromise, detect cybersecurity incidents that affect or have the potential to affect CCS and minimize the impact of cybersecurity incidents affecting critical cyber systems.

This legislation would also help confront supply chain issues. With the increasing complexity of supply chains and increased reliance on the use of third party products and services, such as cloud-based data storage and infrastructure as a service, designated operators can be exposed to significant cybersecurity risks from those sources.

When a designated operator, through its CSP, identifies a cybersecurity risk to its CCS in relation to its supply chain or its use of third party services or products, the CCSPA would require the designated operator to take reasonable steps to mitigate those risks. Taking reasonable steps to mitigate risk is understood to mean reducing the likelihood of the risk materializing by, for example, securing a supply chain by carefully crafting contractual agreements to gain more visibility into equipment manufacturing, or by choosing another equipment supplier. It can also mean reducing the impact of a risk that materializes.

*Government Orders*

Under the CCSPA, there would also be a new obligation to report cybersecurity incidents affecting or having the potential to affect critical cyber systems to the Communications Security Establishment, for use by the cyber centre. A threshold defining this reporting obligation would be set in regulations. This would provide the government with a reliable source of information about cybersecurity threats to critical cyber systems. The availability of incident reports would enhance visibility into the overall threat for the cyber centre. Findings from the analyses of incident reports would make it possible for the centre to warn other designated operators and any operator of a cyber system of potential threats or vulnerabilities, and it would help to inform Canadians of cybersecurity risks and trends, allowing one organization's detection to become another's prevention.

The CCSPA would also create a new authority for the government. Under the act, the Governor in Council would be allowed to issue cybersecurity directions when it decides that specific measures should be taken to protect a critical cyber system from a threat or known vulnerability. Directions would apply to specific designated operators or to certain classes of designated operators. They would require those designated operators to take the measures identified and to do so within a specific time frame. Failure to comply with directions could be subject to an administrative monetary penalty or an offence that can lead to fines or imprisonment. The CCSPA would also include safeguards to ensure that sensitive information, such as information that was obtained in confidence from Canada's international allies, is protected from disclosure.

All of this provides an overview of strong new legislation, which I hope I have adequately described in two distinct parts. I look forward to our continued debate of this landmark bill, and I encourage all colleagues to join me in supporting Bill C-26 today.

• (1245)

**Ms. Marilyn Gladu (Sarnia—Lambton, CPC):** Madam Speaker, I certainly agree that something needs to be done about cybersecurity in this country, but I am increasingly alarmed when I see that the bills continually coming from the Liberal government say ministers would have all powers to do whatever they want. There is no transparency because there is no public record. Then they say not to worry about what the government is really going to do because the Governor in Council, which is really cabinet, will decide afterward with no parliamentary oversight what will be done.

Does the member agree that the government needs to have parliamentary oversight and at least have this subject to the scrutiny of committees?

**Mr. Francesco Sorbara:** Madam Speaker, of course, fundamentally I believe in the oversight of government and ensuring that there are checks and balances.

When bills proceed to committee, obviously members within the pertinent committee should bring forth ideas to strengthen them, and that includes Bill C-26. Our main priority as MPs is to bring forth good legislation, to improve it and to protect the security of Canadians, whether it is their cybersecurity or health and safety. Bill C-26 would take us down that path.

[*Translation*]

**Mrs. Julie Vignola (Beauport—Limoilou, BQ):** Madam Speaker, clause 2 of the bill would enable the government to issue orders to force users of telecommunications services to use products or services that do not come from certain providers, including Huawei.

Does that mean that a person who has already bought a Huawei cellphone, because that is a product, will not be able to use it anymore and will have to buy a new phone much sooner than they expected?

What is more, since decisions will be made by order, does that mean that, under this bill, the government will be using orders to govern in this area instead of going through parliamentarians?

**Mr. Francesco Sorbara:** Madam Speaker, I thank my colleague from Quebec for her question.

[*English*]

In the preliminary version of the Library of Parliament's assessment of the bill, there is a reference that the bill specifies that no one would be entitled to any compensation from the federal government for any financial losses resulting from these orders. I am not certain if these orders pertain to exactly what the member was speaking to, but I do believe so. I would have to get back to the member on that specific question, because it is a pertinent question.

**Mr. Gord Johns (Courtenay—Alberni, NDP):** Madam Speaker, we are all in agreement here. We know that Canada needs to strengthen protections when it comes to cybersecurity to protect Canadians and Canadian businesses.

One thing we are all unified on over on this side in the opposition parties is that we need to have some assurances for everyday Canadians that these sweeping powers, broad powers that are going to be given to the minister, are not going to be applied to everyday Canadians in terms of surveillance.

I know we keep hearing from Liberal colleagues that they will get it to committee and will answer these questions. However, does my colleague not agree that the minister failed in bringing forward this legislation without addressing some of these concerns at all? This is fairly substantial legislation, and the Liberals have not been able to address any of the concerns we brought forward today around these very real concerns.

**Mr. Francesco Sorbara:** Madam Speaker, we must always protect the civil liberties and rights of Canadians. Any legislation brought to the House needs to pass that means test, if I can call it that.

With reference to Bill C-26, it is definitely required that we update our cybersecurity laws to reflect the ongoing changes in technology that have happened over the last number of years and the increasing use of cybersecurity, cyber-threats, increasing digitization that has been going on in the world, and the fact that Canadians are increasingly interconnected in this world.

We need to maintain checks and balances within the system and ensure that individual rights of Canadians are protected.

*Government Orders*

● (1250)

**Mr. Arnold Viersen (Peace River—Westlock, CPC):** Madam Speaker, I will be splitting my time with the member for Sherwood Park—Fort Saskatchewan, a good friend of mine.

Today I get to address Bill C-26, and right off the top I will say that I think this is dumb legislation. Why do I say that? I say that because I do not think that it has attempted to do what it has stated it would do. Generally I find that this is another piece of legislation, probably the third or fourth that I have spoken on in this session of Parliament, where I am frustrated with the government in that it does not seem to do the hard work of governing.

Governing is a matter of balancing the interests and coming up with a statement or something that is clear. On the rule of law, we would anticipate the public and anticipate what the rules ought to be and then look at the law, read the law somewhere and say, “Oh, that is what we are supposed to be doing.”

Again, here we have a piece of legislation where there is a clear, identifiable problem. Canadians have seen a number of issues around the country and around the world where cybersecurity is under threat. Canadians are asking the government to govern, to set some parameters and guidelines as to what the expectations are around who gets to participate in cyberspace and how we ought to operate in cyberspace.

We see in this piece of legislation the classic attitude of “We’re the government. We’re here to help. Trust us. We got this.” We do not trust the government. Particularly, the Conservatives do not trust the government to do the things it needs to do. We have seen it try to hand out billions of dollars to its friends. I mentioned the WE scandal. We have seen it hand out money to its friends over at Baylis Medical. We have ample evidence of why we should not trust the government.

When it comes to cybersecurity, it is also an area where I do not trust the government. The government has been in power for seven years, and we have watched it drag its feet with an inability to come to a decision, for a whole host of reasons, around the Huawei situation. Was a particular company allowed to participate in the building of the infrastructure of our Internet architecture?

This is a major issue. We told the government that we don’t think this Chinese Communist Party government-controlled company should be able to participate in the Canadian Internet infrastructure. We called on the government to ban the use of Huawei technology in our Internet infrastructure, yet it could not do it. It took the government years of dragging its feet, wringing its hands and doing a whole host of things. When the Liberals come forward with a bill like Bill C-26 and say to trust the minister and that they will get this right, I am sorry, but we do not trust the minister to get this right.

We have seen a number of security threats challenging our basic infrastructure. One we should really take note of, which was fairly recent, is the shutdown of a particular pipeline. We saw a dramatic spike in fuel prices across North America because the cybersecurity of a particular piece of pipeline infrastructure was not to the state that it should have been. This, again, comes to the fact around trusting the government to do its job, particularly this government.

One of the key roles of government in Canada and anywhere is the maintaining of peace and security, and we have a military, a police force and a judicial system for that. A growing area where we need to be concerned about peace and security is in cyberspace.

● (1255)

We should be able to feel that our property should not go missing. We should be able to own property, and it should be able to be maintained by us, all of these kinds of things. We expect the government to put forward registries so we can register our property, so that, if it goes missing, the government has a registry of it and we can use that to get our property back. It cannot just be expropriated from us, all of these kinds of things.

In the same way, that is increasingly a part of cybersecurity. The ownership of things in cyberspace, the ownership of websites and the ownership of even our own Twitter handles, for example, are increasingly things that are deemed to be cybersecurity.

The government seems to be lacking in the ability to protect Canadians’ cybersecurity.

There is an iconic Canadian company, Ski-Doo. I do not know if people are snowmobilers, but I do enjoy snowmobiling, and Ski-Doo is an iconic Canadian company.

I do not know if people know this but, recently, Ski-Doo has been the victim of a cyber-attack and has lost control of its entire dealership network. Its own computer system has gone down. It has not been able to get it back. Somebody else has control of it now and it has not been able to get it back.

These are the types of things that I think are crucial. When one is going to bring in a bill that talks about cybersecurity, these are the kinds of things the government should be trying to keep secure. This is Canadian property. These are Canadian identities. These are Canadian brands. These are the things we need to ensure we can prosecute, that we can track these people down who are doing this kind of thing and that we can ensure cybersecurity.

I guess that is where I get a little frustrated with a bill like this. It says a lot of nice things at the top of it. The government comes here with a blanket statement around how it is going to defend cybersecurity, how cybersecurity is important and how we should all vote in favour of this particular bill. I imagine that we will.

However, the bill does not necessarily tell us what we are going to do. The banning of Huawei is not necessarily laid out in this. There are no criteria as to what the expectations are for companies to operate in this space, in terms of what they can be tied to and what they should not be tied to. It is just, “Trust us. We are the government and we are here to help.”

In addition, we have seen over the last number of years the opportunities for the government to put resources into law enforcement's ability to track some of this down. We can see changes to the Criminal Code, to ensure that some of these malware attacks or ransomware attacks could be tracked down and prosecuted here in Canada. This is a major concern for companies looking at investing in the world. They look at a country's ability to protect them from a cyber-attack but then also to prosecute those cyber-attacks.

I have a friend who works for the Calgary city police. He works in cybercrimes. He often works with police forces from around the world to track down folks who are using ransomware on Canadian companies.

He tells me they rarely, if ever, prosecute in Canada because our laws are so non-distinct around this that it is impossible to prosecute. Because these are multi-jurisdictional crimes, they will often take the prosecution of this to a jurisdiction that has better laws. He says he will work with 23 law enforcement organizations and they will bring a case in Europe, in eastern Europe or in Israel, because those places have much better laws to protect cybersecurity.

• (1300)

**Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.):** Madam Speaker, I am glad the member will be voting in favour of the legislation going to committee. Hopefully many of the concerns he raises on the issues surrounding the worthiness of the legislation, will be addressed at that stage.

The legislation would empower the minister to be able to take actions. It would allow for financial penalties. It would allow for us to deal with cyber-attacks from a legislative perspective. That does not necessarily mean that this is the only thing we have done over the last number of years. There has been a great number of financial resources, individuals, committees and so forth ensuring our industries are protected.

This is yet another step forward in dealing with cyber-attacks, keeping us consistent with other allied countries. I am wondering if the member would acknowledge the importance of moving forward with allied countries in dealing with things, such as cyber-attacks?

**Mr. Arnold Viersen:** Madam Speaker, I am hopeful that this bill would get us in line with other countries from around the world because, increasingly, Canada is left out of the discussions around cybersecurity.

We are no longer invited to some of the many important forums that do take place in battling this. If that is what this bill is attempting to do, to bring us in line with some of these other countries, I hope that is the case. However, I would note, I was talking to my friend with the Calgary Police Service who said that Canada is increasingly not the jurisdiction where they pursue these prosecutions because we are so lacking in good legislation to protect our cybersecurity.

[Translation]

**Mr. Alexis Brunelle-Duceppe (Lac-Saint-Jean, BQ):** Madam Speaker, I thank my colleague for his speech.

### Government Orders

He talked about trust in the government or perhaps a lack of trust. In the current global context, there is interference by countries like China. We know that the RCMP has launched investigations into 11 electoral candidates. In fact, we also know that on July 7, 2016, the Prime Minister authorized a Chinese bank to do business on Canadian soil. At the same time, on July 6 and 7, 2016, the Papeineau Federal Liberal Association received more than \$70,000 in donations in 48 hours.

Is that not a reason to lose trust in the Prime Minister and the government?

[English]

**Mr. Arnold Viersen:** Madam Speaker, that is another prime example among many of why Canadians do not trust the Liberal government, whether it this particular case of accepting interesting money for an approval; the Huawei decision that needed to be made; the WE Charity scandal, where the Prime Minister was trying to give an organization \$1 billion, an organization that had funded nearly half a million dollars to his personal family; or the sweetheart deal with Baylis Medical.

Over and over again, we see that the government is not trustworthy. When it comes forward with bills that do not have a lot of details and that just give blanket permission to cabinet ministers, I am sorry, but we do not trust it.

**Ms. Bonita Zarrillo (Port Moody—Coquitlam, NDP):** Madam Speaker, today in the House we have heard the NDP speak about its concerns, also about its concerns with oversight.

Are Conservatives also in support of those changes around oversight?

**Mr. Arnold Viersen:** Madam Speaker, yes, that is for sure the case. We are in support of more oversight. We would like to see a detailed bill, not a bill that just says that it would give the minister broad powers to do all the things.

That is not governing. That is not providing legislation. That is basically saying, "We love puppies. You should support us because we love puppies."

• (1305)

**Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC):** Madam Speaker, I appreciate the opportunity to speak in the House today to a very serious subject, cybersecurity and the security of our country in general.

I will say, on a lighter note, that my friend from Peace River—Westlock spoke about snowmobiling companies and cyber-attacks. I have some personal experience with snowmobiling at his house, and I would say that the government's approach to security is the equivalent of driving a snowmobile over a four-foot retaining wall, which may or may not have happened the last time I tried to drive one of those machines.

### *Government Orders*

The situation of security in this country is very much worth the House taking note of. For much of the time that I have been engaging with and following politics, the primary area of security we would talk about would be concerns about our readiness for and our response to the threat of terrorism. However, it is important to take stock of how things have changed and the fact that, while there are still concerns about terrorism and how we respond to potential acts of terrorism, the primary security threat we face as a country, and indeed that the western world faces, is the threat of foreign state-backed and directed interference in our national affairs. Our abiding concern should be the reality that various foreign states are trying to shape and interfere with our democratic life to try to bend not only our government institutions, but also our civil society institutions, toward their desired objective.

Members of the government have said that the purpose of this interference is to cause total chaos and confusion. We should acknowledge that there are some cases of foreign interference that are aimed at causing chaos, but very often it is about simply trying to subvert and control the direction of institutions toward the will and the interests of that particular foreign power. We have discussed how the Chinese Communist Party is the biggest player when it comes to foreign state-backed interference, but it is far from the only player.

We have seen reports about Chinese government interference in our elections. There have also been recent reports about death threats from the Iranian regime targeting individuals in Canada. There are various other countries that CSIS and other organizations have identified as being involved in this activity of trying to interfere with, subvert and direct Canadian institutions, government really at all levels, as well as civil society organizations, universities and the like, toward their objective.

This kind of invisible, or sometimes a little more visible but often hard to detect, interference in the direction of our national life toward objectives that are not consistent with the objectives Canadians have established is a great threat to our security and our sovereignty. It is something that we should all be seized with and working to respond to.

Part of the context as well is that we are in what some analysts have described as a second cold war. Of course, there are many features of the current conflict between democratic and authoritarian values that are different from the last Cold War, but we have this reality of intensifying global competition between two different value systems that are represented by different countries at different times, and we have countries that are in the middle that are being pulled in different directions.

I tend to think that kind of cold war frame is a reasonably useful way of understanding the current tensions we face in the world. In the context of those tensions, we see how powers with political values that are fundamentally different from ours, where governments are trying to protect their own position, are trying to project their influence around the world. Again, this requires vigilance. It requires a strong response from Canada.

I have been struck by some of the recent comments from the Prime Minister on these matters. I think he has been showing a real lack of transparency around acknowledging what he knew when,

and refusing to answer direct questions from the opposition about foreign interference, but he has also stated quite openly the reality that we have a serious problem with foreign interference. This is a reality that opposition members, in particular in the Conservative Party, have been raising for years. We have been asking the government to do more. We have been calling for strong legislative frameworks to respond to the problem of foreign state-backed interference.

• (1310)

We have also sought to elevate the voices of victims of foreign interference, people who have faced threats and intimidation from foreign state actors to try to silence their advocacy, which those foreign state actors see as contrary to their interests. It has been widely reported some of these victims really struggle to actually get proper support. They often get the runaround.

They go to their local police force, which does not necessarily have the capacity to handle a foreign state-backed organized campaign of threats and intimidation. Do they go to Global Affairs? Do they go to CSIS? Do they go to the RCMP? There can be a bit of confusion and passing of the buck concerning support for these victims of foreign state-backed interference.

We have a lot of work to do in legislation and policy, and our preparedness in general and our understanding of these issues. It is critical that we step up to strengthen our understanding of and response to the threats facing our country.

One thing we need to see more from the Prime Minister and the government is transparency because being transparent about this reality can help to counter the impact of that foreign interference. If we know it is happening, if we know what it is directed toward, then we can respond more effectively.

This is not only a responsibility of the federal government to respond to. Provincial and municipal governments need to be aware of the issues of foreign interference. Our universities need to step up as well. Private companies need to be aware of the risks around interference, theft of technology and the ways in which certain things may have a dual military use. There needs to be a broader awareness of this threat to the national interest, a threat to our values across all sectors of society, and a broader response to it.

The government has an important role to play in leading the response and making changes at the national level. We have been far behind, as far the national government goes, in responding to these threats. The Conservative opposition has been calling for a response to foreign interference for years. Now we are seeing the government start to talk about it a bit more.

I noted in some of the language in the Indo-Pacific strategy, for example, the government is starting, or trying, to sound a bit more like Conservatives in the way it talks about some of the challenges confronting us and the steps we need to take in the Indo-Pacific region. While the government is adopting some of that language, it is failing to substantively adjust its approach.

*Government Orders*

We have a bill in front of us today that deals with one avenue where we need to be engaged with and responding to the problem of foreign state-backed interference, and that is the issue of cybersecurity. I will be supporting this legislation at this stage to see it go to committee, mainly because we clearly need a new cybersecurity bill. We clearly need a new framework. The committee study will identify some of the significant gaps we see in the legislation right now, the ways the legislation needs to be improved and possibly the many additional steps required. I will just note that it is far past due that we have some kind of proposal for a framework on cybersecurity that, in a way, gives the committee the opportunity to add to and build on what the government has initially put forward.

This is really the first time we see any kind of legislation proposed by the government that substantively touches on this emergent problem of foreign state-backed interference. We need a much broader range of responses from the government. We need so much more to be done to counter this major security threat.

This is about preserving our country. It is about preserving the integrity of our institutions. It is about defending the principle that the direction of our democracy and the direction of our society should be shaped through the open deliberation of Canadians, not by foreign powers who have particular interests that may be contrary to our interests who are trying to push and pull that discussion in their preferred direction.

Having this framework that opens the door for the committee to discuss further, fill in some of the gaps and try to push the government to have greater specificity in the framework around what they are going to do provides us with the opportunity to do that. This is late, lacking in detail and really a small piece of the much broader picture that is required.

The government has been so delayed. I mentioned the decision around Huawei. We were way behind all of our allies in making the decision. It is important now, finally, at this late stage where the government is starting to mention the problem, that we actually see concrete action. Conservatives will be pushing the government to act in line with some of the words it has been saying.

• (1315)

**Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.):** Madam Speaker, I would just correct the member. Yes, this legislation is very important and we hope to see it get to the committee stage where it will no doubt be well discussed and debated. There will be presentations where members can digest information and see if there are ways in which we can improve upon the legislation. However, to try to give an impression that this is the only thing the government has done on the issue of cyber-threats is a bit of a false impression.

Not only have we been seeing a great deal of dialogue and actions from different departments to date in the form of formalized advisory groups, but we have seen literally tens of millions of dollars, not to mention the other incentive programs that were there, for the private sector, for example.

I wonder if the member would not agree that this issue is not new and this is just one very important aspect in taking a step forward.

**Mr. Garnett Genuis:** Madam Speaker, the member is correct that this is not a new issue. That is precisely why I think the government is very late in coming to the table. The issue of foreign interference, which is part of the context of the cyber-threats we face, is also not a new issue. Again, we have been calling for action from the government, but we have not seen other action from it. The member says that the Liberals have done all these other things, such as maybe giving some money over here or over there, but he evidently could not articulate specific measures that the government had taken.

We are behind when it comes to defending our security. We are behind what we should have known much earlier. We are behind our allies. We were the last of the Five Eyes and very late to step up on recognizing the risks associated with Huawei.

When it comes to foreign interference, I will challenge the government on one point: Why has the government not expelled foreign diplomats involved in interference and intimidation in Canada? That would be a simple step and the government has not taken it.

[*Translation*]

**Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ):** Madam Speaker, the bill before us seeks to reinforce our security systems and may affect critical infrastructure in Quebec such as Hydro-Québec. I always think about the Conservatives and their famous great energy corridor. That is the type of project in which the federal government could appropriate provincial responsibilities and critical infrastructure in the name of national security. This sets off major alarm bells in my mind.

Can the member reassure me about the Conservatives' intentions? Can he assure me that if they come to power some day, they would not misuse legislation like this piece of legislation?

[*English*]

**Mr. Garnett Genuis:** Madam Speaker, the member asked what we would do if we were in government. We would make the right decision on every one of those.

With respect to the particulars the member raises with respect to what powers the federal government would have in intervening with provinces, this is an important issue for the committee to look at. I am supporting this legislation because we need to have a cybersecurity framework in Canada. It is important that this goes through to the committee and that those issues be looked at there.

I did not have time to go into it, but there are a significant number of problems in the legislation that do have to be worked out by the committee. No doubt there has to be a role for federal leadership around security, but it has to be a constructive, collaborative relationship, because there are steps for other levels of government. We see foreign interference at the very granular local level, so that collaboration across levels of government is really important.

*Government Orders*

**Mr. Larry Maguire (Brandon—Souris, CPC):** Madam Speaker, this morning my colleague from Kildonan—St. Paul made an excellent presentation on this bill. She talked about the transparency that may be lacking in certain areas and the effects on small businesses and how they may not be able to afford the cost like a larger company. I wonder if my colleague could expand on that.

**Mr. Garnett Genuis:** Madam Speaker, that is an excellent point. I did not have a chance in my remarks to talk specifically about the transparency issues. Again, we need to support this bill through the second reading stage out of agreement with the general principle that we need to do more on cybersecurity, recognizing how far behind the government has been.

However, there are significant issues with respect to ensuring transparency. There are significant issues on whether the bill is clear and specific enough about the steps that are required, instead of just leaving it, as we see often with the government and legislation, and giving an open-ended blank cheque to the government.

There are definitely issues. This requires a detailed committee study. I hope Conservative proposals will be adopted and we will be able to strengthen the bill as a result.

• (1320)

[*Translation*]

**Ms. Kristina Michaud (Avignon—La Mitis—Matane—Matapédia, BQ):** Madam Speaker, I will begin by saying that I will be sharing my time with the hon. member for Abitibi—Témiscamingue.

I am pleased to speak to this bill, which, I must say, was eagerly awaited by my party.

The Standing Committee on Public Safety and National Security had the opportunity to study the issue of cyber security. We heard from experts in this field, who told us what they think about Canada's cyber security preparedness or posture. The idea came from my Conservative colleagues, and it was a very good one.

Given what is happening in Ukraine with the Russian invasion, we know that there are still military threats in the 21st century. However, we are also dealing with the emergence of new technologies that pose non-military threats. I had the opportunity to talk about these non-military threats at the Organization for Security and Co-operation in Europe Parliamentary Assembly last week in Warsaw, Poland. I discussed non-military threats and how different countries must prepare for or guard against them.

What the Standing Committee on Public Safety and National Security heard is how difficult it is to prepare for these threats, because they are evolving so quickly. No one had anything particularly positive to say about Canada's preparedness.

I think that the willingness is there, and that is what the experts told us: Canada is trying to prepare for and guard against potential cyber-attacks. I said "potential" cyber-attacks, but they are already happening. We know there have been cyber-attacks on various infrastructure and companies in Quebec and Canada, especially in the private sector, in the past. Canada is not as prepared as it could be to face these attacks, but we were told that it may never be totally

prepared. The same is true for all countries because, as I said, the technology is changing so rapidly.

For this reason, I think that adopting a cybersecurity framework is an extremely positive step. That is what the government promised. In its national cyber security strategy, it pledged to better regulate cyber systems in the federally regulated private sector. The 2019 budget earmarked \$144.9 million to develop a new framework to protect critical infrastructure. That is exactly what the two main parts of this bill do. They are aimed at strengthening the security of the Canadian telecommunications system.

Part 1 of the bill amends the Telecommunications Act to add the promotion of security, authorizing the government to direct Internet service providers to do anything, or refrain from doing anything, that is necessary to secure Canada's telecommunications system. Part 2 enacts the new critical cyber systems protection act to provide a framework for the protection of critical cyber-infrastructure and companies under federal jurisdiction.

The act is essentially a regulatory framework. As my colleague from Abitibi—Témiscamingue mentioned earlier in his question to our Conservative colleague, we will have to see what impact this bill could have on Quebec, especially companies and organizations like Hydro-Québec, since it designates interprovincial power line systems as vital services and vital systems. More on that later.

We will also have to see in committee whether the vast regulation-making powers provided for in Bill C-26 are justified or whether they bypass Parliament for no reason. Certain groups that raised concerns in the media have contacted us as well. Their concerns about this bill are well founded. I will get back to this a little later on.

I would say that it is important to proceed carefully and properly with this bill. Any amendments made to the bill will have a direct impact on every transmission facility in Quebec, including those that will soon be built in my riding to offer adequate cell service to those who are still waiting. Some Canadian ridings are unfortunately still without cell service in 2022. Since my riding is one of them, the bill will have a significant impact.

• (1325)

Local telephone service providers, IP-based voice services, Internet service providers, long distance providers and wireless services will be subject to the amendments to the act.



*Government Orders*

This means that the amendments would allow authorities to secure the system if there is reason to believe that the security of the telecommunications system is under threat of interference, manipulation or disruption. In that case, telecommunication service providers could be prohibited from using or supplying certain goods or services.

As I understand the wording of the bill, which is rather complex, telecommunication service providers could even be prohibited from supplying services to a specific individual. It is important to realize that these are vast powers, and I hope that, when the bill is sent to committee for study, it will be detailed enough to include the factors that will be taken into account before such powers are granted.

As I was saying earlier, the act will make it possible to designate certain systems and services under federal jurisdiction as critical to national security or public safety. The new Critical Cyber Systems Protection Act will protect critical cyber systems in the private sector.

What, then, is a critical cyber system? I found it difficult to find a clear definition in French of what a critical cyber system is, but the government defines the term itself in the bill. It appears that it is a “system that, if...compromised, could affect the continuity or security of a vital service or vital system.”

The bill lists six vital services and systems in its schedule. These obviously include telecommunications services, interprovincial or international pipeline and power line systems, nuclear energy systems, transportation systems that are under federal jurisdiction, banking systems, and clearing and settlement systems.

These are the areas this bill addresses. That is a lot to verify, and several actors are involved. Several ministers will be involved in the regulatory process after that, so it is important to study the bill carefully.

At this stage, a number of questions arise. For example, what impact will the bill have on certain interprovincial infrastructures, such as power lines and power grids? The act could impact Hydro-Québec and other non-federal infrastructures, such as aluminum smelters. As I understand it, the bill itself would designate interprovincial power lines as a vital service. That could have an impact.

In principle, the bill is not a problem for my party. When we call experts to testify before the committee, we will be able to determine whether or not it will have a positive impact. I think it could be very positive, but we need to look at its scope.

The Bloc Québécois has often supported the government in its efforts to ensure stricter control of broadcasting for certain vital infrastructures that could be in the crosshairs of foreign nations. Let us consider China and Russia, as I mentioned earlier. There is the Huawei saga and the development of the 5G network. The government's indecision for so many years proves that it would have been better to act beforehand rather than to react to the current situation. China's increasing power and its attempts at interference on several occasions, as well as Canada's vulnerabilities in terms of cybersecurity, are real. For example, we know that Hydro-Québec has been a potential target for Chinese espionage. The same could happen directly in our infrastructures. I think that this bill is relevant. We are very happy that the government introduced it. That is why the Bloc

Québécois will vote in favour of sending the bill to a parliamentary committee so that we can hear what the experts have to say.

I would like to take these final moments to talk about the concerns voiced by certain groups. Professor Christopher Parsons of the University of Toronto said that the bill was so imperfect that authoritarian governments around the world could cite it to justify their own repressive laws. That is a worrisome statement. I will elaborate during questions and comments.

• (1330)

**Ms. Marilyn Gladu (Sarnia—Lambton, CPC):** Madam Speaker, I thank the member for her speech.

My question is the following. Is the member concerned that this bill gives too much power to the federal government and the minister?

**Ms. Kristina Michaud:** Madam Speaker, yes, that is a concern.

It was mentioned by the University of Toronto professor I cited earlier and certain groups that seek to protect individual freedoms. This bill may give too much power to the minister. We will have to properly study it in committee.

We must bear in mind that this bill seeks to secure and protect Canada's critical infrastructure. I believe that the government is acting in good faith. It is prepared to authorize the circulation of some information so we can help one another and safeguard businesses from potential cyber-attacks. I believe it is a good objective. We will have to ensure that there is nothing sinister about wanting more information.

[*English*]

**Ms. Bonita Zarrillo (Port Moody—Coquitlam, NDP):** Madam Speaker, my question for the member is around protection of seniors. I wonder if the member has some comments on how the bill would protect vulnerable groups, like seniors, from scams.

[*Translation*]

**Ms. Kristina Michaud:** Madam Speaker, that is an excellent question.

Based on what I have seen of the bill so far, I could not say. Quite honestly, I have no idea if this bill will do more to protect seniors from scams.

*Government Orders*

I know these kinds of scams are happening in my riding in the Lower St. Lawrence region. People call seniors, posing as grandsons in custody or living in another country. They ask their victims to transfer money because they need it right away, and some seniors fall for it.

I have no idea if this bill will help with that kind of thing. If not, the government really should do something to put a stop to it.

**Ms. Monique Pauzé (Repentigny, BQ):** Madam Speaker, I thank my colleague for her excellent speech. Her understanding of all these things is much greater than mine.

The member talked about interference and disrupting essential infrastructure, of course, as well as cyber-attacks from other countries or even individuals. My colleague also shared what experts told the committee. To hear them tell it, Canada's security system is a long way from being secure.

I would like my colleague to comment on that.

**Ms. Kristina Michaud:** Madam Speaker, indeed, the committee has heard from several experts on this subject. They told us that there is currently nothing to force companies, whether they are federally regulated or not, to report when they are victims of cyber-attacks, for example. They can just not report it and try to work through it on their own, even though there are authorities in place to help them through these kinds of events.

The experts were telling us that it might be worth having a framework that forces companies to work with the government or cybersecurity bodies to report and help prevent attacks so that a solution can be found. My understanding of the bill is that it would create a framework to compel federally regulated companies to do exactly that. I think that is a very good idea. It follows through on what the experts were proposing in committee.

**Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ):** Madam Speaker, I am pleased to rise to speak to Bill C-26, which will strengthen the security of critical infrastructure and Canada's telecommunications system.

Since June, many experts have been working to learn more about the provisions of this act and assess the value of what the government is proposing.

First, this bill is not structured in the usual way. I see that the urgent need to manage cybersecurity has been taken into account. This bill would give the minister new responsibilities, but the Governor in Council would also be able to act. The law is essentially a regulatory framework that will enable the government to make regulations to ensure the security of critical cyber systems.

I want to focus on the second part of the bill, because passing it will create a new law, the critical cyber systems protection act, which will provide a framework for the protection of critical cyber-infrastructure or businesses under federal jurisdiction. The affected sectors of our economy are identified as designated operators. It is easy to determine which businesses and organizations are affected.

The government has done well to specify who will must comply with the obligations: persons, partnerships or unincorporated organizations that belong to any class of operators set out in schedule 2 of the new law. Those classes will be identified by order.

Each class of operators will be assigned a corresponding regulator, such as the Minister of Innovation, Science and Industry, the Minister of Transport, the Office of the Superintendent of Financial Institutions, the Canadian Energy Regulator, the Bank of Canada or the Canadian Nuclear Safety Commission.

Schedule 1 of the new act sets out the vital services and vital systems that will form the basis of these designations, which may be added at a later date: telecommunications services, interprovincial or international pipeline and power line systems, nuclear energy systems, transportation systems that are within the legislative authority of Parliament, banking systems, and clearing and settlement systems.

I would like to draw my colleagues' attention to Hydro-Québec. An important part of the bill that has the Bloc Québécois concerned is the part on vital services and vital systems, which could potentially involve interprovincial power lines and distribution networks. It is of paramount importance that this section of the bill be studied and clarified in committee to assess whether this will affect Hydro-Québec and, if so, how.

However, we are not against the underlying principles and objectives of securing and protecting interprovincial infrastructure. Hydro-Québec reportedly suffers more than 500 cyber-attacks a year, or roughly 41 attacks a month. That is more than one attack a day. This could jeopardize our power grid, putting the life and economic health of every Quebecker at risk. It could also jeopardize customers' personal information, although that is generally a secondary target in any attack against a publicly owned energy corporation.

Although Hydro-Québec has managed to fend off these cyber-attacks and protect itself by investing in systems, firewalls and employee training, why should we not take proactive measures? Not only is it very time-consuming for businesses like Hydro-Québec and Desjardins to protect themselves and react to the constant onslaught of cybersecurity attacks, but it is also very expensive. Hopefully, this bill will help prevent or limit these attacks by taking a proactive approach and regulating and promoting new cybersecurity frameworks among Internet service providers. This is particularly important in light of the increased threat to our infrastructure from bad state actors such as Russia or China.

Hopefully, unlike today, businesses will have resources they can consult for information about cyber-attacks.

This is also a national security issue. These states have become emboldened not just by the Canadian government's passive reaction, but also by the regulatory void. We need only think of Huawei and the threat it represents, as well as the damage it has caused to the national security of countries around the world, especially in Africa. The examples are quite striking. China has passed a law forcing all businesses to contribute to the advancement of the objectives of Chinese intelligence services, which is particularly alarming when we consider that this country uses coercive diplomacy, blatantly disregarding international standards.

Even though the federal government has finally banned Huawei technology, the decision was preceded by many years of uncertainty because of the pressure, power and influence that China could unfortunately bring to bear on us.

• (1335)

This decision showed how vulnerable we are to malicious actors on the world stage. That is why we need a regulatory framework, a way to respond to cybersecurity threats, particularly from foreign powers that are in a position of power and use the weakness of others to advance their own positions.

I met this morning with representatives from Shakepay, a Quebec-based financial technology company that operates a platform dedicated entirely to bitcoin, with over one million Canadian customers. One of the things that struck me in that meeting was the importance they place on security and customer protection. Of course, I had Bill C-26 in mind. They told me that all customer funds are held in a trust at a ratio of 1:1 with Canadian financial institutions and leading cryptocurrency depositories. I learned that they are continually working to improve and promote the implementation of cybersecurity measures to protect their systems.

In preparing for my remarks today on Bill C-26, I started thinking that we need to examine how we can build on the security standards of Quebec companies like Shakepay and that we need to determine whether the bitcoin and cryptocurrency industry should also be considered in Bill C-26. Whether we like it or not, technology and customer habits may be leading us in that direction.

I would like to discuss cyber-resilience. I understand that the bill will not be studied by the Standing Committee on Industry and Technology, on which I sit. However, I see issues that affect industries that are in that niche of protecting systems from cyber-attacks. There are two things to keep in mind here: The attackers go after data using methods that were previously unimaginable, and they tend to favour methods that significantly delay the ability to resume operations. The desired consequences are financial and reputational damage.

The inherent complexity of the systems currently in place requires increasingly specialized resources. Innovation, research and development must be encouraged, in short, the entire ecosystem of this industry that works on the cyber-resilience of very high-risk systems. We need to ensure to attract the best talent in the world. The government must carry out its responsibilities at the same pace as it introduces these changes. Let us not forget, as the opportunities for cyber-attacks keep increasing, that we are always one incident away from our continuity of operations being disrupted.

### *Government Orders*

Is there an urgent need for action? Yes, clearly. Is the government on the same page as the people involved in this industry? Unfortunately, it has fallen behind.

For the past year, the Standing Committee on Industry and Technology has been studying topics that enabled it to get to the heart of the advanced technologies used in the industries covered by this bill. The inherent complexity of the environments in which those industries operate expose critical data and system configurations to greater risks than ever before, so much so that we are no longer assessing the likelihood of a successful cyber-attack, but instead how to recover. In fact, as IT infrastructure has become increasingly complex, cyber-attacks have become increasingly sophisticated too.

I dare not imagine what will happen in the coming years, when AI reaches its full potential and quantum computing becomes available. What I am hearing is that hundreds of pieces of users' electronic data are stored each day on international servers. They cannot be thoroughly processed using currently available technology, but what will happen when quantum computers are able to process those data? Maybe we will be very vulnerable as a result of actions we take today by casually agreeing to things in an app or allowing our data to be collected. In short, in five years' time, we may be paying for what we are giving away today.

In conclusion, the Bloc Québécois supports the bill. We want it to be sent to committee to be studied in detail, as my colleague from Avignon—La Mitis—Matane—Matapédia said. I also welcome forthcoming opportunities for specialists in Quebec industries who are renowned for their expertise.

• (1340)

[*English*]

**Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.):** Madam Speaker, it is encouraging when we get support for legislation. This legislation goes a long way in recognizing that cyber-threats are something on which we do need legislation to come forward and be voted upon. This legislation would allow for financial penalties and for the minister to take direct action. I wonder if the member could provide his thoughts on the importance, once we get into committee stage, of listening to what presenters have to say. I understand there are some concerns with regard to the legislation.

• (1345)

[*Translation*]

**Mr. Sébastien Lemire:** Madam Speaker, that is indeed essential, and it is also essential that the act have more teeth. In my opinion, it is vital that the act provide for a mechanism for issuing sanctions or fines in order to enforce compliance with orders and regulations aimed at securing telecommunications.

*Government Orders*

Let me give an example. We have learned that China maybe funding elections, meaning that there must be a network out there that is a threat to our country. Our national security and our ability to decide for ourselves who will lead our country are being influenced by foreign money. That is something that really worries me.

As a result, our systems need to be strengthened and penalties need to be imposed. Before that, however, we must know what happened, diagnose the problem accurately and be transparent. That is just one example of many, but that is how the problems should be resolved, particularly with respect to cybersecurity.

[*English*]

**Mr. Colin Carrie (Oshawa, CPC):** Madam Speaker, I want to thank my colleague for a very thoughtful speech. He was very good at pointing out some of the issues with this that we have heard from stakeholders. We have heard from privacy and civil liberties groups about the secrecy that could impair accountability, due process and public regulation.

The government orders issued under this bill may be made in secret without public reporting requirements, making it impossible for rights groups and the public to monitor and challenge how power is exercised under the bill. The secrecy of this could be very concerning.

I wonder if the member and the Bloc had any thoughts, once this goes to committee, about anything that could be added to improve the required balance between civil liberties and secrecy.

[*Translation*]

**Mr. Sébastien Lemire:** Sorry for the delay, Madam Speaker. I was waiting for the interpreter to finish. In passing, I want to thank the interpretation team. The fact that we can count on excellent interpreters when we are working on complex bills like this one is a strength of our democracy. I want to thank them.

Ultimately, we are here to protect the people we represent. I am very concerned about this, but I do not profess to be an expert. However, as intermediaries and legislators, we have access to the real experts. It is essential that they appear in committee to tell us how we can strengthen these bills. It is very clear that we need to make decisions today that will protect us against future attacks, which will come in forms that we cannot even fathom right now.

As I said, we have no way of knowing right now how much quantum computing will change our lives, by allowing the attacks to become increasingly sophisticated and rendering our existing defence systems obsolete.

[*English*]

**Mr. Gord Johns (Courtenay—Alberni, NDP):** Madam Speaker, because it is the holiday season I will not slight the government for taking so long to bring legislation like this forward. We know that France and the U.K. are far ahead of us in terms of addressing cybersecurity issues. I will give credit to the minister for at least starting to move this process forward.

Our shared concern with the Bloc is that the minister is going to have these extra powers. We are disappointed that this legislation has come forward without ensuring that Canadians will not be un-

justly examined or that this is not going to be applied to ordinary Canadians.

Maybe my colleague could speak about how important it is, when government brings forward legislation, that these things are presented in the initial piece of legislation, rather than assuming it will go to committee and get improved upon there. There should be some effort from the government to address these areas at the beginning.

[*Translation*]

**Mr. Sébastien Lemire:** Madam Speaker, I will simply say that I agree with my colleague.

[*English*]

**Ms. Marilyn Gladu (Sarnia—Lambton, CPC):** Madam Speaker, it is a pleasure to rise today to speak to Bill C-26 on cybersecurity. I will be sharing my time today with the member for Edmonton Manning.

Canadians recognize that we need to do something in the area of cybersecurity. We have all experienced hackers. Myself, when I have bought something online, the next thing I know is my credit card is hacked and then all the pre-authorized transactions need to be changed. It is very time-consuming. I have been hacked numerous times on Facebook, as I am sure many have, as well as on Instagram and other places. Those are small examples that Canadians are seeing.

Let us think about the more serious cyber-hacking we are seeing, whereby government systems are hacked and breaches of information are happening. Businesses are experiencing this. I have a friend who is an anti-cyber hacker. For \$2,500 a day, he goes around the world, helping companies that have been hacked to improve their protections.

Something needs to be done. I would like to talk today about what needs to be done, and then how the bill does or does not meet that need.

First, we have to identify what the critical systems are. What are the things we want to protect? If somebody hacks my Netflix account, it is not earth-shattering. However, there are things that are important, and I think everyone would agree that databases that protect our identity or have information about our identity are critical.

Financial institutions and people's financial information are critical. On our medical information, we have spent a lot of time on legislation and regulations on protecting medical privacy. Those, to me, would be three of them, but certainly, the critical systems need to be identified.

We need to make sure there are adequate protections in place. Not every business and level of government has the same amount of protections and technology in place. There is a journey of defining what adequate protection is and helping people get there.

*Government Orders*

In the case of breaches and having them investigated and addressed, the bill gives very broad powers to the minister. It allows the federal government to secretly order telecom providers to “do anything or refrain from doing anything...necessary to secure the Canadian telecommunications system, including against the threat of interference, manipulation or disruption.”

Those three terms are not well defined, so I think there is some work to be done to define those better, but I do not really believe we want to give the government power to do anything it wants. Certainly, shutting down a system for protection is important when there is an actual threat and not just a potential future threat or a possible threat. In the case of a threat, the government needs the ability to act, but certainly we have to tighten up the language in the bill on that.

After there has been a breach, there needs to be preventive and corrective action. Preventive action would be additional technology walls or additional controls that are put in place to ensure that we have enhanced protection in the future. Corrective action is fixing the holes that people got into in the first place and punishing the hackers. It does not seem like any of that is happening today. The bill does not address that, but there should be some measures there to take corrective action.

I talked about the overarching powers and my concern with them. We cannot have the government continually coming up with bills in which it has not really defined what it is going to do but it tells us not to worry about it because the Governor in Council, after the fact and without any parliamentary oversight, will determine what we are going to do.

The Governor in Council means the Liberal cabinet ministers. I think we are at a place where people have lost trust in the government because there is no transparency. The bill allows the government to make orders in secret, without telling people what is done. The public cannot see it and is suspicious, because people have seen numerous examples of the government hiding things.

We have just come through a \$19-million emergency measures act situation in which the Liberal cabinet ministers and the Prime Minister knew they were never going to disclose the documents that would prove or disprove whether they met the threshold, because they were going to hide behind solicitor-client privilege.

They have done it before, hiding behind cabinet confidence, like on the Winnipeg lab issue. Look at the documents we tried to get hold of there. The Liberals even sued the Speaker in order to hide that information from Canadians.

• (1350)

In the SNC-Lavalin scandal, we saw them hiding behind cabinet confidence. In the WE Charity scandal, we saw them hiding behind cabinet confidence. I am a little concerned, then, to find that in this cybersecurity bill, the Liberals are saying the government can make secret orders that the public is not going to ever know about. I think that is very dangerous. This is one of the reasons we are seeing an erosion of trust in Canada.

A recent poll posted by The Canadian Press showed that if we look at the trust index in Canada, only 22% of Canadians trust the

government or politicians. That means four out of five Canadians do not trust the government or politicians, and it is partly because of what has gone on before, when things have been done such as people's banks accounts frozen and drones surveilling citizens. People have lost trust, so I do not think they are going to be willing to give a blank cheque to the government to do whatever it wants for cybersecurity, to control enterprises outside the government to get them to stop operating, for example. The riverbanks need to be much tighter on that.

People are concerned about their civil liberties, and I know there has been a lot of conversation about the lack of privacy protection in this country. We have regulations like PIPA and PIPEDA. My doctor cannot reveal my medical information; my employer cannot reveal my medical information, but various levels of government in the pandemic made it so that every barmaid and restaurant owner could know my private medical information and keep a list of it, which is totally against the law. Therefore, when it comes to cybersecurity we are going to have to make sure the privacy of Canadians' information is better protected, and I do not see that element here in the bill—

• (1355)

**The Assistant Deputy Speaker (Mrs. Carol Hughes):** I have a point of order from the hon. member for Timmins—James Bay.

**Mr. Charlie Angus:** Madam Speaker, it is important that we not use disinformation in the House. The member mentioned that restaurant waitresses were breaking the law by asking for vaccine information. That is a falsehood. Could the member correct that?

**The Assistant Deputy Speaker (Mrs. Carol Hughes):** I would say that the information the hon. member is trying to share is more of a point of debate.

The hon. member for Sarnia—Lambton has just under three minutes.

**Ms. Marilyn Gladu:** Madam Speaker, I have no problem clarifying. Several of the places I went into were following provincial orders, to be clear, and they were to record who showed up and whether or not they were vaccinated. That is what was done, and that is against PIPA and PIPEDA.

I will turn to the government's record on protecting us in terms of cybersecurity, and talk about Huawei.

### Statements by Members

In 2018, our Five Eyes partners were concerned about Huawei's connection to the Chinese communist government, and they were not going to allow Huawei into their networks. However, the Canadian government delayed a decision for four years. The Liberals waited until 2022 to ban Huawei. Why did they do that? It was so Bell and TELUS could implement Huawei technology, 4G technology, across the country. That is hardly a protection from a cybersecurity point of view, and it again speaks to why Canadians have lost trust in the government.

However, I will support the bill to go to committee. I have said that we need to do something for cybersecurity, and I have outlined what I think we need to do. I do not think we can leave these huge gaps that have been cited by numerous institutions.

The University of Toronto has written letters to the government, talking about what is wrong with the bill and what it would like to see. If members have not seen the report it did with the Munk School, called "Cybersecurity Will Not Thrive in Darkness", there are a number of recommendations in the report that talk about what needs to be done to Bill C-26 to fix it. I would encourage the government to look at that, and I would expect it to become the substance of amendments that would be brought at committee.

Also, we should look at what the constitutional and civil liberties lawyers are saying. They are very concerned about the parts of the bill that would surveil Canadians, so I think we need to make sure we listen to what they have to say. They have written an open letter to the government, and I would recommend that the government take a look at that as well.

Finally, on accountability, due process and public regulation, there is potential for abuse. I would encourage the government to take a look.

I look forward to more discussion at committee.

---

## STATEMENTS BY MEMBERS

[English]

### GENDER-BASED VIOLENCE

**Mr. Mike Morrice (Kitchener Centre, GP):** Madam Speaker, the 16 Days of Activism Against Gender-based Violence is a critical time to speak about a shadow pandemic we are in the midst of. It is one of femicide, which is the intentional murder of women and girls because they are women and girls. Last year in Canada, there was a 26% increase in femicides compared to the previous year.

Just last week, a woman in my community was killed by her intimate partner. It was one of 158 femicides reported so far this year. The perpetrators of gender-based violence are predominantly men, so we must be part of the solution.

In my community, I am grateful for organizations like the Sexual Assault Support Centre of Waterloo Region, whose male allies program engages boys and men in ending systemic and everyday forms of gender-based violence.

We need more of these programs across the country, but this requires sustained increases in funding to support the increased need

for these services. I encourage all of my colleagues to support this life-saving work.

\* \* \*

● (1400)

### RETIREMENT CONGRATULATIONS

**Mr. Vance Badawey (Niagara Centre, Lib.):** Mr. Speaker, I am both saddened and happy today to stand in the House and recognize the contributions and the retirement of Port Colborne resident Barbara Butters.

First elected to city council in 1997, Barbara went on to serve six terms as a city councillor before adding another term as a regional councillor representing the great people of the city of Port Colborne. While we will miss her wisdom and her service, we also want to wish her and her husband Larry, our city's Santa and Mrs. Claus at this time of year, the very best in her retirement.

Barbara Butters has been an inspiration to anyone who has had the honour of working with her and spent a lifetime setting an example for anyone wishing to serve their communities. Barbara has always been a genuine, loyal and caring individual and a great Canadian. It was an honour to work with her and a privilege to call her a friend.

\* \* \*

### OIL AND GAS INDUSTRY

**Mr. Michael Kram (Regina—Wascana, CPC):** Mr. Speaker, last summer, German Chancellor Olaf Scholz visited Canada and asked us to increase oil and gas exports to his country so that they could stop buying from Russia. The Prime Minister said no. The Prime Minister said that there has never been a strong business case for Canadian oil and gas exports to Europe.

What did the German chancellor do next? He flew to the Middle East and made the same offer to the dictators of the United Arab Emirates and Qatar. Those Middle Eastern dictators said yes. They said yes to a multi-year memorandum of understanding that will guarantee steady exports, long-term employment and economic spinoffs for years to come.

It is too bad that Canadian workers were left out in the cold, and all of those economic benefits will be in those Middle Eastern countries.

When is the Prime Minister going to learn that the world needs more Canadian energy?

### CANADA-TAIWAN RELATIONS

**Hon. Judy A. Sgro (Humber River—Black Creek, Lib.):** Mr. Speaker, last month, my fellow MPs and I successfully visited Taiwan as a Canada-Taiwan parliamentary friendship group delegation. The focus of this trip was, as it always has been for the friendship group travels, trade opportunities and cultural exchange.

Taiwan is an important stakeholder and a valuable partner for Canada and the international community. I was delighted to learn that there are more than 30 Canadian companies operating in Taiwan and about 60,000 Canadians residing there.

Our friendship group delegation was impressed with the offshore wind project by Northland Power. It is a major Canadian investor that is contributing a great deal to Taiwan's 2050 net-zero emissions strategy.

In 2021, Taiwan was Canada's 11th-largest trading partner, and there are opportunities now to advance this partnership even more. There is a lot of potential in the green economy, agricultural markets, the semiconductor industry, education, science and beyond.

Canada and Taiwan have a long and rich history of cultural exchanges, and I hope our friendship will grow even stronger with the world recovering from the pandemic.

\* \* \*

[Translation]

### FÉLIX BLACKBURN

**Mrs. Claude DeBellefeuille (Salaberry—Suroît, BQ):** Mr. Speaker, I am honoured to share with the House the outstanding achievements of Félix Blackburn, executive director of the Société de conservation et d'aménagement des bassins versants de la Zone Châteauguay, or SCABRIC, an organization dedicated to watershed conservation and planning.

Mr. Blackburn knows everything there is to know about the Châteauguay River watershed. Since 2002, he has dedicated the full measure of his talent and every ounce of his passion to conserving this natural area. Sample after sample, master plan after master plan, campaign after campaign, Félix Blackburn has helped build our community's awareness of the importance of water quality. His work has produced many tangible outcomes, such as the adoption of innovative sustainability practices.

Félix Blackburn is retiring, but, like any good manager, he has made sure his successors are up to the task. A skilled, dedicated, effective team is ready to continue fulfilling SCABRIC's vital mission.

I wish our dear Félix a full and happy retirement. It is certainly well-deserved. I also wish him plenty of paddling time on his beautiful Châteauguay River.

\* \* \*

● (1405)

### UTERINE CANCER SCREENING

**Ms. Annie Koutrakis (Vimy, Lib.):** Mr. Speaker, I rise today to recognize the hard work and dedication of Dr. Lucy Gilbert and her team, who developed DOvEEgene, the world's first genomic uter-

### Statements by Members

ine cancer screening test, at the McGill University Health Centre. Ovarian and endometrial cancers are the fourth most common cause of cancer deaths in Canadian women.

[English]

Deaths related to endometrial cancers are rising while the five-year survival of ovarian cancer patients is below 50%.

However, there is hope. DOvEEgene detects and diagnoses these cancers early, when they are microscopic and have not spread. Early diagnosis means potential cure rates of over 80%.

This work adds to Canada's history of scientific excellence. It is a history that too often goes unsupported. We cannot miss this chance to capitalize on this scientific achievement, because it will save countless women's lives in Canada and throughout the world.

\* \* \*

### COST OF LIVING

**Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC):** Mr. Speaker, Canadians have been struggling, and Liberal inflation is driving up the cost of everything from home heating to buying a tank of gas to buying groceries for one's family.

The government is committed to making life more unaffordable by raising taxes on the necessities of life for Canadians. It is forcing record numbers of people to turn to food banks to feed their families. In fact, 1.5 million Canadians used food banks in a single month. While that is a staggering statistic, every single one of those people is barely getting by. These are folks who are teetering, because the Liberal government has made life so unaffordable, and it has become personal.

I recently met with Alee at the Brockville food bank, and she told me that the need has truly never been higher. Therefore, if people are able to, please consider giving to the local food bank this season.

The Liberal government needs to remove the tax on home heating so Canadians do not freeze in the dark. It needs to end its inflationary spending.

Canadians deserve better than what they are getting from the Liberals. They need hope, and that is exactly what Canada's Conservatives are going to provide.

\* \* \*

### INTERNATIONAL DAY FOR THE ABOLITION OF SLAVERY

**Hon. John McKay (Scarborough—Guildwood, Lib.):** Mr. Speaker, December 2 marks the International Day for the Abolition of Slavery.

*Statements by Members*

Slavery has been a blight on humanity since the dawn of time. Canadians unwittingly participate in this scourge by purchasing products made by slaves. We can hardly decry the plight of these slaves if we simultaneously create a market for their products. A transparency bill works on the theory that sunlight is the best disinfectant. Yesterday, Bill S-211 returned to this place for its final reading. Is it enough? Should we stop here? Of course not. The bill is merely a marker on this journey.

However, I hope colleagues will reflect on the legislative genius of William Wilberforce. When the legislative path to the abolition of slavery was blocked, he got the trading of slaves abolished instead, thereby making the ownership of slaves worthless. Shortly thereafter, the British Empire abolished slavery forever.

On this occasion of the International Day for the Abolition of Slavery it is important to remember that sometimes one has to do indirectly what cannot be done directly.

\* \* \*

**GENDER-BASED VIOLENCE**

**Ms. Ya'ara Saks (Parliamentary Secretary to the Minister of Families, Children and Social Development, Lib.):** Mr. Speaker, in Canada a woman is murdered every 2.5 days. Fifty per cent are killed by intimate partners and 26% are killed by a family member.

The early signs are there, and too many look away: "It's just that they do not like my friends or family." "It's just that they are keeping me on a tight budget." "It's just that they have a short temper." "It's just a bruise." "It's just a scratch." "It's just a burn." "It's just how it is." These are some of the myriad of ways that victims of coercive control, intimate partner and gender-based violence are trapped and silenced around us each and every day, and it is just not right.

This week and the next, the 16 Days of Activism Against Gender-based Violence sends the message that "it is not just". It means that we are working to making sure victims are not trapped and that we will not be silent in our pursuit to protect them. We are not only standing together, but also stating clearly and with conviction that it is just not right.

Today and every day we need to listen to the victims of gender-based violence. We need to hear them, see them and believe them.

\* \* \*

● (1410)

**PUBLIC SAFETY**

**Mr. Blaine Calkins (Red Deer—Lacombe, CPC):** Mr. Speaker, since the government took office in 2015, gang-related homicides have increased by 92%. The Liberals reduced sentencing requirements for serious gun crimes and now violent crime is up 32%. The Liberals will not admit their soft-on-crime approach is failing all Canadians.

Last week, the government initiated a ban on rifles and shotguns. This will ban hundreds of thousands of firearms in Canada that are used for hunting. The ban includes slow-to-fire guns and purpose-built hunting firearms that are designed to shoot birds or deer. It said it would not, but it did. There is no trust in the government.

Instead of addressing gang crime and gun smuggling, the government is vilifying hunters and farmers. The Liberals know Canadian hunters are not causing the crime surge in Canada, but they are going after them anyway because it is all about politics and not fighting crime. Their ill-conceived plans to go after hunters is the largest attack on law-abiding firearms owners in Canadian history. It is a direct attack on our Canadian cultural heritage.

The Conservatives will always stand up for victims, go after gangs and smugglers and trust Canada's law-abiding gun owners.

\* \* \*

**CRIME PREVENTION**

**Mr. Paul Chiang (Markham—Unionville, Lib.):** Mr. Speaker, today I am proud to rise in the House and acknowledge the great work that is being done to keep communities safe in my riding of Markham—Unionville.

In collaboration with the York Regional Police, I will be hosting my third crime prevention town hall, which provides essential safety tips and risk-management information to the residents of Markham.

Working together with law enforcement and other levels of government is critical to understanding our diverse communities and their needs. While in Ottawa, our government has taken comprehensive steps to improve public safety through our \$250-million building safer communities fund and Bill C-21, which would put a freeze on handguns in our country, increase penalties for firearms traffickers and provide additional tools to law enforcement across the country.

\* \* \*

**INDIGENOUS AFFAIRS**

**Mr. Gary Vidal (Desnethé—Missinippi—Churchill River, CPC):** Mr. Speaker, the Conservatives promote and believe in economic reconciliation. It is the solution to eradicating poverty and, with it, the social issues that poverty creates. Treating symptoms rather than the root cause has failed.



*Statements by Members*

It is time to fundamentally change that approach and, away from the Ottawa bubble, that change has already begun. From the Kiti-mat LNG project in British Columbia to Cameco's uranium supply in Saskatchewan, from Vale's base metal mining in Ontario to the Mi'kmaq communities of Nova Scotia and their acquisition of Clearwater Seafoods, first nations communities are taking control of their economic destinies. They want to be true partners in responsible resource development. They have started business, created employment, increased capacity and have generated opportunities that will pay dividends for generations to come.

Self-determination truly begins when indigenous communities manage prosperity instead of poverty.

\* \* \*

**CARBON TAX**

**Mr. John Williamson (New Brunswick Southwest, CPC):** Mr. Speaker, families across the country are paying higher prices for gasoline, groceries and home heating because of the Liberal carbon tax. People in Atlantic Canada rely more on home heating fuels, which is a vital necessity to stay warm.

Here are some astonishing numbers. Since last year, home heating prices are up over 50% in New Brunswick and P.E.I., up 68% in Nova Scotia and up 78% in Newfoundland and Labrador. The Liberals say that they are sick and tired of people talking about this cold winter. That is too bad for the Liberals, because this winter is just beginning. Prices are going to be even higher than last year for families because of the Liberal government.

The rebate the Liberals are promising is a scam. The Parliamentary Budget Officer says that over 80% of Canadians are going to pay more in the carbon tax than they receive from the rebate. This is a plan to bankrupt Canadians. We need to end the scam. We need to end the carbon tax.

\* \* \*

[*Translation*]

**LAVIOLETTE POULTRY FARM**

**Mr. Francis Drouin (Glengarry—Prescott—Russell, Lib.):** Mr. Speaker, the Ontario-Quebec francophonie trade awards ceremony took place on November 15 in Trois-Rivières. The event was organized by the Fédération des chambres de commerce du Québec, the Fédération des gens d'affaires francophones de l'Ontario and the governments of Quebec and Ontario.

I would like to congratulate Ferme avicole Laviolette on winning this year's award. Ferme avicole Laviolette has been producing eggs in the St. Isidore, Ontario, area since 1977. It has grown from 6,200 to 45,000 laying hens and employs 13 people. Its eggs can be found in grocery stores and restaurants throughout eastern Ontario and southern Quebec. This is a successful interprovincial business model that can serve French-speaking customers.

Congratulations to Marcel Laviolette, the Laviolette family and their employees for all their hard work. We are lucky to have them in our community.

• (1415)

[*English*]

**HOUSING**

**Mr. Blake Desjarlais (Edmonton Griesbach, NDP):** Mr. Speaker, in the last three years, over 453 people have died on the streets of Edmonton because they did not have shelter. Just last month, three more people died in encampments, and hundreds more are facing another brutal Alberta winter in tents. Some of them will not survive.

Community organizations in my district of Edmonton Griesbach do heroic life-saving work, but they have had to shoulder this burden alone. Conservative and Liberal consecutive governments have refused to step up and fight the corporate greed that is the cause of the housing crisis. Decades of cuts and neglect have left Canada with one of the lowest shares of public housing in the G7.

The state of our public housing is horrific. Many sites I toured this summer had black mould and even had no running water. It is time for the government to get serious about tackling the housing crisis.

The New Democrats will never stop fighting until no one has to spend another Alberta winter in a tent. People should not have to die like this today.

\* \* \*

[*Translation*]

**350TH ANNIVERSARY OF BERTHIERVILLE**

**Mr. Yves Perron (Berthier—Maskinongé, BQ):** Mr. Speaker, today, I am pleased to mark the 350th anniversary of the municipality of Berthierville.

In 1672, Intendant Talon gave the seigneurie to Sieur Randin, who sold it the following year to Sieur Alexandre Berthier, for whom it is now named.

Its coat of arms is rich in symbolism. The dragon is the emblem of the town of Bergerac where Sieur de Berthier was born, the flame symbolizes the Eddy Match Company, a large match factory from 1919 to 1957, and the silver horn represents the Melchers distillery, one of the main industries from 1898 to 1985.

After giving us Guy Rocher, Gilles Villeneuve and Joannie Rochette, who knows what Berthier has in store for us in the future.

I would like to thank the Corporation du patrimoine de Berthier and the volunteers who are organizing the festivities. I invite all Berthelais to celebrate our community together.

Happy anniversary.

*Oral Questions*

[English]

**THE ECONOMY**

**Mrs. Stephanie Kusie (Calgary Midnapore, CPC):** Mr. Speaker, everything in our country seems to be broken since the Liberal government took office in 2015.

The government's reckless spending has led to a 40-year-high inflation rate, 6.9% just this month, and Canadian families simply cannot absorb those rising costs.

Instead, 1.5 million Canadians a month are having to use a food bank and one in five Canadians are skipping meals; nine in 10 Canadians are now tightening household budgets; and the average credit card balance held by Canadians was at a record high of \$2,121 by the end of September. The RBC estimates that households will soon have to allocate 15% of their income to debt servicing alone.

The government needs to take this inflation crisis seriously. It needs to cap government spending and inflationary deficits, and bring inflation down now.

\* \* \*

**GENDER-BASED VIOLENCE**

**Ms. Jenna Sudds (Kanata—Carleton, Lib.):** Mr. Speaker, this morning, the Minister for Women and Gender Equality and Youth launched Canada's first youth-focused gender-based violence awareness campaign, "It's Not Just". "It's Not Just" is a call for each of us to speak up when we see gender-based violence in any form.

Gender-based violence is more than just physical and sexual violence. Emotional, financial and cyber violence can be just as harmful, with lasting psychological impacts. It can happen to anyone of any age or gender identity. It is not just locker room talk. It is not just how someone is. We want Canadians and Canadian youth to know that gender-based violence is not just.

---

**ORAL QUESTIONS**

● (1420)

[Translation]

**FIREARMS**

**Hon. Pierre Poilievre (Leader of the Opposition, CPC):** Mr. Speaker, with violent crime up 32%, we would think that the government would invest in border security, in the police, or that it would make other investments to protect Canadians, but no, instead it wants to ban hunting rifles.

An academic expert said yesterday that the ban will cost another billion dollars, money that could have been spent protecting our borders and stopping street gangs. Why not use the money to protect the public instead of targeting hunters?

**Hon. Marco Mendicino (Minister of Public Safety, Lib.):** Mr. Speaker, I want to reassure my colleague and the entire House that Bill C-21 does not target hunters or gun owners. Bill C-21 targets assault-style weapons like the ones that were used in Nova Scotia,

Quebec City and Ontario. They caused a lot of deaths. That is exactly why we need to work together to protect all Canadians with policies that make sense.

[English]

**Hon. Pierre Poilievre (Leader of the Opposition, CPC):** Mr. Speaker, based on the list that the minister has provided in his very legislation, it is not assault rifles. It is hunting rifles. Let me list off some of the rifles: the Montefeltro Super 90 Turkey, the Mossberg 715T Tactical 22 Duck Commander, the Benelli Super Black Eagle Ducks Unlimited. These are firearms specifically designed to hunt small fowl and to go after vermin and other farm pests.

Why is the government not targeting real crime rather than targeting farmers and hunters?

**Hon. Marco Mendicino (Minister of Public Safety, Lib.):** Mr. Speaker, I assure my colleague that we are going to work with the members of the Standing Committee on Public Safety with regard to this amendment, but, more important, our goal here is to target those assault-style rifles, those AR-15 style guns, which have been used in far too many casualties in Portapique, in Quebec and in Ontario, where most recently we saw two frontline police officers gunned down.

I do not know how anyone can look the families of the victims in the eye and say that we cannot do everything that is necessary to take these guns off our streets. These AR-15's have no place on our streets.

**Hon. Pierre Poilievre (Leader of the Opposition, CPC):** Mr. Speaker, he is doing nothing to take dangerous guns off the street. In fact, 82% of guns used in crime in Toronto, according to the city's police, come smuggled across the border. He has done nothing about that, but he wants to spend another billion dollars going after rifles and shotguns that are specifically designed and used by hundreds of thousands of law-abiding and licensed Canadians for hunting. These are law-abiding people who have been vetted by the RCMP.

Why does he keep targeting the lawful people rather than keeping the illegal guns out?

**Hon. Marco Mendicino (Minister of Public Safety, Lib.):** Mr. Speaker, my hon. colleague from the Conservative Party can continue to spread disinformation, but I will tell members very clearly that on this side of the House we are targeting those AR-15 style guns that have been used in mass casualties. This is part of a broader plan, a plan that will actually eradicate gun violence.

He talks about supporting CBSA. This government put \$138 million into the CBSA to stop illegal smuggling. What did the Conservatives do? They voted against that. That is wrong. They should support frontline law enforcement so we can stop illegal smuggling of guns at our borders.

## HOUSING

**Hon. Pierre Poilievre (Leader of the Opposition, CPC):** Mr. Speaker, National Bank came out with staggering housing statistics today. It now takes 67% of the average monthly income to pay bills on the average home. In fact, the average mortgage payment for a new home in Toronto is now \$7,000, and that is if one can afford the home, because it takes now 27 years for the average person to save up for the down payment on that home.

How is it possible that the average Canadian cannot afford the average home here in the nation with the second biggest supply of land anywhere on earth?

**Hon. Ahmed Hussen (Minister of Housing and Diversity and Inclusion, Lib.):** Mr. Speaker, we know that one of the main challenges facing the housing market is enough housing supply. We have the fastest growing population in the G7 but very little supply.

That is why we introduced the housing accelerator fund, to work directly with municipalities to increase and double the new construction of housing in the country. We are also introducing a new, innovative rent-to-own program and putting together a first-time homebuyer tax-free savings account of \$40,000, as well as doubling the first-time homebuyers' tax credit. Those are real actions that those members voted against.

• (1425)

[Translation]

**Hon. Pierre Poilievre (Leader of the Opposition, CPC):** Mr. Speaker, the only thing they doubled is the cost of housing. House prices have doubled since this Prime Minister came to power. Inflationary spending with printed money inflated the price of houses. Now, rising tax rates are making mortgage payments more expensive too. The vast majority of Canadians cannot even dream of owning a home these days.

When will the government change its inflationary policies and encourage municipalities to allow large-scale housing construction so Canadians can have a home to live in?

[English]

**Hon. Ahmed Hussen (Minister of Housing and Diversity and Inclusion, Lib.):** Mr. Speaker, the biggest gatekeeper against municipalities building more housing supply is the leader of the official opposition because he voted against the housing accelerator fund, a fund designed precisely to invest in more housing supply. When we were talking about the first-time homebuyers' \$40,000 tax-free savings account, the leader of the official opposition directed his team to vote against it.

These are real efforts at making sure more and more Canadians can access the dream of home ownership, but the fact of the matter is that, while the Conservatives talk about gatekeepers, they are the biggest gatekeepers. They are not serious about this issue. They do not have a plan. It has been 300 days since he became leader—

**The Speaker:** The hon. member for Beloeil—Chambly.

## Oral Questions

[Translation]

## DEMOCRATIC INSTITUTIONS

**Mr. Yves-François Blanchet (Beloeil—Chambly, BQ):** Mr. Speaker, the government seemingly does not realize that it has put Canada in a very precarious situation by provoking the Chinese government. China is more powerful economically, demographically and geopolitically speaking, yet Canada, instead of aligning itself with the United States, even if it means hiding behind it, is showing just how weak it is. Worse, it is showing how vulnerable it is. China is getting the impression that it can do whatever it wants in Canada. By not revealing which ridings allegedly received illegal funding and by not clearing the air about the \$70,000 in his own riding, the Prime Minister is making us vulnerable.

Which ridings were targeted?

**Hon. Marco Mendicino (Minister of Public Safety, Lib.):** Mr. Speaker, our government takes all allegations of threats of foreign interference very seriously. That is why we established two panels to review all allegations. The panels confirmed the integrity of the 2019 and 2021 elections.

We will continue to provide all the tools that the national security community needs to protect our democratic institutions.

**Mr. Yves-François Blanchet (Beloeil—Chambly, BQ):** Mr. Speaker, that may be why the Prime Minister put on a show in front of the Chinese president. It is because nothing happened.

Quebeckers and Canadians must stop accepting superficial answers. The government needs to be held accountable. It claims to be protecting institutions, but it is actually protecting the Prime Minister, the Liberal Party and Chinese interests by remaining silent. It is only natural that we are asking questions about financing in the Prime Minister's riding.

To put all of this behind it, is the government prepared to ask for an investigation into financing in the Prime Minister's riding in 2016?

**Hon. Marco Mendicino (Minister of Public Safety, Lib.):** Mr. Speaker, my colleague knows that we created an independent, non-partisan panel to examine all allegations of foreign interference and that the panel confirmed that the 2019 and 2021 elections were free, fair and just. That is why we will continue to protect our democratic institutions.

*Oral Questions***HEALTH**

**Mr. Alexandre Boulerice (Rosemont—La Petite-Patrie, NDP):** Mr. Speaker, for weeks now, doctors have been sounding the alarm about the catastrophic situation in Quebec's emergency rooms. People have even died while waiting. Just yesterday, Dr. Guylaine Larose, a pediatrician at Sainte-Justine Hospital, said she had never seen so many children in respiratory distress. Doctors and nurses are exhausted, and parents are worried. We are in the middle of a crisis, but it appears the Liberals do not sense the urgency. Our seniors suffered during the pandemic. Now our children are suffering and are at risk.

What will it take for the Liberals to do something and invest so that kids can get the care they need?

• (1430)

**Mr. Adam van Koevorden (Parliamentary Secretary to the Minister of Health and to the Minister of Sport, Lib.):** Mr. Speaker, I thank my hon. colleague for his question. Urgent action is needed to address the current health care worker crisis. That is why we have taken significant steps like creating the coalition for action for health workers, which will provide immediate and long-term solutions to address significant health workforce challenges. We also announced the appointment of a chief nursing officer to provide strategic advice from a nursing perspective to Health Canada on priority policy and program areas.

\* \* \*

[English]

**INDIGENOUS AFFAIRS**

**Mr. Charlie Angus (Timmins—James Bay, NDP):** Mr. Speaker, in the fight to block justice for first nation children, the government has put up 23 non-compliance orders, spent millions on lawyers and are now back again fighting in federal court. It has lost every single legal action.

Fixing the broken child welfare system is possible, but it requires trust and good will. Will the minister just call off his lawyers, take the arbitrary deadline off the table, sit down with the communities and the child welfare experts, and put an end to the systemic discrimination and underfunding facing first nation children once and for all? Will he do the right thing?

**Hon. Patty Hajdu (Minister of Indigenous Services and Minister responsible for the Federal Economic Development Agency for Northern Ontario, Lib.):** Mr. Speaker, we are so encouraged by the historic work that we have done with indigenous first nations partners to arrive at an agreement in principle, a final settlement agreement that is historic in a number of ways, not just for the sum of money that first nations children who have been harmed by a systemically discriminating system would receive but also in the nature at which we arrived at that final settlement agreement.

It was, indeed, led by first nations, and I am proud to work with partners on ensuring that we complete this work.

\* \* \*

**THE ECONOMY**

**Mr. Jasraj Singh Hallan (Calgary Forest Lawn, CPC):** Mr. Speaker, Canada was seen as a country of prosperity. That is why

my family came here. Like so many newcomers, we came here with very little, but with hard work we were able to succeed.

Today, that dream for so many newcomers and citizens has gone up in smoke because of Liberal mismanagement of the economy. We have 40-year highs in grocery prices. Home prices have doubled under the Prime Minister, and now mortgages cost Canadians 64% of their income. The Liberals plan to pile on even more pain.

Will the Liberals stop their inflationary spending and stop driving up the cost of gas, groceries and home heating?

**Ms. Rachel Bendayan (Parliamentary Secretary to the Minister of Tourism and Associate Minister of Finance, Lib.):** Mr. Speaker, we have shown that we are there for Canadians, particularly vulnerable Canadians.

I would like to start off by saying that the Conservatives voted against a dental benefit that is becoming available to Canadian parents today. Today, Canadian parents can apply for \$650 in support per child. There is also the Canada workers benefit, which is already benefiting Canadian workers across the country. In 10 days time, they will be able to apply for the rental benefit.

We are there for Canadians.

**Mr. Jasraj Singh Hallan (Calgary Forest Lawn, CPC):** Mr. Speaker, that member is clueless. She knows the vast majority of Canadians will not see a penny from those announcements.

What they will see is the Liberals' reckless spending, which will cost each Canadian \$3,500, according to the Governor of the Bank of Canada. They will continue seeing their home heating costs soar because this "leave it in the ground" Liberal government cancelled pipelines across the country. The Liberal government's greed knows no bounds, and it will continue to charge Canadians even more.

Why will the Liberals not stop their reckless spending, get off the backs of Canadians, and axe their failed carbon tax?

**Ms. Rachel Bendayan (Parliamentary Secretary to the Minister of Tourism and Associate Minister of Finance, Lib.):** Mr. Speaker, I know that I am successfully countering the disinformation on the other side when they insult me.

Today Canadian families are able to apply for the dental benefit. We will continue supporting vulnerable Canadians while ensuring that Canada maintains the lowest deficit and the lowest debt of all the G7 countries. We have been extremely fiscally responsible, and the AAA credit rating proves it.

### CARBON PRICING

**Mrs. Tracy Gray (Kelowna—Lake Country, CPC):** Mr. Speaker, a new Ipsos poll shows that 26% of Canadians say that they will be accessing charitable services over the next six months for basic essentials, such as food, clothing and shelter.

The survey also says that 25% of Canadians will be donating less to charities, and they cite the biggest reason being the increase in inflation and the effects of their personal finances, yet the Liberal government continues to make it worse by increasing their taxes.

When will the Liberals stop their forced carbon tax on people, and stop charging them for—

• (1435)

**The Speaker:** The hon. parliamentary secretary to the Minister of Families, Children and Social Development.

**Ms. Ya'ara Saks (Parliamentary Secretary to the Minister of Families, Children and Social Development, Lib.):** Mr. Speaker, on this side of the House, we understand how challenging life is for Canadians right now.

As my colleague mentioned, we have been putting forward significant benefits to help them, whether it is the Canada child benefit; the dental benefit, which is accessible today; or the increase to the Canada workers benefit. As of next week, low-income renters can also access benefits.

We have been there for Canadians at every single stage of their life, and we continue to be there. Unfortunately, I cannot say the same for my colleagues across the way. The Conservatives keep voting against supporting Canadians each time. If they would like to—

**The Speaker:** The hon. member for Kelowna—Lake Country.

**Mrs. Tracy Gray (Kelowna—Lake Country, CPC):** Mr. Speaker, there is an obvious disconnect between the Liberals and what people are actually going through. The Governor of the Bank of Canada said that the average Canadian will be paying \$3,500 more because of inflation. That represents \$14,000 for the average family of four.

No wonder more people are saying that they will be accessing charitable services. No wonder more people are saying that they will be donating less, yet the Liberals continue to make things worse by charging more people on their taxes.

Again, will the Liberals stop forcing their failed carbon tax on Canadians?

**Ms. Rachel Bendayan (Parliamentary Secretary to the Minister of Tourism and Associate Minister of Finance, Lib.):** Mr. Speaker, I would like to remind the member opposite that Canadians, even if they are having a tough time, are seeing that, around the world, global economic instability is causing inflation to be much higher elsewhere. Higher inflation among our peers can be seen around the world. We are continuing to invest to support vulnerable Canadians.

I would also like to remind the member that it was a policy of our government that lifted over two million Canadians, including

### Oral Questions

450,000 children, out of poverty. When she talks about her concern for children and families, her voting record should prove it.

[Translation]

**Mrs. Dominique Vien (Bellechasse—Les Etchemins—Lévis, CPC):** Mr. Speaker, we all know Canadian families are feeling the financial pinch. Liberal inflation is hitting them right in the pocket-book. The Liberal government needs to give them a break.

The easy way to do that is to agree to our one key demand: do like other G7 countries and cancel the carbon tax hike. Canada is the only country fixated on increasing the carbon tax.

Will this government finally agree to our demand and follow in the other G7 countries' footsteps?

**Ms. Rachel Bendayan (Parliamentary Secretary to the Minister of Tourism and Associate Minister of Finance, Lib.):** Mr. Speaker, I have news for my colleague. Pollution pricing does not apply in Quebec. What is more, Quebecers wholeheartedly agree that we must tackle climate change.

I would also add that our government has a strong plan to address the economic instability we are all experiencing by ensuring a fiscally responsible approach to the debt and the deficit, which are the lowest in the G7.

**Mrs. Dominique Vien (Bellechasse—Les Etchemins—Lévis, CPC):** Mr. Speaker, the plan she is referring to is a tax plan.

At the same time that the Liberal government is insisting on increasing the carbon tax, it is announcing new spending to please the NDP, which, members will recall, is keeping the Liberals in power.

People living in rural areas no choice but to drive because there is no public transit. Families, workers and businesses are being hit hard by the carbon tax.

How can this government just look away and pretend that it does not see that the carbon tax is slowing down the economy, making Canadians poorer and not helping the environment?

[English]

**Mr. Terry Duguid (Parliamentary Secretary to the Minister of Environment and Climate Change, Lib.):** Mr. Speaker, as my hon. colleague said, the federal pricing on pollution does not apply in Quebec, but it does apply on the Prairies, where I come from. There was good news for Atlantic Canada last week, and good news for the Prairies coming up this spring. As of April 1, a family of four will get up to \$1,500 in Alberta and Saskatchewan, and \$1,000 in Manitoba. Those cheques are going to be coming every three months. It is going to help with cash flow, and it is going to help with affordability.

The Conservatives have no plan.

*Oral Questions*

• (1440)

*[Translation]***OFFICIAL LANGUAGES**

**Mr. Mario Beaulieu (La Pointe-de-l'Île, BQ):** Mr. Speaker, Quebec's minister of the French language is meeting with the federal government today. That is good timing.

Last Thursday, we celebrated a historic anniversary. Two years ago, the Quebec National Assembly adopted a unanimous motion calling on Ottawa to work with Quebec to apply the Charter of the French Language to federally regulated businesses. Bill C-13 does the opposite. It lets businesses off the hook.

Will the minister announce to her counterpart that she will amend Bill C-13 to stop supporting the anglicization of Quebec?

**Hon. Ginette Petitpas Taylor (Minister of Official Languages and Minister responsible for the Atlantic Canada Opportunities Agency, Lib.):** Mr. Speaker, it is really disappointing that the Bloc Québécois continues to spread inaccurate information about Bill C-13.

We are the first government to recognize the decline of French, and that is why we are moving forward with an ambitious bill. Yes, I am very pleased to have the opportunity to meet with my counterpart, Mr. Roberge, this evening. We look forward to beginning to work together. Once again, as Minister of Official Languages, I will make sure I work closely with all of the provinces and territories to promote French across the country.

**Mr. Mario Beaulieu (La Pointe-de-l'Île, BQ):** Mr. Speaker, Quebec's minister of the French language is concerned because all indicators point to French being in decline. One of the main indicators comes from Statistics Canada: One in five Quebecers cannot work in French in Quebec. The numbers are even worse in Montreal and the Outaouais region.

Knowing that, why does the minister want to allow federally regulated companies to use Bill C-13 to circumvent the Charter of the French Language?

Her own statistics prove the contrary. There is a decline in the use of French in the workplace in Quebec. Does she not listen to science?

**Hon. Ginette Petitpas Taylor (Minister of Official Languages and Minister responsible for the Atlantic Canada Opportunities Agency, Lib.):** Mr. Speaker, our government and the Government of Quebec share a common goal, which is to do everything possible to protect and promote French across the country. That is why we are implementing an ambitious bill to ensure that federally regulated private companies' clients and employees will have the right to work in French and to be served in French, and this also applies to regions with a strong francophone presence.

I hope the Bloc and the Conservative Party will support this bill, as stakeholders across the country want us to take the next step.

**Mr. Mario Beaulieu (La Pointe-de-l'Île, BQ):** Mr. Speaker, Quebec's minister of the French language also called for a national awakening, urging Quebecers to open their eyes to the decline of French. It is high time the federal Liberals from Quebec woke up.

Their Bill C-13 does not protect French in Quebec. It protects English in the workplace and anglicizes Quebec.

It is time the federal Liberals remembered they do not work for Air Canada. They do not work for the Royal Bank of Canada. They work for Quebecers, and Quebecers' language of work is French. When will they wake up?

**Hon. Ginette Petitpas Taylor (Minister of Official Languages and Minister responsible for the Atlantic Canada Opportunities Agency, Lib.):** Mr. Speaker, the national awakening we should be seeing is the Bloc Québécois choosing to work with us to do everything we can to protect and promote French across the country. What we are seeing here is, once again, just for show.

The federal government has to be honest. We are the first government to recognize the decline of French across the country. That is why we put forward an ambitious bill. Now is not the time to squabble. Now is the time to work together closely to make sure this bill moves forward.

\* \* \*

*[English]***DIVERSITY AND INCLUSION**

**Ms. Melissa Lantsman (Thornhill, CPC):** Mr. Speaker, two days ago, Liberal members of Parliament and the Minister of Transport welcomed a dangerous anti-Semite, Holocaust denier and terrorist sympathizer to this place. Nazih Khatatba and Meshwar Media, which the government already gave tax dollars to, has referred to the Holocaust as a "Holohoax" and "the biggest lie in history". This newspaper called Judaism a terrorist religion. Worse yet, this man praised last week's heinous murder of 16-year-old Canadian teenager by terrorists.

Will the Minister of Transport denounce this man, his publication and apologize to Canadians?

**Hon. Omar Alghabra (Minister of Transport, Lib.):** Mr. Speaker, anti-Semitism is real and all of us must condemn it whenever we see it. This individual should not have been invited to this event. He should not have been welcomed to this event. That event was hosted by MPs from all parties. I am always happy to participate in parliamentary events, but we all should condemn anti-Semitism and all forms of hate wherever we see it.

• (1445)

**Ms. Melissa Lantsman (Thornhill, CPC):** Mr. Speaker, there was no apology and no condemnation. Members of the Canadian government should not be meeting with Holocaust deniers and Hamas sympathizers who praise the murder of children. They invited him and they got caught.

I will ask this again. Will the Minister of Transport have the courage to stand up on his feet in the House and apologize to Canadians?

**Hon. Omar Alhabra (Minister of Transport, Lib.):** Mr. Speaker, the member is misleading the House. I did not meet with the individual. Let me be very clear that as members of Parliament, we attend events everywhere, we are accessible to our community members and there is always a risk of us meeting unsavoury individuals. The issue here is how we, as MPs, react to this.

I want to make sure that I am clear. I condemn anti-Semitism. I will always condemn anti-Semitism. Will the members of the opposite side do the same when they encounter people who are spreading hate and anti-Semitism across Canada?

\* \* \*

[Translation]

### FIREARMS

**Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC):** Mr. Speaker, listen to this.

Hunting is part of Québec's history, and has become a way of reconnecting with nature and escaping the daily grind. Whether for the challenge...or to obtain good quality meat, hunting is within everyone's reach.

Who said that? It was the Government of Quebec.

What is more, the Conference Board of Canada said that, in 2018, nearly three million Canadians participated in hunting, trapping, sport shooting and fishing activities. This sector supports nearly 107,000 jobs.

Does the minister understand that hunters are not a threat to society? Will he stop this foolishness?

**Hon. Marco Mendicino (Minister of Public Safety, Lib.):** Mr. Speaker, I completely agree with my colleague. We have a lot of respect for hunters.

However, the bill and all of the policies that have been introduced by the government target the criminal element and the assault-style weapons that have been used in tragedies across Canada.

That is why we need to reverse the position of the Conservatives, who still want to make assault-style weapons legal. That is wrong.

\* \* \*

[English]

### CLIMATE CHANGE

**Ms. Laurel Collins (Victoria, NDP):** Mr. Speaker, Canadians are living with more frequent and extreme weather events that have left Canadians devastated. While people are dealing with the impacts of the climate crisis and trying to keep up with rising costs, the biggest polluters are getting even richer.

Like the NDP, 350 Canada, Leadnow and Greenpeace are calling on the Liberals to tax the excess profits of oil and gas so they pay their fair share. When will the minister stop defending the interests of the oil and gas industry and start making them pay what they owe?

**Mr. Terry Duguid (Parliamentary Secretary to the Minister of Environment and Climate Change, Lib.):** Mr. Speaker, we know two things. We know that energy profits are at record levels and we know that emissions have to come down.

### Oral Questions

We are investing \$9.1 billion in an emissions reduction plan. We have put our money on the table. Oil and gas companies have to come to the plate. They have to put their shoulder to the wheel. They have to work with us to get those emissions down and to realize the ambitious targets we have set through our emissions reduction plan.

**Mr. Blake Desjarlais (Edmonton Griesbach, NDP):** Mr. Speaker, the last three auditors general have been clear. The government has failed to help first nations communities protect themselves against natural disasters. The Auditor General is fed up with the government's inaction and Canadians are fed up too. Even the deputy minister sees that the government is leaving first nations communities to fend for themselves.

The climate emergency is here. We have no time to wait. When will the government drop the platitudes and deliver the \$358 million first nations need?

**Hon. Patty Hajdu (Minister of Indigenous Services and Minister responsible for the Federal Economic Development Agency for Northern Ontario, Lib.):** Mr. Speaker, I am happy to say that I agree with the member opposite that the climate emergency is real and that it is challenging first nations communities and indeed all communities across the country.

Indigenous Services Canada works closely with first nations communities that are under threat from fire, from torrential rain and from wind to make sure that people can get to safety and that we can protect infrastructure when those events happen. I also agree with the member opposite that as a nation we are going to have to pivot to ensuring Canadians have the prevention and the plans they need to adapt.

\* \* \*

● (1450)

[Translation]

### FIREARMS

**Mrs. Sophie Chatel (Pontiac, Lib.):** Mr. Speaker, hunters across Canada carry on a proud tradition, and some are worried.

I can say from experience that spending time in nature with family and friends is not just good for mental health, it also provides food security to many indigenous families and communities.

Can the Minister of Public Safety assure us that the changes in Bill C-21 will not affect our hunters?

**Hon. Marco Mendicino (Minister of Public Safety, Lib.):** Mr. Speaker, I thank my colleague for the question. I agree with her. Hunting is not only a fine tradition, it is also an activity at the heart of many communities.

*Oral Questions*

That is why the guns commonly used for hunting will still be allowed. We will make sure of it.

Bill C-21 is about making our communities safer. Our government has been clear: Guns designed for war have no place in our communities.

\* \* \*

[English]

**DEMOCRATIC INSTITUTIONS**

**Hon. Michael Chong (Wellington—Halton Hills, CPC):** Mr. Speaker, CSIS advised the Prime Minister in its top secret briefing note that the way to combat foreign interference was through “a policy that is grounded in transparency and sunlight in order to highlight the point that [foreign interference] should be exposed to the public”.

Why are the Prime Minister and the government not heeding this advice? Why are they not going public and telling Canadians exactly which candidates and which riding associations were involved in Beijing's foreign interference?

**Hon. Marco Mendicino (Minister of Public Safety, Lib.):** Mr. Speaker, I agree with my colleague that we need to take allegations of foreign interference very seriously. That is why we created independent, non-partisan panels to shine a light on the allegations of foreign interference, both of which confirmed that the elections in 2019 and 2021 were free and fair.

We will continue to shine a light on the tools, on the investments, that we are putting in our national security community to protect all our democratic institutions, including elections.

**Hon. Michael Chong (Wellington—Halton Hills, CPC):** Mr. Speaker, intelligence experts here and in the Five Eyes are saying that the best way to combat foreign interference is transparency and sunshine, to go public with information. That is why last summer the U.K. government and MI5 went public about a Beijing agent in the U.K. Parliament, Christine Lee. She was publicly named and so were the MPs who were the target of her donations.

Those MPs took action to protect the integrity of the U.K. Parliament. Why will the government not do the same thing in this country?

**Ms. Jennifer O'Connell (Parliamentary Secretary to the Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.):** Mr. Speaker, that could not be further from the truth. Let us review some of the facts about what our government has actually done.

One of the first things we did was repeal Stephen Harper's unfair elections act. What did that do? It actually closed foreign funding loopholes that the Conservatives and that member seemed to have had no problem with in past elections.

In addition, let us also talk about the fact that the 2019 NSICOP annual report that was tabled in this very House talked about the foreign interference attacks, and that member knows members could access—

**The Speaker:** I want to remind hon. members that when someone is speaking, shouting at them is not parliamentary and it is not polite.

The hon. member for Sherwood Park—Fort Saskatchewan.

**Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC):** Mr. Speaker, I invite that hon. member to read the NSICOP report that was tabled by a member of her own government, which was, in fact, scathing about the government's failure to respond to the persistent problem of foreign interference.

We know that the Prime Minister's secrecy and refusal to answer basic questions about foreign interference is putting this debate on its back foot. He is putting his personal interest ahead of the national interest by not listening to CSIS on the benefits of sunlight and giving us the information.

Will the Prime Minister answer the question. Has he received briefings or memos on this subject since he last denied it, yes or no?

**Ms. Jennifer O'Connell (Parliamentary Secretary to the Minister of Intergovernmental Affairs, Infrastructure and Communities, Lib.):** Mr. Speaker, it seems I have hit a nerve with members opposite.

Let us review the facts. The first is the fact that foreign interference does happen and, as a result, in this country, we have put in place strong measures to strengthen our democracy. The Conservatives seem to just be waking up to this fact now. Foreign interference, due to the strength of our democracy, does not always mean that those attempts work.

When it comes to the work we are doing, like I said, and the member opposite should know, I was a member of NSICOP and am very well aware of the reports. However, they received briefings and they—

• (1455)

**The Speaker:** The hon. member for Mégantic—L'Érable.

[Translation]

**Mr. Luc Berthold (Mégantic—L'Érable, CPC):** Mr. Speaker, let us talk facts. I have a note here from the director of our national security agency concerning a top secret briefing for the Prime Minister that says: “Canada could make good use of an open and transparent policy that would draw attention to the fact that [foreign interference] must be made public”. Yesterday, the Prime Minister himself said, “I know the member opposite, who sat in a cabinet, understands the importance of respecting national security guidelines.”

Why does the Prime Minister refuse to follow our national security agency's instructions? Why continue to withhold information from Canadians?



*Oral Questions*

[English]

**Hon. Marco Mendicino (Minister of Public Safety, Lib.):** Mr. Speaker, on this side of the House, we have put in place a number of measures to increase transparency about threats of foreign interference. For example, we have the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency, independent bodies that have issued two reports confirming that the 2019 and 2021 elections were free and fair. We will improve transparency because it is a value that protects our democratic institutions.

\* \* \*

**HEALTH**

**Mr. Mario Simard (Jonquière, BQ):** Mr. Speaker, children's hospitals are overflowing like never before, yet, the day before yesterday, the Prime Minister once again blamed the provinces instead of announcing solutions.

Seriously, this has to stop. The provinces are not to blame; underfunding is. For two years now, Quebec and the provinces have been asking the government for \$28 billion, and, for two years, the government has been fighting them on it.

Does the government finally realize that holding back money needed for hospitals has consequences?

**Mr. Adam van Koevorden (Parliamentary Secretary to the Minister of Health and to the Minister of Sport, Lib.):** Mr. Speaker, I thank my colleague for his question.

Our government has been working with the provinces and territories for a long time now, not only to provide funding, but also to create a national vision for health care and systems that meet Canadians' needs. We will increase Canadian health transfers by 10% in March 2023, which is in addition to the extra 5% increase announced a few months ago.

We will continue to work with the provinces and territories to improve health care in Canada.

**Mr. Mario Simard (Jonquière, BQ):** Mr. Speaker, it has to be said that the only two things the federal government has done to respond to the crisis at children's hospitals is to blame the provinces and hold back the money. I challenge any Liberal member to visit a pediatric emergency room in their riding and tell a parent that it is the provinces' fault that there are no health transfers.

We do not have any more time to waste playing political games. The federal government has but one thing to do and that is transfer the money. When will the government transfer the money?

**Mr. Adam van Koevorden (Parliamentary Secretary to the Minister of Health and to the Minister of Sport, Lib.):** Mr. Speaker, I thank my colleague for his question.

Since the start of the pandemic, our government has invested more than \$72 billion to protect Canadians' health. We will continue to work with the provinces and territories.

Our health system is facing significant challenges, and it is vital that we work together to improve health care for Canadians. By working together we will move forward.

**CARBON PRICING**

**Mrs. Kelly Block (Carlton Trail—Eagle Creek, CPC):** Mr. Speaker, inflation is at a 40-year high. Interest rates have increased at their fastest rate in decades, and the Bank of Canada is telling us that they need to go higher. The Prime Minister's solution is to spend more and raise taxes. While his inflation tax eats into the paycheques of Canadians, they are cutting into their diets.

If the Prime Minister really was serious about making life more affordable for Canadians, he would cancel his carbon tax increase immediately. Will the Liberal government stop forcing its failed carbon tax on Canadians?

**Ms. Rachel Bendayan (Parliamentary Secretary to the Minister of Tourism and Associate Minister of Finance, Lib.):** Mr. Speaker, we have put forward a responsible plan that is going to help vulnerable Canadians while ensuring that we maintain the lowest deficit and the lowest debt among G7 countries.

Unlike the Conservative leader, who has proposed no economic plan for Canadians, we have put forward something solid. The Conservative plan can be summed up as abandoning our fight against climate change and advising Canadians to invest in cryptocurrency to opt out of inflation. As a result of the news this week that Block-Fi declared bankruptcy, I think we can all agree that was—

● (1500)

**The Speaker:** The hon. member for Carlton Trail—Eagle Creek.

**Mrs. Kelly Block (Carlton Trail—Eagle Creek, CPC):** Mr. Speaker, The Liberals have not met an environmental target yet. Canadians are staring at bare cupboards and wondering how they are going to pay their heating bill this winter. Some 1.5 million Canadians have been forced to use food banks in a single month. One in five are skipping meals, and with the cost of home heating going up, they will not be able to afford to heat their homes.

The choice for Canadians is not between Disney+ and Netflix; it is between heating and eating. Will the Liberal government stop forcing its failed carbon tax on Canadians?

**Mr. Terry Duguid (Parliamentary Secretary to the Minister of Environment and Climate Change, Lib.):** Mr. Speaker, as usual, the Conservatives are spreading misinformation. Emissions are going down. We are on track to meeting our targets. Eight out of 10 families will be better off under our price on pollution.

What is the Conservatives' record? They cut \$350 million from the climate change budget. They blew up Kyoto and blew up our emissions targets at the same time. Now they are blaming us for their inaction.

*Oral Questions*

They have no plan for climate change. They have no plan for the economy. They have no plan for affordability.

**Mr. Colin Carrie (Oshawa, CPC):** Mr. Speaker, it is the Liberals who have no plan for the environment. It is a tax plan.

I just received a propane bill from a mother of three. It was \$614 for propane and \$55 for the Liberal carbon tax, and winter is just starting. This is getting vindictive. A carbon tax will triple home heating, gas and food.

While the Prime Minister spends Canadian tax dollars on ritzy \$6000-a-night hotels, Canadians are suffering. The Liberals are out to lunch and Canadians are being forced to skip theirs. When will the Liberals stop punishing hard-working Canadians and axe their failed carbon tax?

**Ms. Anita Vandenberg (Parliamentary Secretary to the Minister of International Development, Lib.):** Mr. Speaker, we must address the current affordability pressures while concurrently continuing to address the threat of climate change and building a prosperous low-carbon future. A price on pollution is an efficient market-based approach to reducing pollution, an approach that squarely addresses affordability. Under our plan, eight out of 10 Canadians receive more than what they pay, and that is the truth.

\* \* \*

[Translation]

**DISASTER ASSISTANCE**

**Ms. Lena Metlege Diab (Halifax West, Lib.):** Mr. Speaker, as Nova Scotians continue to rebuild their lives after hurricane Fiona, they have been helped by the fact that this government has been there for them. Thanks to the hurricane Fiona recovery fund, businesses across my region have been able to begin the process of rebuilding in the aftermath of this horrible storm.

Can the Minister responsible for the Atlantic Canada Opportunities Agency tell the House and all Atlantic Canadians how this government will continue to help our communities rebuild?

**Hon. Ginette Petitpas Taylor (Minister of Official Languages and Minister responsible for the Atlantic Canada Opportunities Agency, Lib.):** Mr. Speaker, I want to thank the hon. member for Halifax West for her important question and her hard work.

In the past few months, I have been fortunate enough to travel to Atlantic Canada on several occasions and have seen first-hand the impact of hurricane Fiona on the ground. Our communities were greatly affected. That is why we quickly set up the hurricane Fiona recovery fund.

This week we announced that people may begin submitting their applications so that we can support the hardest-hit communities and sectors that are not eligible for other sources of funding. We will always be there for Atlantic Canadians, in good times and in bad.

\* \* \*

[English]

**FINANCE**

**Mr. Kevin Waugh (Saskatoon—Grasswood, CPC):** Mr. Speaker, Canadians are struggling to make ends meet. The one-time

handouts by the Liberal government are not a solution to financial insecurity. The government continues to give its friends lucrative contracts, raising the price on groceries, gas and heating just to subsidize its reckless spending. Canadians are rightly concerned about their financial future.

Will the government finally listen to Canadians and stop its inflationary spending?

**Ms. Ya'ara Saks (Parliamentary Secretary to the Minister of Families, Children and Social Development, Lib.):** Mr. Speaker, I find it really interesting that our colleagues across the way do not understand what it means to invest in Canadians. For example, this government signed agreements with every province and territory across this country to make sure that Canadian families have affordable, high-quality and inclusive child care, which is not just good for families but great for the economy. On average, families across this country are seeing a 50% reduction in fees, with \$4,000 of real cash, in addition to all of the other benefits, whether it is the CCB or those for the dental and rental, which the Conservatives voted against.

This is not about spending; it is about investing in families. Why are—

● (1505)

**The Speaker:** The hon. member for Peace River—Westlock.

**Mr. Arnold Viersen (Peace River—Westlock, CPC):** Mr. Speaker, the Liberals' malevolent spending is causing Canadians' lives to get more and more expensive. The Parliamentary Budget Officer has recently raised the alarms about costs going up and said that the massive spending plans have no transparency. We know that the Liberal government has tried to funnel funds to its friends at WE Charity in the past while the Prime Minister's own family was receiving almost half a million dollars.

On what date will the Liberals stop their malevolent inflationary spending?

**Ms. Rachel Bendayan (Parliamentary Secretary to the Minister of Tourism and Associate Minister of Finance, Lib.):** Mr. Speaker, we know that Canada has the lowest deficit and the lowest debt among G7 countries. Experts have said that we have been extremely fiscally responsible. That is reflected in the numbers.

However, we have also been there to support Canadians, and today Canadian parents will be able to apply for the new dental benefit that is going to help 500,000 Canadian children under 12 in this country. That is real money going back into the pockets of Canadians.

*Oral Questions*

[Translation]

**THE ECONOMY**

**Mr. Jacques Gourde (Lévis—Lotbinière, CPC):** Mr. Speaker, these are the consequences of Liberal inflation: everything is expensive, too expensive. Groceries, gas, rent, interest rates, heating, clothing, all of our daily needs cost an arm and a leg.

Liberal inflation is also a headache for Canadians just before the holidays, especially with the new taxes planned for 2023.

Is there a solution to inflation?

**Some hon. members:** Yes.

**Mr. Jacques Gourde:** Mr. Speaker, the solution is to replace the Liberal government.

**Ms. Rachel Bendayan (Parliamentary Secretary to the Minister of Tourism and Associate Minister of Finance, Lib.):** Mr. Speaker, we put forward a solid plan that will help vulnerable Canadians while being fiscally responsible.

The Conservatives have no plan to offer Canadians—

**Some hon. members:** Oh, oh!

**The Speaker:** Order.

I will ask members to quiet down a bit. I appreciate the members' enthusiasm, but at some point they need to calm down.

The parliamentary secretary can start her intervention over again since I know that some people were unable to hear the whole thing.

**Ms. Rachel Bendayan:** Mr. Speaker, we put forward a solid plan that meets the needs of vulnerable Canadians while being fiscally responsible.

The Conservatives have no economic plan to offer Canadians. Excuse me. Let me rephrase that. Their plan involves going after the price on pollution, our seniors' pensions and employment insurance. It also involves encouraging Canadians to invest in cryptocurrency, when we know that doing so will cause them to lose their savings.

That is ridiculous.

\* \* \*

[English]

**LABOUR**

**Mr. Taleeb Noormohamed (Vancouver Granville, Lib.):** Mr. Speaker, protecting and extending workers' rights is a priority for this government, and these rights must never be taken for granted. The House unanimously passed Bill C-3, which established 10 days of paid sick leave for all federally regulated workers.

Can the Minister of Labour tell us when paid sick leave for workers will come into effect and discuss the importance of these measures for Canadians in federally regulated sectors?

**Hon. Seamus O'Regan (Minister of Labour, Lib.):** Mr. Speaker, right around this time last year, the House unanimously committed to providing 10 days of paid sick for workers in the federally regulated private sector, and I am happy to stand here today to say

we made good on that promise. Paid sick leave is now in force today for all federally regulated private sector workplaces.

This is good for all of us. It will make our economy stronger and it will make our workplaces safer. Workers should not have to choose between getting paid and getting better. I want to thank the Speaker and all members of the House.

\* \* \*

**HEALTH**

**Mr. Taylor Bachrach (Skeena—Bulkley Valley, NDP):** Mr. Speaker, Terrace, B.C., has the third-highest death rate from toxic drug overdoses in our province, yet northern residents are still struggling to access detox and treatment services. People often have to wait weeks to get a bed in a facility, and when they do get a space, they have to travel hours away from home.

The Northern First Nations Alliance has a real plan for a new treatment centre right in northwest B.C. It just needs support with the cost.

Will the minister step up and ensure this project is completed as soon as possible?

● (1510)

[Translation]

**Mrs. Élisabeth Brière (Parliamentary Secretary to the Minister of Mental Health and Addictions and Associate Minister of Health, Lib.):** Mr. Speaker, I thank my colleague for his question.

We all know that the toxic drug and overdose crisis has a very painful effect on families and communities. We are working with the provinces and territories to put in place every tool and program we can to improve the situation.

Since 2017, we have invested over \$800 million to respond to this crisis and we will continue in that direction.

\* \* \*

[English]

**HOUSING**

**Mr. Mike Morrice (Kitchener Centre, GP):** Mr. Speaker, last week Canada's federal housing advocate was clear that the national housing strategy is failing. In my community we are seeing this first-hand. Over the past three years, the number of people experiencing homelessness has tripled. Organizations across the Waterloo region are ready to build the affordable housing we need, but they are still waiting on federal funding.

Will the Minister of Housing commit to ensuring the national housing strategy actually reduces homelessness in my community and in others across the country?

*Government Orders*

**Hon. Ahmed Hussen (Minister of Housing and Diversity and Inclusion, Lib.):** Mr. Speaker, this is a really important issue. That is why our government has prioritized investments to reduce and eventually eliminate chronic homelessness from Canada. We have doubled the federal program to combat homelessness, from \$2 billion to just over \$4 billion. In addition to that, we have introduced the rapid housing initiative, which has resulted in 10,250 deeply affordable homes, targeting the most vulnerable members of our communities.

We know those investments are working all across the country. Some 64,000 Canadians were prevented from joining the ranks of the homeless in this country, and 32,000 were taken out of homelessness.

\* \* \*

**PRESENCE IN GALLERY**

**The Speaker:** I wish to draw the attention of members to the presence in the gallery of the Social Sciences and Humanities Research Council of Canada 2022 Impact Award winners: Cindy Blackstock, Fannie Lafontaine, Semra Sevi, Jordan Stanger-Ross and Jan Grabowski.

**Some hon. members:** Hear, hear!

[*Translation*]

**The Speaker:** The hon. member for Mégantic—L'Érable on a point of order.

**Mr. Luc Berthold:** Mr. Speaker, during oral question period, I quoted a document from the director of the Canadian Security Intelligence Service. I decided to follow his instructions and ask for permission to openly and transparently table the report that he submitted to the Standing Committee on Procedure and House Affairs regarding foreign interference in our election.

**The Speaker:** All those opposed to the hon. member moving the motion will please say nay.

**Some hon. members:** Nay.

---

**GOVERNMENT ORDERS**

• (1515)

[*English*]

**NATIONAL COUNCIL FOR RECONCILIATION ACT**

The House resumed from November 30 consideration of the motion that Bill C-29, An Act to provide for the establishment of a national council for reconciliation, be read the third time and passed.

**The Speaker:** It being 3:11 p.m., pursuant to order made on Thursday, June 23, the House will now proceed to the taking of the deferred recorded division on the motion at third reading stage of Bill C-29.

[*Translation*]

Call in the members.

• (1525)

[*English*]

(The House divided on the motion, which was agreed to on the following division:)

(*Division No. 230*)

**YEAS**

## Members

Aboultatif	Aitchison
Albas	Aldag
Alghabra	Ali
Allison	Anand
Anandasangaree	Angus
Arnold	Arseneault
Arya	Ashton
Atwin	Bachrach
Badawey	Bains
Baker	Baldinelli
Barlow	Barrett
Barron	Barsalou-Duval
Battiste	Beaulieu
Beech	Bendayan
Benzen	Bergen
Bergeron	Berthold
Bérubé	Bezan
Bibeau	Bittle
Blaikie	Blair
Blanchet	Blanchette-Joncas
Blaney	Block
Blois	Boissonnault
Boulerice	Bradford
Bragdon	Brassard
Brière	Brock
Brunelle-Duceppe	Calkins
Cannings	Caputo
Carr	Carrie
Casey	Chabot
Chagger	Chahal
Chambers	Champoux
Chatel	Chen
Chiang	Chong
Collins (Hamilton East—Stoney Creek)	Collins (Victoria)
Cooper	Cormier
Coteau	Dabrusin
Dalton	Damoff
Dancho	Davidson
Davies	DeBellefeuille
Deltell	d'Entremont
Desbiens	Desilets
Desjarlais	Dhaliwal
Dhillon	Diab
Doherty	Dong
Dowdall	Dreeshen
Drouin	Dubourg
Duclos	Duguid
Duncan (Stormont—Dundas—South Glengarry)	Duncan (Etobicoke North)
Dzerowicz	Ehsassi
El-Khoury	Ellis
Epp	Erskine-Smith
Falk (Battlefords—Lloydminster)	Falk (Provence)
Fast	Fergus
Ferreri	Fillmore
Findlay	Fisher
Fonseca	Fortier
Fortin	Fragiskatos
Fraser	Freeland
Fry	Gaheer
Gallant	Garneau
Garon	Gaudreau
Gazan	Généreux

*Business of the House*

Genuis  
Gill  
Godin  
Gould  
Gray  
Hajdu  
Hanley  
Hepfner  
Holland  
Hughes  
Hutchings  
Idlout  
Jaczek  
Johns  
Julian  
Kelloway  
Khera  
Kmiec  
Kram  
Kurek  
Kusmierczyk  
Lake  
Lambropoulos  
Lamoureux  
Lapointe  
Lattanzio  
Lawrence  
Lebouthillier  
Lemire  
Lewis (Haldimand—Norfolk)  
Lightbound  
Lobb  
Longfield  
MacAulay (Cardigan)  
MacKenzie  
Maloney  
Masse  
May (Cambridge)  
Mazier  
McDonald (Avalon)  
McKay  
McLean  
McPherson  
Mendès  
Miao  
Miller  
Morantz  
Morrison  
Motz  
Naqvi  
Ng  
Normandin  
Oliphant  
O'Toole  
Paul-Hus  
Perkins  
Petipas Taylor  
Poilievre  
Qualtrough  
Redekopp  
Richards  
Robillard  
Rogers  
Rood  
Sahota  
Saks  
Sarai  
Scarpaleggia  
Schiefke  
Serré  
Shanahan  
Shields  
Sidhu (Brampton East)

Gerretsen  
Gladu  
Goodridge  
Gourde  
Green  
Hallan  
Hardie  
Hoback  
Housefather  
Hussen  
Iacono  
Ien  
Jeneroux  
Jowhari  
Kayabaga  
Kelly  
Kitchen  
Koutrakis  
Kramp-Neuman  
Kusie  
Kwan  
Lalonde  
Lametti  
Lantsman  
Larouche  
Lauzon  
LeBlanc  
Lehoux  
Lewis (Essex)  
Liepert  
Lloyd  
Long  
Louis (Kitchener—Conestoga)  
MacDonald (Malpeque)  
MacKinnon (Gatineau)  
Martel  
Mathysen  
May (Saanich—Gulf Islands)  
McCauley (Edmonton West)  
McGuinty  
McKinnon (Coquitlam—Port Coquitlam)  
McLeod  
Melillo  
Mendicino  
Michaud  
Moore  
Morrice  
Morrissey  
Murray  
Nater  
Noormohamed  
O'Connell  
O'Regan  
Patzner  
Pauzé  
Perron  
Plamondon  
Powlowski  
Rayes  
Reid  
Roberts  
Rodriguez  
Romanado  
Ruff  
Sajjan  
Samson  
Savard-Tremblay  
Scheer  
Seeback  
Sgro  
Sheehan  
Shipley  
Simard

Singh  
Sorbara  
Steinley  
Stewart  
Strahl  
Sudds  
Taylor Roy  
Thomas  
Tochou  
Trudeau  
Turnbull  
Valdez  
van Koeverden  
Vandal  
Vidal  
Viersen  
Villemure  
Vis  
Warkentin  
Weiler  
Williamson  
Zahid  
Zimmer — 315

Small  
Soroka  
Ste-Marie  
St-Onge  
Stubbs  
Tassi  
Therrien  
Thompson  
Tolmie  
Trudel  
Uppal  
Van Bynen  
Van Popta  
Vandenbeld  
Vien  
Vignola  
Virami  
Wagantall  
Waugh  
Wilkinson  
Yip  
Zarrillo

## NAYS

Nil

## PAIRED

## Members

Champagne	Joly
Jones	Martinez Ferrada
Muys	Schmale
Sidhu (Brampton South)	Sinclair-Desgagné
Vecchio	Williams — 10

**The Speaker:** I declare the motion carried.

(Bill read the third time and passed)

**The Speaker:** The hon. member for Regina—Qu'Appelle is rising.

**Hon. Andrew Scheer:** Mr. Speaker, a colleague voted by the app, encountered some technical difficulties and could not log on in time to switch his vote. I am wondering if the House would allow, as we have done in the past for other members, for the hon. member for Foothills to change his vote. His intention was to vote in favour. If the House would grant consent for that change, this would be a unanimous vote in favour of the bill.

**The Speaker:** Do we have unanimous consent of the House?

**Some hon. members:** Agreed.

**The Speaker:** I wish to inform the House that because of the deferred recorded division, Government Orders will be extended by 12 minutes.

We now have the Thursday question.

\* \* \*

## BUSINESS OF THE HOUSE

**Hon. Andrew Scheer (Regina—Qu'Appelle, CPC):** Mr. Speaker, I shudder to think what would happen if the Thursday question was not asked.

*Government Orders*

I have taken the advice the Speaker has given me and the government House leader over the past couple of weeks, so I have a more focused Thursday question. I wonder if the government House leader can inform the House as to the business of the House for this week and next week?

While I am on my feet, I was wondering if the House would give me unanimous consent to table in the chamber the list of firearms used for hunting, because there seems to be some confusion on the government side as to which firearms it would actually be banning in its new amendment to Bill C-21.

**The Speaker:** We will separate that. The hon. member can bring this up right after the Thursday question.

In the meantime, I will ask the government House leader to respond to the question.

**Hon. Mark Holland (Leader of the Government in the House of Commons, Lib.):** Mr. Speaker, we will need to wait for the unanimous consent motion to see what will happen. I will wait for that. There is good news for the member opposite in that he has the opportunity, at committee of course, to review those guns and make any suggestions his members would like. I am sure, as a long-serving member, he would be aware of that opportunity, but I just remind him of that.

The Speaker will be pleased to know we will continue with debate at second reading of Bill C-26, an act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other acts. Tomorrow we will begin debate at second reading of Bill C-23, the historic places of Canada act.

On Monday, we will begin debate at report stage and third reading on Bill C-32, the fall economic statement implementation act, 2022. Thursday will be the final allotted day of the current supply period. For the rest of the week, priority should be given to Bill C-32.

I would also like to indicate that on Tuesday there will be a statement by the minister on the commemoration of the Polytechnique massacre.

• (1530)

**Hon. Andrew Scheer:** Mr. Speaker, I am rising on a point of order.

Hope springs eternal, and maybe while the government House leader was answering my question, he reflected on the benefit of all members having this information right now, because oftentimes the answers to questions indicate some confusion on the government side as to the hunting rifles that would be banned in the bill.

Do I have unanimous consent—

**The Speaker:** This is not the debate we are going to.

\* \* \*

### TELECOMMUNICATIONS ACT

The House resumed consideration of the motion that Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, be read the second time and referred to a committee.

**Mr. Ziad Aboultaif (Edmonton Manning, CPC):** Mr. Speaker, we live in a world where every person is increasingly concerned with cybersecurity. So much of our lives is stored on our personal devices, protected by passwords and multi-factor authentication in the hopes of keeping our most private information secure.

Corporations are increasingly at risk. It seems as if every day we hear a new report of companies' computer systems being hacked and their data held for ransom by thieves who have managed digital anonymity. Law enforcement officials say many such cybercrimes go unreported, with companies paying quietly and privately so as to avoid publicity.

Our public institutions are not immune either. Hospitals have had their computer systems attacked by intruders, putting patients' lives at risk. Emergency services have been attacked, as have the parliamentary computer systems.

Cyber-threats remain a national security and economic issue that threatens the safety and security of Canadians. Government and industry alike have highlighted the need for regulation in cybersecurity. There has been a lot of talk, but not much else.

Currently the Canadian government does not have a legal mechanism to compel action to address cyber-threats or vulnerabilities in the telecommunications sector, yet cybersecurity has become one of the primary issues each person and institution has to address. I am pleased that the government has introduced this legislation to allow us in the House to examine the cybersecurity concerns and needs of our nation.

Bill C-26 would amend the Telecommunications Act as well as other related acts. The intention would be to amend the Telecommunications Act to add the promotion of the security of the Canadian telecommunications system as an objective of Canadian telecommunications policy and to authorize the Governor in Council and the Minister of Industry to direct telecommunications service providers to do anything, or refrain from doing anything that is necessary to secure the Canadian telecommunications system.

I do not think there is anyone in the House, indeed in the country, who would disagree with the objective. As I have already pointed out, there is a problem with cybersecurity in our society, and government has an important role to play in protecting Canadian individuals and institutions. Some may wonder about giving such power to the Governor in Council and the Minister of Industry, but there are rules for the judicial review of those orders and applications. This is not a granting of absolute power, but of limited power subject to the checks and balances needed in a democracy.

*Government Orders*

The bill would also enact the critical cyber systems protection act to provide a framework for the protection of the cyber systems of services and systems vital to national security or public safety. This, among other things, would authorize the Governor in Council to designate any service or system as a vital service or vital system. It would require designated operators to establish and implement cybersecurity programs, mitigate supply chain and third party risks, report cybersecurity incidents and comply with cybersecurity directions.

One would think that such cybersecurity measures should be common sense and not need to be mandated by government. Is it right to compel private corporations and organizations to use their own resources to invest in cybersecurity? It would seem to me that well-run businesses would put cybersecurity first. Not every aspect of a business generates income, and smart business managers and owners know that. As the cliché goes, they have to spend money to make money.

Implementing cybersecurity measures comes with a cost. There is no doubt about that. It would seem to me, though, that the cost would be considerably less than the cost of dealing with criminals holding their data for ransom after they have invaded their computer system and locked them out of it.

• (1535)

Cybersecurity makes common sense for business. However, given that implementing cybersecurity measures comes with a financial cost with no corresponding revenue, do we really want to rely on those who might put short-term profits first, or does it make more sense in this case for government to step in to save some business owners from themselves?

As someone who has spent most of his life working as a businessman, I am reluctant to suggest that business owners need to be saved from themselves, but as a Canadian I know that sometimes such action is necessary.

We have only to look at the history of one of Canada's most successful companies: Nortel. It is a company that might still exist if those running it had taken cybersecurity more seriously. With more than 94,000 employees worldwide, Nortel was a high-tech leader until its headquarters were bugged, its computer systems breached and its intellectual property stolen. Now it is just a memory. We will never know for sure, but perhaps if cybersecurity had been a higher priority at Nortel, it would still be providing jobs, products and services for Canadian people. If anyone ever asks why we would take cybersecurity seriously, the one-word answer is "Nortel".

Though I am a little uneasy that this bill would almost certainly increase regulations and red tape, maybe there are ways that some of the excessive paperwork that seems to be beloved by the Liberals can be made reasonable. Certainly there is a need to ensure a level playing field of regulatory burdens for small and medium-sized businesses and organizations. If there is not, then I can see companies being forced into bankruptcy by the cost of implementing government-mandated cybersecurity procedures. I know that is not the government's intention, but as we have seen in the past, sometimes not all the impacts of government rule-making are foreseen. The Minister of Industry especially needs to ensure that the

rules are workable and provide protection against attacks by criminals and malicious states.

Indeed, it is perhaps malicious states that we should be concerned about the most. The interconnectedness of computer systems and their use in controlling and maintaining our infrastructures mean we are increasingly vulnerable to a devastating attack. An enemy that could seize control of our electricity grid or our banking system could bring our nation to its knees without firing a shot. The nature of warfare has changed, and as a result we must change our defences.

Canada's national security requires being prepared for the security warfare threats that we face. The government has been slow to address cyber-threats and has seen a number of serious incidents occur, with no substantive legislative response for seven years. I am pleased that the government has finally chosen to act, and I am hopeful that we in the House can help improve this legislation. Cybersecurity is of paramount importance in the modern world. Canada cannot neglect it.

• (1540)

[*Translation*]

**Mr. Martin Champoux (Drummond, BQ):** Madam Speaker, I want to congratulate my colleague on his speech.

Cybersecurity is essential, and it is also a race against time because hackers are becoming better and better organized. They are fast, equipped, cunning and, on top of that, dishonest. That gives them an advantage over us presumably honest people.

The government has been slow to act, legislate and get aggressive with cybersecurity.

Does my colleague think that there is still time to take the lead in this race, or are we going to continue to fall behind international hacker organizations?

[*English*]

**Mr. Ziad Aboultaif:** Madam Speaker, I mentioned at the end of my speech that the government was very late in putting forward such a bill. It is a very tough question to answer as to whether or not we can catch up. We know the existing wars and challenges and future wars are mostly around cybersecurity. It will be important in this motion of the House, with this bill, to assess how prepared Canada is for facing future threats.

**Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.):** Madam Speaker, within the legislation there is consideration given to how financial penalties would empower the minister to take strong action to ensure that providers are keeping up with what they need to keep up with.

*Government Orders*

My question to the member is this. Would he agree that when we take a look at the issue of cyber-attacks, they are not something unique to Canada? It is happening around the world. We are working with allied countries and others. This is one part. It does not stop here. There is a need to continue, as we have for the last number of years, investing tens of millions of dollars and putting people to the task of protecting us against cyber-threats.

Could the member just provide his thoughts in terms of the broader picture of cyber-threats?

**Mr. Ziad Aboultaif:** Madam Speaker, I will answer the end of the question and go back to the beginning of what the hon. member asked.

We are still not there in terms of assessing our preparedness and our cybersecurity position. I do not know if we have enough understanding of those challenges, what our position is and how prepared we are. That is a very important task for the government.

As far as financial penalties on businesses, I mentioned in my speech that such things could put some businesses into bankruptcy, because they would not be able to afford the services that would provide the protection needed for them not to end up in such a disastrous situation.

Therefore, a balance is needed, and this has to be done by working together with the industry. If we are truly prepared, the financial penalties should be less, because the government should have done more in the last seven years, or even the years before that, in terms of looking to the future.

It all remains in the hands of the government that is putting this bill forward. We hope to get some answers.

**Ms. Heather McPherson (Edmonton Strathcona, NDP):** Madam Speaker, that was a very interesting intervention. I am not a specialist in cybersecurity, so I am finding this debate very informative.

I guess one of the questions I have is about how we balance the need for cybersecurity with the need for transparency. That is really what the big question is for this. How do we make it effective but also adhere to the Canadian values of transparency, human rights and whatnot?

I wonder if the member has anything to say about the fact—

**The Assistant Deputy Speaker (Mrs. Alexandra Mendès):** I have an hon. member with a point of order, and I think I know what the hon. member is going to say. The hon. member asking the question does not have her headset, and we do not allow members to speak without a headset. That is on me, with my apologies.

I will have to interrupt the hon. member right now and give the hon. member for Timmins—James Bay a very short question, please.

• (1545)

**Mr. Charlie Angus (Timmins—James Bay, NDP):** Madam Speaker, cyber-threats are not new. In 2011, Canada's two main financial centres in government, Finance and the Treasury Board, were pushed off-line for days by hacks from Chinese operators, yet the Harper government did nothing about that. It did not want to

talk about it because it was busy selling off sections of the oil sands and Nexen to Chinese state-owned operators and then signing a free trade deal with China, the deal that would allow it to take on Canada outside of the court system.

I find it kind of special that the Conservatives are suddenly concerned about cybercrime now, when they did nothing to take on China's state threats to Canada under Harper.

**Mr. Ziad Aboultaif:** Madam Speaker, the NDP member always wants to politicize things. This is a very serious issue, and there is not one party that is more serious about this than others. I wish he had stayed within the non-partisan notion of this bill. Let us talk about facts. Let us talk about logic and stop the attacks.

**Mr. Ryan Turnbull (Whitby, Lib.):** Madam Speaker, before I begin, I will just say that I will be splitting my time with the member for Kingston and the Islands.

It is an honour to rise today in the House to debate the second reading of Bill C-26, an act respecting cybersecurity. To me, cybersecurity is essential, and it certainly relates directly to our national security.

When we consider the challenges and opportunities we face in this field, the theme of collaboration underpins and needs to underpin all that we do.

The prevalence of cybercrime in an increasingly online world, improving cyber-defence posture in an unstable global environment, deep thinking about what the future holds in a world where innovation and change are exponential, a critical look at whether our policies and laws are up to the task, and the protection of content and intellectual property as data becomes one of the world's most precious resources: These are just some of the reflections that we have to have when considering this bill.

In Canada, being online and connected is essential. Now, more than ever, Canadians rely on the Internet for their daily lives. It is about more than just conducting business and paying bills. It is also about staying connected with loved ones across the country and around the world. We should be able to do all these activities safely and securely.

I would like to offer a few words about what we are doing here in Canada to get that balance right, and I would like to reinforce the importance of our commitment to protecting the cyber systems that underpin our critical infrastructure.

We can take the emergence of new technologies, such as 5G, as one clear reason we need to redouble our efforts. We think about our increased reliance on technology in light of the COVID-19 pandemic. We think about international tensions amidst Russia's unprovoked and unjustified ongoing invasion of Ukraine, with threats ranging from supply chain disruptions to state and non-state malicious cyber-activity.



Through all of these remarkable events, the government has been working tirelessly to keep Canadians safe. We recognize that, now more than ever, secure and reliable connectivity is a necessity for our daily lives and our collective safety and security. It underpins the delivery of critical services, such as energy production, financial transactions, safe transportation and emergency communications.

As part of his mandate, bestowed by Prime Minister Trudeau, the Minister of Public Safety is seized with the opportunity and challenge of developing a renewed national—

**The Assistant Deputy Speaker (Mrs. Alexandra Mendès):** The hon. member for Battle River—Crowfoot is rising on a point of order.

**Mr. Damien Kurek:** Madam Speaker, as was pointed out by the parliamentary secretary to the government House leader yesterday, the use of the Prime Minister's name is not an accepted practice of this place.

**The Assistant Deputy Speaker (Mrs. Alexandra Mendès):** The hon. member is correct. We do not use the names of current members of Parliament.

**Mr. Ryan Turnbull:** Madam Speaker, as part of the mandate bestowed upon him by the Prime Minister, the Minister of Public Safety is seized with the opportunity and challenge of developing a renewed cybersecurity strategy. We need to make sure we articulate Canada's long-term plan to protect our national security and economy, deter cyber-threat actors, and promote norms-based international behaviour in cyberspace.

The Government of Canada is working to enhance the cybersecurity of the country's critical infrastructure. The work to identify cyber-threats and vulnerabilities, and to respond to cyber-incidents, is around the clock and ongoing. Unfortunately, we have seen that malicious actors continue to attempt to take advantage of the current environment to exploit certain sectors. I would like to use one example that is relevant for my riding and the region I come from.

My riding is the riding of Whitby, and Durham District School Board is the public school board in our area. On Friday, November 25, just very recently, there was a cyber-incident at the Durham District School Board. It resulted in online classes being cancelled. They were forced to postpone scheduled literacy tests. They have had phone lines down and email service down. They even do not have access to emergency contacts, and they are trying to limit this incident so it does not impact payroll for the over 14,000 Durham District School Board employees. There are 75,000 students who go to school across our region.

They have notified police of the attack. Their investigation is said to be very complex and time consuming, and they will be assessing the privacy impacts, but we can just imagine how this has impacted students and employees at Durham District School Board.

This is a really serious topic. I think we all need to give it the weight it deserves, and this legislation is trying to ensure we do our utmost to protect against these cyber-threats in the future.

However, we are not starting from scratch to tackle these threats. Since 2018, the Government of Canada has invested a total of approximately \$4.8 billion in cybersecurity. Through the national cy-

### *Government Orders*

bersecurity strategy, the Government of Canada would be taking decisive action to strengthen Canada's defence, preparedness and enforcement against cyber-threats. The strategy was paired with the largest investment in cybersecurity ever made by the Government of Canada, totalling close to \$800 million in the 2018 and 2019 federal budgets.

In the 2021 budget, the government allocated an additional \$791 million to improve and defend cyber-networks, enhance data collection and protect taxpayer information, and in the 2022 budget, another \$852.9 million was committed to enhance the Communications Security Establishment and its ability to conduct cyber-operations, make critical government systems more resilient, and prevent and respond to cyber-incidents on critical infrastructure.

Under the strategy, two flagship organizations were established. One is the Canadian centre for cybersecurity, otherwise known as the cyber centre, under CSE, and the other is the national cyber-crime coordination centre under the RCMP.

The cyber centre is a single, unified team of government cybersecurity technical experts. The centre is the definitive source of unique technical advice, guidance, services, messaging and support on cybersecurity operational matters for government, critical infrastructure owners and operators, the private sector, and the Canadian public.

The NC3 coordinates Canadian police operations against cyber-criminals and established a national mechanism for Canadians and businesses to report cybercrime to police. In the example I mentioned in my riding of the Durham District School Board, it would report the cybercrime to the local police, and that would go up through NC3 as well.

Public Safety Canada's Canadian cybersecurity tool also helps owners and operators of Canada's critical infrastructure to evaluate their cyber-maturity against established benchmarks and by peer comparison. It offers concrete guidance on how they can become more cyber-resilient.

● (1550)

Public Safety Canada also coordinates and delivers cyber-based exercises for the critical infrastructure community to test and develop capabilities to respond to and recover from malicious cyber-activities. More broadly, the department, as the federal lead on cybersecurity policy, promotes communication and collaboration to raise awareness of cyber-threats and risks, including with our international partners. Public Safety Canada works closely with the Communications Security Establishment's Canadian centre for cybersecurity to enhance the resilience of critical infrastructure in Canada. The cyber centre, in addition to providing public advisories, shares valuable cyber-threat information with Canadian critical infrastructure owners and operators.

*Government Orders*

Today I am very proud to say that we can begin to debate a new piece of legislation to further strengthen what we have built as a government. Today we are debating Bill C-26 for the second reading, and this legislation's objective is twofold.

The first part proposes to make amendments to the Telecommunications Act, which include adding security as a policy objective, adding implementation authorities and bringing the telecommunications sector in line with other critical infrastructure sectors. This would allow the government, when necessary, to mandate any action necessary to secure Canada's telecommunications system, including its 5G networks. This would include authority to prohibit Canadian telecommunications service providers from using products and services from high-risk suppliers.

The second part introduces the critical cyber systems protection act, or CCSPA. This new act would require designated operators in the federally regulated sectors of finance, telecommunications, energy and transportation to take specific actions to protect their critical cyber-systems, and it would support organizations' ability to prevent and recover from a wide range of malicious cyber-activities, including malicious electronic espionage and ransomware.

• (1555)

[*Translation*]

**Mr. Denis Trudel (Longueuil—Saint-Hubert, BQ):** Madam Speaker, I am not a cybersecurity expert either.

A few weeks ago, I attended a demonstration in Montreal with 10,000 people to support the people who are fighting for their freedom in Iran, which, as we know, is not a democratic state. I have also strongly supported people from the Uighur community, who I have met with many times here in Ottawa. We know that they are facing genocide in China. The small white square that I am wearing is a sign of support for people who, at this time, are rising up against the health measures in China, as well as the people in Russia who are protesting against the war in Ukraine.

I want to know if there are concrete measures in Bill C-26 that would prevent Iran, China and Russia from carrying out cyber-attacks on social networks and, for example, hacking my account and interfering in my life as an MP? I would like my colleague to clarify that.

[*English*]

**Mr. Ryan Turnbull:** Madam Speaker, I share the member opposite's ethical concerns with other state-sponsored actors, disinformation and ensuring that our cyber-infrastructure and our lives as MPs are also protected from the attacks and incidents that are too often affecting some of our institutions and even us, as individuals.

This bill really looks to strengthen the work the government has been doing year over year to invest in protections against cyber-attacks in our critical infrastructure and to ensure that we are enhancing those tools and investments, and leveraging them to the best degree possible to protect against the kinds of threats the member opposite identified.

**Mr. Damien Kurek (Battle River—Crowfoot, CPC):** Madam Speaker, cybersecurity cannot be underestimated in its importance, especially in the world in which we live.

One of the concerns that has been highlighted to me, as I listened to security experts surrounding this issue, is how far behind Canada is in taking action on cybersecurity, whether that be the decision regarding Huawei, or how Canada lags behind its Five Eyes partners. Taking action is essential in ensuring that we are on the same playing field.

I am wondering if the member from the government would be willing to expand as to why, after years of being in government, this is only now being debated in the House of Commons.

**Mr. Ryan Turnbull:** Madam Speaker, I am not really sure how we get these types of critical remarks coming from the opposite side of the House given that in my speech I gave very tangible examples of two agencies that have been set up and some pretty significant investments that have been made since 2018. The \$4.8 billion for cybersecurity is no small amount. We are making investments and setting up the systems and tools.

I have been briefed, as a member of the procedure and House affairs committee, on our House of Commons cyber-infrastructure and cybersecurity. Although those briefings were in camera, I know full well that very strong and resilient systems have been set up to identify and neutralize threats ahead of time to ensure our critical infrastructure in the House of Commons is protected. I think that extends right across Canada with the work that our government has been doing.

• (1600)

**Ms. Heather McPherson (Edmonton Strathcona, NDP):** Madam Speaker, I want to take a moment to apologize to the interpreters for when I completely forgot my headset previously. I am not feeling my best, and I am obviously not on my game.

I want to thank my colleague for his intervention today. It was very interesting. I agree with my colleagues from the Conservative Party that we are very late to the game, but I think it is vital that we get it right. It is just so important that we do that balance.

One of the concerns we are hearing from the stakeholders we have spoken to is that this bill has orders that will be exempt from the Statutory Instruments Act. Therefore, it would be unable to be reviewed under scrutiny at the regulations committee. Could the member speak to why the government made that decision?

**Mr. Ryan Turnbull:** Madam Speaker, as I am not sure of the specific details the member opposite is referring to in her question, I would have to say, in good faith, that I will get back to her on that after doing a bit more research on why that decision was made.

What I can tell her is that the key provisions in this act really do further the overall objectives of protecting our critical infrastructure. It specifically adds to the Telecommunications Act the objective of the "promotion of the security of the Canadian telecommunications system as an objective of the Canadian telecommunications policy and to"—

*Government Orders*

**The Assistant Deputy Speaker (Mrs. Alexandra Mendès):** I must interrupt the hon. member. We are way over time.

Resuming debate, the hon. parliamentary secretary to the government House leader, Senate, has the floor.

**Mr. Mark Gerretsen (Parliamentary Secretary to the Leader of the Government in the House of Commons (Senate), Lib.):** Madam Speaker, I thank the member for Whitby for sharing his time with me.

It is very important that we talk about such an important piece of legislation that has been brought forward, Bill C-26. The reality is that the changes in technology are happening so incredibly quickly. At times, it seems a daunting task to keep up with them and to make sure that we are always ahead of those actors out there, whether state or non-state, who are trying to engage in activities that could seriously cripple our economy or other aspects of society in Canada.

It seems as though it was just yesterday that we did not have the Internet. I remember vividly when I signed up for my first Internet connection, a dial-up connection, and having access to the Internet. That was when I was a computer engineering student at a local college in Kingston back in 1995 or 1996. Downloading something as simple as a single image sometimes would take two or three minutes to get the full image on the screen.

**Mr. Philip Lawrence:** What did you download?

**Mr. Mark Gerretsen:** Madam Speaker, it was not an image of the member opposite who is asking.

The point here is that things are evolving so quickly, and we have come so far in such a short period of time in terms of our ability to utilize, perfect and, for lack of a better term, exploit everything that the Internet has to offer. We have seen it change commerce. We have seen it change how we engage with each other. We have seen it change just about every aspect of our lives. Unfortunately, with that comes new opportunity for people to try to affect what we do in our day-to-day lives. They are trying new forms of fraud, theft, harassment, intimidation and influencing elections, which are all nefarious manners in which people are trying to now utilize the Internet.

Of course, cybersecurity is a huge part of any government operation now, and every government should be seized with doing everything it can to secure it, because when we think about it, everything is connected. There could be a cyber-attack on a utility company, on a functioning parliament, a democracy. There could be an attack on just about every aspect of our lives, and it is critical that we have legislation in place to ensure that we can properly safeguard those things.

I have heard individuals in the House, and in the last two questions, one from the Conservatives and one from the NDP, suggesting that this is taking way too long and that we are behind other countries. I would caution members on that and suggest that it is not entirely accurate. For example, the United Kingdom has a very similar bill to this one that is being studied right now by its members of Parliament, a Conservative government, I might add. They are going through the exact same process as we are now. I think it

is always easy to say, and it is one of the things we hear quite a bit from opposition parties, why is this taking so long?

I have my own opinion on why things take so long in this House, but the reality is that I do not believe we are significantly trailing behind other countries. Yes, some countries have done more than us. I am not going to disagree with that, but I disagree that we are significantly behind. I will come back to the United Kingdom where a Conservative government has introduced a very similar piece of legislation to what we have. This brings me to the legislation that we are debating today.

This bill has two primary parts to it. The first part would amend the Telecommunications Act to add the objective of the promotion of cybersecurity of the Canadian telecommunications system to Canadian telecommunications policy.

• (1605)

It also authorizes the Governor in Council and the Minister of Industry to direct telecommunications service providers to secure the Canadian telecommunications system. I think that is incredibly important. In this process, we have to remember that a huge part of what we need to do is work with private partners and the various telecommunications services that are out there. We need, from a policy or government perspective, to put in place some of the things that they need to do.

The reality is that in a competitive business environment where various different telecommunications companies are fighting to be more competitive and more efficient to maximize profit, which we all appreciate is important in the capitalist environment we live in, we have to respect the fact that in order to ensure that some of these safeguards are in place, we are going to need to make sure that the legislation is there to make sure companies are doing what they need to be doing to create those safeguards. Otherwise, it might not happen to the degree it needs to because of the nature of the competitive environment they are in.

The other aspect of this bill is that it enacts the critical cyber systems protection act to provide a framework for the protection of critical cyber systems that are vital to national security and public safety. Of course, this is key because this is what everything else is built on in terms of our national security and the systems that we have. We need to make sure we can properly safeguard those. In that regard, it authorizes the Governor in Council to designate any service or system as a vital service or vital system. Just think about that.

When I was in college studying computer engineering and I went to get my first dial-up connection, who would have thought that a mere 25 years later we would be talking about designating some of these services as being vital to national security or public safety? The reality is that is where we are now. As we rely so heavily on these systems, we rely so heavily on ensuring that we have the systems in place that we do in order to protect our security as it relates to cyber-threats.

*Government Orders*

I appreciate the opportunity to talk about this very important piece of legislation. I get the sense it is being widely supported in the House. I hope we can move this along so we can get to the next steps, continue to move forward and get what we need into place in order to properly protect our cyber systems from a security perspective.

• (1610)

[*Translation*]

**Mr. René Villemure (Trois-Rivières, BQ):** Madam Speaker, I thank my colleague from Kingston and the Islands for his speech, which was informative as always.

However, I would like to know how this bill will enhance public trust in the Internet. What mechanism in Bill C-26 will help guarantee public trust?

[*English*]

**Mr. Mark Gerretsen:** Madam Speaker, as I said in my speech, one of the things the bill does is it specifically directs what the various telecommunications providers need to do in order to maintain that security. That is what we do from a policy perspective. We establish what those requirements are that are required of the telecommunications systems in order to ensure that security is there. What we will see coming out of this is that the telecommunications systems, in a unified fashion, will promote these particular policies and safeguards that will be put through those directives.

**Mr. Charlie Angus (Timmins—James Bay, NDP):** Madam Speaker, one of the things that has become very clear, particularly since the Russian invasion of Ukraine, is how destabilized our world is and how many bad actors are out there at the state level trying to undermine democracy.

My concern is about the ability of the federal government to withstand cyber-attacks. Earlier today, I talked about 2011 when actors out of China were able to shut down finance and the Treasury Board for days on end with relentless attacks. With the amount of financial information for Canadians that is in those departments, that is very serious.

We know that in the immigration department, which has turned into an absolute nightmare for anybody trying to navigate it, the system is breaking down. Staff in the department cannot access information files because the system is not up to speed. This will require a major investment to protect people, but also to deal with dark forces, whether they are Russians, the Chinese or any other non-state actor.

Has the government put in a credible plan to ensure we get our federal systems up to speed to be able to withstand hackers?

**Mr. Mark Gerretsen:** Madam Speaker, this is the basic fundamental principle to having our full and complete autonomy over our nation.

We need to ensure that these systems are secure—

[*Translation*]

**The Assistant Deputy Speaker (Mrs. Alexandra Mendès):** Order. The hon. member's microphone is causing an audio problem that is interfering with the interpreter's audio.

[*English*]

**Mr. Mark Gerretsen:** I apologize, Madam Speaker. It is not my first day. I should not have let that happen. I apologize to the interpretation staff, through you.

Getting back to what I was saying, in order to maintain that autonomy which we must have as a country, we need to make sure that the proper investments are in place to do that. The member indicated there would need to be a major investment. My own personal perspective is that we should spare no expense to ensure that security is absolutely robust.

Will there be penetrations or will there be times when it might be challenging to maintain that? Yes, but we learn from those. With regard to his example from 2011, I believe we learned from that and we made our systems even better as a result.

• (1615)

**Mr. Philip Lawrence (Northumberland—Peterborough South, CPC):** Madam Speaker, I can attest that this is not the gentleman's first day. It seems like I have spent a year staring into his eyes here.

In the legislation, there is a fair bit of gray area with respect to definitions. Will the government be releasing additional information on such undefined terms as “cyber- incidents”?

**Mr. Mark Gerretsen:** Madam Speaker, I am flattered to hear that the member has been staring into my eyes for a year.

In all seriousness, the member asks a good question. I do not have the answer to that. I am certainly not in a position to be able to provide to him what the government would release later. When the government tables a bill or releases information to Parliament, it does so in a fashion that allows every member of Parliament access to that at the same time. The member's access to that would be no different from mine.

**Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC):** Madam Speaker, I will be sharing my time with the member for Battle River—Crowfoot.

I am proud to rise on behalf of my constituents in the not-quite-fully-connected riding of Renfrew—Nipissing—Pembroke. As the longest-serving member of the national defence committee, I fully appreciate the need for Canada to secure critical cyber systems.

For too long, the government remained indifferent while Canada's telecom companies were being infiltrated, robbed of intellectual property and sabotaged. It took the collective pressure of our Five Eyes allies before the government put up any resistance to the Huawei expansion throughout Canada's telecom infrastructure.

Only after having been thoroughly shamed and threatened with being cut off from critical security intelligence has the government finally responded with legislation. However, as is so often the case with all governments, having finally been shamed into action, the executive branch overreacted. It now falls upon Parliament to moderate the executive overreach.

*Government Orders*

Cybersecurity is not a partisan issue. No party ran on a platform to make Canada insecure again. The Conservatives support sending this bill to committee for carefully considered amendments. I hope my colleagues across the aisle will be open to working in a collegial way to ensure that we as parliamentarians strike the right balance. This legislation must balance security with privacy and transparency. It must balance expeditiousness with efficiency and effectiveness.

I appreciate that the members opposite will place greater trust in this government than most Canadians will, but what about the next government or the one after that? Our duty as parliamentarians is to keep in check not just this government but future governments as well. To that end, I encourage all parties to work together at committee and bring back a bill that we can all support.

There are four main issues that need high-level scrutiny. However, as we saw with the invocation of the Emergencies Act, even when Parliament gives clear definitions, the executive branch believes it can extrapolate or simply opt for an overly broad interpretation. While the government has been forced to defend its decision on the use of the Emergencies Act in a public inquiry, Bill C-26 lacks any significant accountability measures while granting even more extraordinary powers, including issuing secret orders.

It should not fall upon the operators of critical cyber systems to guess what the government means by “immediately”. The bill currently grants the government the power to order telecom providers to do anything necessary to secure the telecommunications system. Granting the executive the power to do anything would be a dereliction of our duty as parliamentarians. To give the government the power to do anything while enabling those things to remain secret would be an outright betrayal of our duty.

It is understandable and reasonable that some secrecy is required to combat foreign espionage, but there must be clearly defined limits. There must be avenues for operators to appeal and for Parliament to scrutinize the government’s actions. By “Parliament” I mean Parliament. I do not mean some government committee of parliamentarians but a parliamentary committee.

This bill grants the government the power to deny services to any company or person by secret order. Had this law already been in place, there would be nothing to stop a government from cancelling the Internet and phone service of protesters the government disagrees with.

Granting the government the power to deny services to individuals using secret orders clearly violates the legal rights of Canadians. I do not want to trust the government with that kind of power. I expect my Liberal colleagues would not trust that kind of power when the Conservatives form government, hopefully very soon.

To paraphrase a great comic character, with great power must come great accountability. There are serious cyber-threats and those threats are growing. The government must have the tools to respond quickly and decisively, yet when governments move quickly, mistakes are made. That is why it is all the more important for there to be a robust set of measures to review their actions and ensure accountability when the government makes a mistake.

This legislation takes the extraordinary step of placing personal liability on individual employees of critical infrastructure operators. We threaten people with jail time to ensure they are accountable for their companies' cybersecurity, yet we do not hold government employees or ministers to the same standard. Just as the House must find the appropriate balance between security, secrecy and accountability, so too must we find the balance between privacy and transparency.

● (1620)

The government learned first-hand the public’s reaction to its undisclosed use of mobility data from millions of cellphone users. Canadians had demonstrated a willingness to abide by public safety measures, even extraordinary measures, but the minute the government started tracking our cellphones, even for a public health purpose, Canadians reacted strongly. Even Canadians who supported forced vaccination and punishing the unvaccinated drew a line at cellphone tracking.

The legislation before us would grant even more power to collect data from telecom providers with no restrictions on distributing it to other departments. Even if this data was held by the CRTC, Canadians would be concerned about their privacy. However, it would not be the CRTC doing the data scoop; it would be the Communications Security Establishment.

I appreciate the government feels the CSE is best equipped for countering cyber-threats, but the main purpose of the CSE is collecting intelligence from abroad. The CSE does not report to the public safety minister, who is responsible for keeping Canadians secure. The CSE does not report to the industry minister, who is responsible for telecoms regulations. The CSE reports to the defence minister. It is a fundamentally different type of organization from CSIS or the CRTC.

The legislation would fail to place sufficient limits on what the CSE can do with the data it can secretly order telecoms to provide. In no way is this meant to disparage the work done by the CSE, but as we expand the powers of the CSE, we must also constrain the scope of what it can do with those powers.

*Government Orders*

These are just some of the trade-offs we must consider when the bill goes to committee. Groups such as the Canadian Civil Liberties Association, the Citizen Lab and the Business Council of Canada have raised several more. However, the one area none of these groups have touched on, at least to my knowledge, is the role private citizens can play in securing Canada against cybersecurity threats. Parliamentarians have studied this both at the defence committee and with our fellow legislators at the NATO Parliamentary Assembly. Canada can take a lead role internationally in cybersecurity by enlisting the aid of ethical hackers, commonly referred to as “white hats”.

White hat hackers represent an untapped resource for a country as large as ours. Our critical infrastructure spans a continent. The job of securing it exceeds the capacity of the federal government and infrastructure operators. If we can develop a framework that protects and incentivizes white hat hackers, we may have a solution. As with the measures already in the legislation, such a framework would involve trade-offs. Even an ethical hacker could unwittingly cause significant cyber-disruption and damage, but they can just as easily expose flaws and gaps.

Regardless of whether the government acknowledges the existence of ethical hackers, they will continue to operate, and it is better for critical infrastructure operators, public servants and the Canadian public if we find a way to incorporate them into our defence strategy. We need to enlist ethical hackers because we simply do not have the resources as a nation to confront the threats.

Globally, cybercrime costs reached over \$600 billion U.S. in 2021. Investments in cybersecurity were only \$220 billion U.S. last year. Between criminals, terrorists and authoritarian states, the potential for significant damage is accelerating. Our enemies are going to match the best cyber-defences in the world. We do not have the resources to match the United States or the EU. That is why we must be even smarter than our adversaries and our allies.

The legislation is all stick and no carrot. Governments are quick to punish because it is easy. If company X fails to properly secure a critical system, they get a fine, but what if the company innovates and not only prevents an intrusion into their system but detects the source? The bill would require companies to immediately report intrusions, but what about failed attacks? If Bell, Telus and Rogers were to all successfully fend off an attack on the same day, would that not be something we would want the CSE to know about? Punishing failure is an important deterrent, but rewarding success is a powerful incentive.

● (1625)

In this cyber age, we need data to flow both ways. We can enhance our cybersecurity by taking both a carrot and a stick approach. We must pass robust cybersecurity legislation, but it must not compromise the rights of Canadians. We need a cyber-shield and a cyber-sword. As a vast, underpopulated nation full of remote critical infrastructure, we must be smart and creative in how we utilize every possible resource available, including enlisting white hats.

**Mr. Chris Bittle (Parliamentary Secretary to the Minister of Canadian Heritage, Lib.):** Madam Speaker, it was interesting to follow that speech, with all the conspiracy theories laid in, but I

will note the most bizarre part of it. We hear the Conservatives talk about corporate welfare a lot, but it seems the hon. member wants to give money to Bell, Rogers and Telus for doing their job. That is an interesting part of her solution to this problem, which she seems to acknowledge, even though she also suggests that members of our armed forces will do wrong by the new powers they are given.

I am wondering why the member wants to focus on giving Bell, Rogers and Telus more money to help solve the issue of cybersecurity.

**Mrs. Cheryl Gallant:** Madam Speaker, first of all, I in no way insinuated that the people who serve in the Canadian Armed Forces would do any wrong intentionally. They have to be given the proper direction, and that is why we have to get the legislation right.

Furthermore, when the Liberals talk about conspiracy theories, that only tells us they do not have an answer to the point that we are making. It is just something they throw out when they do not have an explanation for something or they cannot deny it.

[*Translation*]

**Mr. Denis Trudel (Longueuil—Saint-Hubert, BQ):** Madam Speaker, I thank my colleague for her speech, in which she mentioned something very interesting.

She said that giving too much power to the executive would undermine the work of parliamentarians. I found that quite odd because Bill C-11, which is exceptionally important for the discoverability of francophone content and for supporting francophone culture in Canada, is currently being held up in the Senate, where Conservative senators have been filibustering it for months.

Does the member think that her friends in the Senate are currently undermining the work of parliamentarians?

[*English*]

**Mrs. Cheryl Gallant:** Madam Speaker, Bill C-11 is a terrible bill. It seeks to censor, and there is no rationale to have such a bill in place. It would do no good for any freedom-loving, law-abiding citizen in this country and it must be struck down.

**Mr. Charlie Angus (Timmins—James Bay, NDP):** Madam Speaker, I am not nearly as old as I look. When I came here I was much younger, but then I had to sit through eight years of the Harper government and my hair turned white. I feel like I am one of the few who remember what actually happened then, and I watch this cultural amnesia play out day after day.

I remember Bill C-30. Stephen Harper decided that he wanted a law allowing the police to check people's phones any time they wanted for whatever reason, and the Conservatives insisted that the telecoms put in a back channel so they could spy on and listen in to ordinary Canadians. That was before we knew there were conspiracy theories, and the Conservatives have a million over there. They would think this had something to do with promoting vaccines, but this was Stephen Harper's attempt to criminalize ordinary people without a warrant.

I want to ask my hon. colleague about that. She talks about, God forbid, the Conservatives coming back. I do not know what would happen to the rest of my hair if that happened. Are they going to continue to promote the kinds of tactics that Stephen Harper used, which criminalized ordinary Canadians in their private homes by listening in to what they were talking about?

• (1630)

**Mrs. Cheryl Gallant:** Madam Speaker, the member opposite does not have to worry about a previous prime minister coming back to power, because right now what he noted is already happening. With Bill C-21, the police could come into people's homes. They are made into paper criminals just by virtue of the Liberals' declaring that certain firearms are now prohibited. It is already happening, and he does not have to wait for the best prime minister this country ever had to return.

**Mr. John Brassard (Barrie—Innisfil, CPC):** Madam Speaker, I honestly thought the member for Timmins—James Bay dyed his hair Arctic chill. I did not realize, but there is a Clairrol product that he can get at the—

**Mr. Charlie Angus:** Madam Speaker, on a point of order. I retract my previous comment. I do dye my hair so I look smarter than I am. I have been called out, so I have to admit it. I dye my hair.

**Mr. John Brassard:** Madam Speaker, the government has proven itself to fail on multiple fronts in delivering multiple projects and multiple bills.

What concern does the member have as far as delivering on this bill?

**Mrs. Cheryl Gallant:** Madam Speaker, this bill gives the government of the day boundless opportunities to abuse our privacy and to issue secret orders.

One can only imagine what would have happened during the lockdowns with secret orders going forth. For even a peaceful demonstration coming to Parliament Hill, imagine the types of punishments, accusations and jail time, not just freezing bank accounts and taking money from lawful people.

**Mr. Damien Kurek (Battle River—Crowfoot, CPC):** Madam Speaker, it is an honour to enter into debate in this place, especially when it comes to issues that are so very pressing in relation to national security and some of the challenges that our nation is facing. I would suggest the whole discussion around cybersecurity is especially relevant, because we are seeing highlighted, each and every day, a drip of new information related to foreign interference in our elections.

It highlights how important the conversation around cybersecurity is. It is often through computer and technological means that

### *Government Orders*

these malicious, foreign state actors will attack Canadian infrastructure. It is particularly relevant that I rise to debate Bill C-26, relating to the Liberals' recently introduced bill on cybersecurity, and I would like to highlight a couple of things.

The first thing is about seven years of inaction. I find it interesting, after seven years, how it was heard at the ethics committee from a whole host of experts in the field, including on cybersecurity and a whole range of issues, that the government is missing in action. It is not just about the government's inaction, but it is missing in action when it comes to some of the key issues surrounding things like cybersecurity. It has the direct consequence of creating uncertainty in terms of the technological space in the high-tech sector, which has massive opportunities.

We hear the Ottawa area referred to as silicon valley north. We have the Waterloo sector that has a significant investment in the high-tech sector. In my home province of Alberta, there is tremendous opportunity that has been brought forward through innovation, specifically in the Calgary area where we are seeing massive advancements in technology, but there is uncertainty.

Over the last seven years, the government has not taken action when it should have been providing clear direction so that industry and capital could prosper in our country. That is on the investment and economic side, but likewise, on the trust in government institutions side, we have seen an erosion of trust, such as the years-long delay on the decision regarding Huawei.

I and many Canadians, including experts in the field, as well as many within our Five Eyes security partners, were baffled about the government's delay on taking clear and decisive action against Huawei. Even though our Five Eyes, a group of countries that shares intelligence and has a strong intelligence working relationship, sees how inaction eroded the trust that these other nations had in Canada's ability to respond to cyber-concerns and threats. There is the fact that a company, a state-owned enterprise, has clear connections to a malicious foreign actor.

That delay led to incredible uncertainty in the markets and incredible costs taken on by private enterprise that simply did not have direction. Imagine all the telecoms that may have purchased significant assets of Huawei infrastructure because the government refused to provide them direction. There were years and years of inaction.

I will speak specifically about how important it is to understand the question around Canadian institutions. I would hope that members of the House take seriously the reports tabled in this place, such as from the public safety committee, which in the second session of the last Parliament I had the honour of sitting on. There is a whole host of studies that have been done related to this.

*Government Orders*

• (1635)

Then there are the CSIS reports tabled in this place containing some astounding revelations about foreign state actors and their incursions and attempts to erode trust in Canadian institutions. Specifically, there was a CSE report for 2021, which I believe is the most recent one tabled, that talks about three to five billion malicious incursions in our federal institutions a day via cyber-means. That is an astounding number and does not include the incursions that would be hacks against individuals or corporations. That is simply federal government institutions. That is three to five billion a day.

There are NSICOP reports as well. The RCMP, military intelligence and a whole host of agencies are hard at work on many of these things. It highlights how absolutely important cybersecurity is.

I find it interesting, because over the last seven years the Liberals have talked tough about many things but have delivered action on very few. Huawei is a great example. Cybersecurity is another. We see a host of other concerns that would veer off the topic of this discussion, so I will make sure that I keep directly focused on Bill C-26 today. The Liberal government is very good at announcing things, but the follow-through often leaves much to be desired.

We see Bill C-26 before us today. There is no question that action is needed. I am thankful we have the opportunity to be able to debate the substance of this bill in this place. I know the hard work that will be done, certainly by Conservatives though I cannot speak for the other parties, at committee to attempt to fix some of the concerns that have been highlighted, and certainly have been highlighted by a number of my colleagues.

The reality is Canadians, more and more, depend on technology. We saw examples, when there are issues with that technology, of the massive economic implications and disruptions that take place across our country. We saw that with the Rogers outage that took place in July. Most Canadians would not have realized that the debit card system, one of the foundational elements of our financial system, was dependent upon the Rogers network. For a number of days, having disruptions in that space had significant economic implications. It just speaks to one of the many ways Canadians depend on technology.

We saw an example in the United States, so not directly in Canada, when the Colonial Pipeline faced a ransomware attack. A major energy pipeline on the eastern seaboard of the United States was shut down through a cyber ransomware attack. It caused massive disruptions.

Another Canadian example that has been reported in talking to some in the sector was Bombardier recreational products. The Quebec company is under a cyber-lockdown because of hostile actions. There are numerous other examples, whether in the federal government or in the provinces, where this has been faced.

There are a number of concerns related to what needs to take place in this bill to ensure that we get it right. It needs to align with the actions that have taken place in our Five Eyes allies. We need to ensure that the civil liberties question is clearly answered.

We have seen the government not take concern over the rights of Canadians to see their rights protected, their freedom of speech, whether that is Bill C-11. I know other parties support this backdoor censorship bill, but these are significant concerns. Canadians have a right to question whether or not there would be a civil liberties impact, to make sure there would not be opportunity for backdoor surveillance, and to ensure there would be appropriate safeguards in place and not give too much power to politicians and bureaucrats as to what the actions of government would be.

As was stated by one stakeholder in writing about this, the lack of guardrails to constrain abuse is very concerning. In Bill C-26, there is vague language. Whenever there is vague language in legislation, it leaves it open to interpretation. We have seen how, in the Emergencies Act discussion and debate, the government created its own definition of some of the things that I would suggest were fairly clearly defined in legislation. We have to make sure it is airtight.

Massive power would be given to the Minister of Industry in relation to many of the measures contained in this bill.

• (1640)

I look forward to taking questions. It is absolutely key we get this right, so Canadians can in fact be protected and have confidence in their cybersecurity regime.

**Mr. Mark Gerretsen (Parliamentary Secretary to the Leader of the Government in the House of Commons (Senate), Lib.):** Madam Speaker, I heard the member talk about Huawei quite a bit. I could not help but reflect on the fact that the former contender to the current leader of the Conservative Party was actually on the legal team to support Huawei through its initiative to try to get onto the 5G network in Canada. I cannot help but wonder why on earth, if the Conservatives are so against Huawei and treat this threat so seriously, the Conservative Party of Canada would green-light—

**The Assistant Deputy Speaker (Mrs. Alexandra Mendès):** The hon. member may know it is not the business of the House to deal with leadership issues of the different parties. I understand what the hon. member is trying to say, but try to keep it to the legislation.

**Mr. Mark Gerretsen:** Madam Speaker, Jean Charest was a lawyer for Huawei. The member brought up Huawei. Jean Charest is a well-known Conservative who ran in the leadership. Why would they have allowed Jean Charest to run in the leadership had that been the case?

**Mr. Damien Kurek:** Madam Speaker, I will suggest this has direct relevance to the debate at hand. It has direct relevance because the victor of that race was not the individual the member referred to, but rather the member for Carleton, who I was proud to support and who will be so pleased to ensure we, as a majority Conservative government after a future election, have the opportunity to get things right and get this country back on track.



*Government Orders**[Translation]*

**Mrs. Caroline Desbiens (Beauport—Côte-de-Beaupré—Île d'Orléans—Charlevoix, BQ):** Madam Speaker, I thank my colleague for his speech.

I would like my colleague to reassure people who are watching, people in our communities who are worried about a device that is in their hands for much of the day. These people live with this device in their home. They use this device to share anecdotes, conversations and occasionally intimate secrets, believing that it all belongs exclusively to them.

Since our colleague does not seem interested in better control of cyber-attacks, how does he expect to reassure the public without moving toward tighter cybersecurity?

• (1645)

*[English]*

**Mr. Damien Kurek:** Madam Speaker, I cannot hold up my cell-phone, but what is absolutely key to the whole conversation we are having is the fact that all of us in this place carry an incredibly powerful computing device that only a few years ago would have been something we would not have seen even in the most futuristic sci-fi novels and movies. The space in which we are discussing cybersecurity has evolved so rapidly.

Specifically to the question the member asked regarding privacy, it is a very important one. It is one that, as a member of the Standing Committee on Access to Information, Privacy and Ethics, we need to make sure the legislation we have in this country, including privacy legislation both on the application of government and the privacy of all Canadians in terms of corporations and that whole space, reflects the modern realities. In many cases, decades old legislation needs to be updated to reflect the realities of today.

**Ms. Bonita Zarrillo (Port Moody—Coquitlam, NDP):** Madam Speaker, when we talk about the updated realities of today, persons with disabilities rely heavily on these technologies and this access. If I think about persons with disabilities who rely on technologies for everyday barrier reduction interactions in their lives, how can their rights to access be protected?

**Mr. Damien Kurek:** Madam Speaker, the right to access is absolutely key. We have seen some incredible technological advancements that have helped those who face disabilities in a wide variety of things. Outside of the context of what Bill C-26 directly addresses in terms of cybersecurity, there is a particular connection, because if we do not have things like secure networks, if we do not ensure that our telecoms have consistent and stable networks that we can trust as a country, then access becomes a real issue. Malicious foreign-state actors could take advantage of that, which would disadvantage all Canadians, but specifically those who depend on technology to mitigate things like disabilities.

*[Translation]*

**The Assistant Deputy Speaker (Mrs. Alexandra Mendès):** Order. It is my duty, pursuant to Standing Order 38, to inform the House that the questions to be raised tonight at the time of adjournment are as follows: the hon. member for Bow River, Taxation; the hon. member for South Okanagan—West Kootenay, Post-Secondary Education.

*[English]*

**Mrs. Sherry Romanado (Longueuil—Charles-LeMoine, Lib.):** Madam Speaker, I will be sharing my time with the fantastic member for Lac-Saint-Louis.

It is with great pleasure that I rise to discuss Bill C-26, an act respecting cybersecurity. I will address elements in the legislation that deal with securing Canada's telecommunications system.

As Canadians rely more and more on digital communications, it is critical that our telecommunications system be secure. Let me assure this House and in listening to the debate today I think we all agree that the issue of cybersecurity is of utmost importance. The Government of Canada takes the security of this system seriously, which is why we conducted a review of 5G technology and the associated security and economic considerations.

It is clear that 5G technology holds lots of promise for Canadians for advanced telemedicine, connected and autonomous vehicles, smart cities, cleaner energy, precision agriculture, smart mining, and a lot more. Our security review also made clear that 5G technology will introduce new security concerns that malicious actors could exploit. Hostile actors have long sought and will continue to seek to exploit vulnerabilities in our telecommunications system.

• (1650)

*[Translation]*

CSIS, the Canadian Security and Intelligence Service, acknowledged this in its most recent publicly available annual report. The report states:

Canada remains a target for malicious cyber-enabled espionage, sabotage, foreign influence, and terrorism related activities, which pose significant threats to Canada's national security, its interests and its economic stability.

The report states, "Cyber actors conduct malicious activities to advance their political, economic, military, security, and ideological interests. They seek to compromise government and private sector computer systems by manipulating their users or exploiting security vulnerabilities".

*[English]*

The CSIS report also highlighted the increasing cyber-threat that ransomware poses. The Communications Security Establishment has similarly raised concerns about threats like ransomware in recent public threat assessments. We have seen how such attacks by criminal actors threaten to publish a victim's data or block access to it unless a ransom is paid. However, it is not just cybercriminals doing this. CSIS warned that state actors are increasingly using these tactics, often through proxies, to advance their objectives and evade attribution.

*Government Orders*

To be sure, Canadians, industry and government have, to this point, worked hard to defend our telecom system, but we must always be on the alert, always guarding against the next attacks. This has become more important as people now are often working remotely from home office environments.

[*Translation*]

5G technology is adding to these challenges. In 5G systems, sensitive functions will become increasingly decentralized in order to boost speeds when required.

Cell towers are a familiar sight in our communities and along our highways. The 5G networks will add many smaller access points to increase speeds. As well, the number of devices that the 5G network will connect will also grow exponentially.

[*English*]

Given the greater interconnectedness and interdependence of 5G networks, a breach in this environment could have a more significant impact on the safety of Canadians than with older technology. Bad actors could have more of an impact on our critical infrastructure than before.

The security review we conducted found that in order for Canada to reap the benefits of 5G, the government needs to be properly equipped to promote the security of the telecommunications system. We need to be able to adapt to the changing technological and threat environment. For these reasons, we are proposing amendments to the Telecommunications Act. The amendments will ensure that the security of our telecommunications system remains an overriding objective.

[*Translation*]

This bill will expand the list of objectives set out in section 7 of the Telecommunications Act. It will add the words “to promote the security of the Canadian telecommunications system”.

It is important for those words to be in the act.

[*English*]

It means government will be able to exercise its powers under the legislation for the purposes of securing Canada's telecommunications system.

The amendments also include authorities to prohibit Canadian telecommunications service providers from using products and services from high-risk suppliers in 5G and 4G networks if deemed necessary and after consultation with telecommunications service providers and other stakeholders.

It would also give the government the authority to require telecommunications service providers to take any other actions to promote the security of the telecom networks upon which all critical infrastructure sectors depend.

We have listened to our security experts; we have listened to Canadians; we have listened to our allies and we are following the right path. We will ensure that our networks and our economy are kept secure. A safe and secure cyberspace is important for Canada's competitiveness, economic stability and long-term prosperity.

It is clear that the telecommunications infrastructure has become increasingly essential. It must be secure and it must be resilient. Telecommunications presents an economic opportunity, one that grows our economy and creates jobs. The amendments to the Telecommunications Act accompany the proposed critical cyber systems protection act. This bill will improve the ability of designated organizations to prepare, prevent, respond to and recover from all types of cyber-incidents, including ransomware. It will designate telecommunications as a vital service. Together, this legislative package will strengthen our ability to defend the telecommunications and other critical sectors, such as finance, energy and transportation, that Canadians rely on every single day.

The legislation before us today fits within the Government of Canada's telecommunications reliability agenda. Under this agenda we intend to promote robust networks and systems, strengthen accountability and coordinate planning and preparedness.

• (1655)

[*Translation*]

Canadians depend on telecommunications services in all aspects of their lives, and the security and reliability of our networks has never been more crucial. These services are fundamental to the safety, prosperity and well-being of Canadians.

[*English*]

We will work tirelessly to keep Canadians safe and able to communicate securely. This legislation is an important tool to enable us to do that. I look forward to working with members in this House to getting this right and making sure that our telecommunications system is as strong as it can be.

**Mr. Philip Lawrence (Northumberland—Peterborough South, CPC):** Madam Speaker, in earnest, the government has had significant failures when it comes to procurement. I would point to shipbuilding, where we are years behind. It has also had significant failures with respect to IT. I point to the Phoenix pay system.

Given these failures, what has the government learned, and how can the Canadian public believe the government will be able to deliver on this legislation?

**Mrs. Sherry Romanado:** Madam Speaker, I had the opportunity to sit on the defence committee during my first mandate, and I had the opportunity to work closely with the then minister of national defence on “Strong, Secure, Engaged”. We are going to be reviewing “Strong, Secure, Engaged” in terms of our defence spending, including what we are going to be doing on procurement.

A lot of things have changed in the last seven years in terms of defence, like what is happening across the way in terms of Ukraine and Russia, cyber and how significantly things have changed. We absolutely need to invest in cyber and make sure we get our defence procurement projects completed.

*Government Orders*

[*Translation*]

**Mr. Denis Trudel (Longueuil—Saint-Hubert, BQ):** Madam Speaker, I thank my colleague for her speech.

There are people from the Fédération des communautés francophones et acadienne du Canada on the Hill today. They met with the Minister of Official Languages. The House is working on Bill C-13 because we know that the French language is declining in Quebec and Canada, so efforts to promote French must be made.

My colleague represents a riding in which 80% of the population speaks French as their mother tongue. She just delivered a speech that was about 80% in English. Does that not make her a bit uncomfortable? Does she not think that a clearer message could be sent here in the House?

Her government could also send a clearer message by giving speeches more openly in French.

**The Assistant Deputy Speaker (Mrs. Alexandra Mendès):** The hon. member's question is a little off topic.

I will nevertheless give the hon. member for Longueuil—Charles-LeMoyne a chance to respond.

• (1700)

**Mrs. Sherry Romanado:** Madam Speaker, if the member wants to ask a question about the subject matter of the bill we are debating, I would be pleased to answer.

With respect to language, I speak both official languages and am very proud to do so.

[*English*]

**Mr. Charlie Angus (Timmins—James Bay, NDP):** Madam Speaker, the question of Canada's ability to deal with our situation in an increasingly unstable world raises serious questions about priorities. For example, we are years behind on the frigates that are supposed to be brought forward by the navy. The cost overruns are staggering, yet we have just seen in Ukraine that the Russian flagship, *Admiral Makarov*, was taken out by drones.

Do we need to completely reassess our thinking? This is the 21st century. We are investing, often, in 20th-century solutions in a world of warfare, cyberterrorism and cyber-power that is completely transforming the nature of warfare and democracy's ability to defend itself.

Does my colleague think we need to do a larger rethink across the board in terms of our strategies and our ability to defend ourselves?

**Mrs. Sherry Romanado:** Madam Speaker, I want to thank the member for that question, because that is one area of our domain awareness that we have not focused on a lot. When we think about the air force, army or navy, we usually talk about those three domains, but we do not talk a lot about cyber. We know that is the fourth domain that we need to focus on.

In terms of our NORAD modernization, I know cyber is top of mind in working with our Five Eyes partners and other partners. We need that modernization to take place so we can make sure this fourth element of our national defence is also included.

**Mr. Mike Morrice (Kitchener Centre, GP):** Madam Speaker, I know the member for Longueuil—Charles-LeMoyne has heard some of the debate today, not just from other MPs but from civil society organizations that have raised concerns with respect to secrecy as it relates to addressing cybersecurity.

I am curious to hear her reflections on potential improvements she thinks could be made to the bill in order to better balance the need to improve cybersecurity while holding on to accountability and transparency.

**Mrs. Sherry Romanado:** Madam Speaker, unfortunately I do not sit on the public safety committee, so I will not be the person debating it when it eventually gets to committee, but obviously there are opportunities for improvement in any piece of legislation. I look forward to seeing the recommendations that might come from our colleagues in the House when it gets to committee.

[*Translation*]

**Mr. Francis Scarpaleggia (Lac-Saint-Louis, Lib.):** Madam Speaker, it is an honour for me to rise at second reading stage of Bill C-26, an act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.

When we consider the opportunities and challenges before us in this area, we see that the theme of collaboration underpins all that we do. Take, for example, the prevalence of cybercrime in an increasingly online world, improving cyber-defence posture in an unstable global environment, deep thinking about what the future holds in a world where innovation and change are exponential, a critical look at whether our policies and laws are up to the task, and the protection of content and intellectual property as data becomes one of the world's most precious resources.

In Canada, being online and connected is essential. Now more than ever, Canadians rely on the Internet for their daily lives. It is about more than just conducting business and paying bills. It is also about staying connected with loved ones across the country and around the world. We should be able to do all these activities safely and securely.

I would like to offer a few words about what we are doing here in Canada to get that balance right. I would like to reinforce the importance of our commitment to protecting the cyber systems that underpin our critical infrastructure.

The emergence of new technologies such as 5G is one clear reason we need to redouble our efforts. Think about our increased reliance on technology in light of the COVID-19 pandemic. Think about international tensions amidst Russia's unprovoked and unjustified invasion of Ukraine, with threats ranging from supply chain disruptions to state and non-state malicious cyber-activity.

*Government Orders*

Through all of these remarkable events, the government has been working tirelessly to keep Canadians safe. We recognize that, now more than ever before, secure and reliable connectivity is a necessity for our daily lives and our collective safety and security. It underpins the delivery of critical services, such as energy production, financial transactions, safe transportation and emergency communications.

As part of his mandate, bestowed by the Prime Minister, the Minister of Public Safety is seized with the opportunity and the challenge of developing a renewed national cybersecurity strategy. We need to make sure we articulate Canada's long-term plan to protect our national security and economy, deter cyber-threat actors, and promote norms-based international behaviour in cyberspace.

The Government of Canada is working to enhance the cybersecurity of the country's critical infrastructure. The work to identify cyber-threats and vulnerabilities, and to respond to cyber-incidents, is ongoing. Unfortunately, we have seen that malicious actors continue to attempt to take advantage of the current environment to exploit certain sectors.

However, we are not starting from scratch in our fight against this threat. Since 2018, the Government of Canada has invested a total of approximately \$2.6 billion in cybersecurity. Through the national cyber security strategy, the Government of Canada is taking decisive action to strengthen Canada's defence, preparedness and enforcement against cyber-threats.

The strategy was paired with the largest investment in cybersecurity ever made by the Government of Canada, totalling nearly \$800 million in the 2018 and 2019 federal budgets. In the 2021 budget, the government allocated an additional \$791 million to improve and defend cyber-networks, enhance data collection and protect taxpayer information.

● (1705)

In the 2022 budget, another \$852.9 million was committed to enhance the Communications Security Establishment, or CSE, and its ability to conduct cyber-operations, make critical government systems more resilient, and prevent and respond to cyber-incidents on critical infrastructure.

Under the strategy, two flagship organizations were established. One is the Canadian Centre for Cyber Security, under CSE, and the other is the National Cybercrime Coordination Centre, or NC3, under the RCMP.

The Canadian Centre for Cyber Security is a single, unified team of government cybersecurity technical experts. The centre is the definitive source of technical advice, guidance, services, messaging and support on cybersecurity operational matters for government, critical infrastructure owners and operators, the private sector and the Canadian public.

The NC3 coordinates Canadian police operations against cyber-criminals and established a national mechanism for Canadians and businesses to report cybercrime to police.

Public Safety Canada's Canadian cybersecurity tool also helps owners and operators of Canada's critical infrastructure to evaluate their cyber-maturity against established benchmarks and by peer

comparison. It offers concrete guidance on how they can become more cyber-resilient.

Public Safety Canada also coordinates and delivers cybersecurity exercises for the critical infrastructure community to test and develop capabilities to respond to and recover from malicious cyber-activities. More broadly, the department, as the federal lead on cybersecurity policy, promotes communication and collaboration to raise awareness of cyber-threats and risks, including with our international partners.

Public Safety Canada works closely with CSE's Canadian Centre for Cyber Security to enhance the resilience of critical infrastructure in Canada. The Canadian Centre for Cyber Security shares valuable cyber-threat information with Canadian critical infrastructure owners and operators, in addition to providing public advisories.

Today, I am very proud to say that we can start debating a new bill to further strengthen what we have built. Today we are starting the debate on Bill C-26, an act respecting cyber security. The objective of this bill is twofold.

First, it would amend the Telecommunications Act to add security as a policy objective, bringing the telecommunications sector in line with other critical infrastructure sectors. This would allow the government, if necessary, to mandate any action necessary to secure Canada's telecommunications system, including its 5G networks. This includes authority to prohibit Canadian telecommunications service providers from using products and services from high-risk suppliers.

Second, it introduces the new critical cyber systems protection act. This new act will require designated operators in the federally regulated sectors of finance, telecommunications, energy and transportation to take specific actions to protect their critical cyber systems, and it will also support organizations' ability to prevent and recover from a wide range of malicious cyber-activities, including electronic espionage and ransomware. Cyber-incidents involving a certain threshold will be required to be reported.

The bill will also give the government a new tool allowing it to take action in response to threats and vulnerabilities with respect to—

● (1710)

**The Assistant Deputy Speaker (Mrs. Alexandra Mendès):** Order. The hon. member's time has expired.

The hon. member for Drummond.

**Mr. Martin Champoux (Drummond, BQ):** Madam Speaker, I want to congratulate my colleague from Lac-Saint-Louis on his speech. He obviously has an excellent grasp of the file.

I put this question to another colleague earlier, after a speech, and it is something that really concerns me. I am asking it again because I do not know if the member was here earlier.

We cannot begin to imagine how organized hackers are. They have such a big head start that it will be hard to catch up to them, even if we invest all the energy and knowledge we can in our systems to protect ourselves against cyber-attacks. We have seen companies like Desjardins and Bombardier fall victim to these hackers, who demand endless ransoms. How many other companies have fallen victim to these attacks without us even hearing about it?

My question is this. Has Canada been too slow to act? It took Canada a long time to decide Huawei's fate, for example. Does the fact that the government seems to have dragged its feet before finally tabling a cybersecurity plan that appears to have some teeth not mean that we will always be one step behind those countries and organizations that are attacking the computer systems of businesses and governments around the world?

**Mr. Francis Scarpaleggia:** Madam Speaker, I know that the Huawei case has been studied extensively with the involvement of our security agencies. I would like to think that the government and security agencies have learned a great deal. They have learned lessons that they can apply in the future to better protect Canadian businesses and critical infrastructure.

In terms of catching up, yes, technology moves so fast that often governments and society have to react, but it is better to react than to do nothing.

• (1715)

**Mr. Richard Lehoux (Beauce, CPC):** Madam Speaker, I thank my colleague for his speech.

I have a question about publicly owned corporations like Hydro-Québec. How will the bill provide a framework for this, while still allowing companies like Hydro-Québec to be proactive about cybersecurity? How will the bill ensure there is no interference? Will there be support? I would like to hear my colleague's point of view on this issue.

**Mr. Francis Scarpaleggia:** Madam Speaker, I dare to believe and hope that a publicly owned corporation as big as Hydro-Québec has the resources to protect itself properly. Obviously, it provides a critical service. I think I said that in my speech. We hope that this bill will also serve as a model for other levels of government.

I think that, just like protecting the environment, cybersecurity is a team effort. We have to work with partners in other governments to come up with a solution that is watertight, well aligned and effective.

[English]

**Ms. Heather McPherson (Edmonton Strathcona, NDP):** Madam Speaker, my colleague and I spent a lot of the day together today. We had an excellent event this morning, which he organized, so I would like to thank the member for Lac-Saint-Louis for that.

There is one question I do have with regard to the bill. It has been written in such a way that secret orders could be issued, and they could be kept from being publicized or published in the

### Government Orders

Gazette. Why was that choice made? Why was the decision made to have that level of secrecy in the legislation?

**Mr. Francis Scarpaleggia:** Madam Speaker, I would also like to thank the member for taking part in a panel in front of about 40 students from the Max Bell School of Public Policy this morning. It was wonderful to have her perspective as a westerner, and as a parliamentarian generally.

I would imagine that, when we are dealing with matters of national security in cybersecurity and systems that are key to our well-being, there might be a need in certain cases to be a little more circumspect. I would hope, believe and expect, because every bill that is introduced to the House has to go through a charter analysis, that any such measure the member refers to would pass the test of the charter.

[Translation]

**Mr. Simon-Pierre Savard-Tremblay (Saint-Hyacinthe—Bagot, BQ):** Madam Speaker, I will give my speech in French. I will be sharing my time with my esteemed colleague from Trois-Rivières, who will no doubt be able to give a more relevant speech than me. I am pleased to share my time with him.

Ottawa is finally proposing a law to deal with the issue of cybersecurity. We are pleased to see that the government is finally addressing this issue. I will not say that it is too little, too late, but I will say that we waited a long time for this.

The purpose of the bill is to force Internet service providers to adopt better practices, something on which we all agree. We commend the government for that.

However, why is Ottawa always in reaction mode? We have been talking about the 5G network and Huawei for years. Hydro-Québec has been experiencing cyber-attacks on a daily basis for years. We have known for years about the rise of China, a country that is interfering more and more. In short, we have known for years that Canada is extremely vulnerable and that it is basically a sieve in terms of cybersecurity.

How can it be that, in this postnational system, everything happens reactively, not proactively? That is all I am going to say about that, because there is no changing the fundamentals of a country that is impervious to reform. Instead, we are going to get out. I just wanted to put that out there.

We support the bill in principle, but there are some grey areas that need clarification. That is what committees are for. The legislation is essentially a regulatory framework that, first and foremost, enables the government to make regulations to ensure the security of critical cyber systems. We have to look at the impact this bill could have on Quebec, especially Hydro-Québec, because it lists interprovincial power line systems under vital services and vital systems. The committee will also have to look at whether the vast regulatory powers provided for in the bill are justified and ensure that they do not needlessly circumvent Parliament.

### *Government Orders*

The threats that weigh on cybersecurity are likely to increase. They are the future, but they are also very much part of our present. In fact, a number of experts on the matter in Quebec talk to us about it. There is someone I really liked to watch when he was on television, although he stopped appearing when he became a deputy minister. I am talking about one of my constituents, Steve Waterhouse, who is always very interesting to listen to. His work helped raise our awareness and raise public awareness. He is from Sainte-Madeleine, which is in the incredible riding of Saint-Hyacinthe—Bagot.

Cyber-threats are already a part of our daily lives. Hydro-Québec is attacked every day by what are referred to as denial of service attacks. These are less sophisticated cyber-attacks and are the easiest ones to deal with, but they can cause major disruptions.

Look at Aluminerie Alouette, on the North Shore, which was the victim of a major cyber-attack that led to a serious outage. A Russian group claimed responsibility. Last summer, during the Rogers outage, which also had a serious impact on debit card transactions, a cyber-attack was the first thing that came to mind.

The objective of the bill is to mitigate the risks upstream. The legislation could certainly help Quebeckers, for example by imposing certain standards on Internet service providers, such as the obligation to avoid using products from suspect companies like Huawei.

In 2020, Parliament adopted a motion to force the government to make a decision about Huawei and Chinese interference in general. Recently, Ottawa finally blocked Huawei after years of dithering. What a waste of time. As Proust wrote, we are in search of lost time.

Madam Speaker, please tell my colleagues that they can let me know if I am disturbing them. I would not want to prevent them from having their conversations.

• (1720)

**The Assistant Deputy Speaker (Mrs. Carol Hughes):** I ask that members who wish to have conversations leave the chamber to do so.

The hon. member for Saint-Hyacinthe—Bagot may continue.

**Mr. Simon-Pierre Savard-Tremblay:** Thank you, Madam Speaker. I see that they are no more interested in what you have to say than what I was saying, so I do not take it personally.

The 5G network is a new communications technology with bandwidth that is 10 to 100 times greater than that of current networks. The technology stands out for more than just its speed. It stands out for its extremely low latency, which is the time it takes for one computer to communicate with another and receive a response.

This opens the door to many possibilities in different areas, but to achieve performance, 5G uses a multitude of pathways. To simplify, let us say that something that is sent from Montreal to a computer in Paris could have a portion pass through New York, another through London, another through Barcelona, and so forth. This makes the technology particularly vulnerable because it becomes difficult to track the path that the data takes.

Huawei has already been implicated in the scandal involving China spying on the African Union headquarters. In 2012, China offered the African Union a fully equipped ultramodern building. Africa is known to be an extremely important location for Chinese investment. China supplied everything: networks, computers and telecommunications systems. After a few years of operation, in 2017, African computer scientists realized that the servers were sending out huge amounts of data at night, when nobody was working in the building. They discovered that the data was going to servers in China, which was spying on all staff and political leaders. Huawei was the main supplier of the network infrastructure. Microphones were also found in the walls and tables.

China passed a new national intelligence law in 2017. One thing is clearly set out in their law. All Chinese companies must absolutely participate in China's intelligence efforts. It is a form of economic and commercial patriotism, and we could also add digital. In other words, all the private players are being mobilized to say that they are going to participate in the construction of the great digital wall of China. This includes military intelligence and civilian intelligence. For instance, a company can be called upon to spy on behalf of another Chinese company in order to place China in an advantageous position on the world stage.

At this very moment, a genomics company called BGI, which works with genes, is still supplying medical equipment to Canadian hospitals. Its machines collect data, and only the company's technicians are authorized to carry out the monthly maintenance. They are the only ones with access. It turns out that this company has close ties to the Chinese military.

There is also Alibaba, a publicly traded Chinese company similar to Amazon that was founded by businessman Jack Ma. It derives its income from online activities, including a public market designed to facilitate transactions between businesses, payment and retail sales platforms, a shopping search engine and cloud computing services.

Another example is Tencent, a company founded in 1998 that specializes in Internet and mobility services and online advertising. Tencent's services include social networks, web portals, e-commerce and multiplayer online games. Tencent manages and operates well-known services, such as messaging services Tencent QQ and WeChat, and the qq.com web portal.

*Government Orders*

Today, China is the champion of data collection. This rising power requires new practices, new barriers and new ways of doing things. We should not think that the U.S. does not have their own giants that collect data, but just in China there are 800 million Internet users. That is more than the U.S. and India put together and one-quarter of all Internet users in the world. This number of users will give public and private Chinese actors, which have a close relationship, access to large sources of data that they can mine at will.

China has built a formidable digital system. There is a reason why it is constantly increasing its data storage. There is no doubt that the issue of cybersecurity is at the centre of the current international economic war that is engulfing an increasingly multipolar world. We need to acknowledge this. We need to act.

• (1725)

We support this bill because it is well-intentioned, but we have to find a way to put some meat on the bones.

[*English*]

**Mr. Kevin Lamoureux (Parliamentary Secretary to the Leader of the Government in the House of Commons, Lib.):** Madam Speaker, I appreciate very much the Bloc's tentative support of the legislation to go to committee, recognizing that this legislation empowers the minister to take direct, specific actions to protect Canadians and businesses. As the member pointed out so accurately, there is a very real cyber-threat out there. It also ensures that there can be financial penalties.

Would the member not agree that this is just one step? We have had literally tens of millions of dollars invested in cyber-threats over the years. We have had all sorts of group discussions and meetings to make sure that the government is keeping up. There are a number of stakeholders with the responsibility of fighting cyber-threats today.

[*Translation*]

**Mr. Simon-Pierre Savard-Tremblay:** Madam Speaker, should that not just be one step? The answer is: of course it should.

I believe we said we are in favour. We are not even sure that this step will be enough, but it is a step in the right direction, and that is why we support it. It is great that there is going to be money for this, but now the real work starts.

I feel there are a lot of areas to consider. We will have to look at industrial espionage and economic espionage too. Regimes have all kinds of legal and digital techniques for acquiring competitors' data and trade secrets.

• (1730)

[*English*]

**Mr. Ziad Aboultaif (Edmonton Manning, CPC):** Madam Speaker, what does the member propose for a solution? What are the immediate steps needed to be taken to deal with the pressing issue of cybersecurity attacks we are facing in the country?

[*Translation*]

**Mr. Simon-Pierre Savard-Tremblay:** Madam Speaker, Bill C-26 does contain some good solutions and some interesting elements.

The only thing is, we will have to look at the details and see what is next. Are we giving the minister too much power? At the same time, we may have to think twice about giving more power to the minister at the expense of Parliament when we are not sure whether the minister will fulfill his commitments. There have been promises followed by waffling in the past. There are definitely things that need to be looked at, yes, but at least this bill is motivated by good intentions. For that alone, it deserves to be supported at this stage.

[*English*]

**Ms. Heather McPherson (Edmonton Strathcona, NDP):** Madam Speaker, my colleague's intervention today was very interesting. He seems to know the subject very well. Looking at this legislation, we have been talking about how it has been a long-time coming, and how we would have liked to have seen this legislation before us sooner.

I wonder if, as he studied this bill, he had an opportunity to look at legislation from other countries, and if there is legislation from other countries that we could be emulating and looking at as we try to improve this bill. After second reading, I think all parties want to make sure this bill improves.

[*Translation*]

**Mr. Simon-Pierre Savard-Tremblay:** Madam Speaker, as I said at the beginning, I was a bit critical. Unfortunately, in this country, in this Parliament and in this postnational system, it is clear that there is much hemming and hawing in far too many files.

Take a look at the general political culture of other countries like the United States. It did not take them long. Consider the example of Huawei; it took no time at all. They looked at it, concluded that it was preposterous and they put an end to it.

Why has it taken Canada years? This is still something to keep an eye on.

The European Union is also starting to take action. It is starting to move on this front by setting up institutes to monitor interference, the extraterritoriality of certain practices, and so on. There are certainly practices that should be monitored.

**Mr. René Villemure (Trois-Rivières, BQ):** Madam Speaker, I thank my colleague from Saint-Hyacinthe—Bagot, who said he wished that we could talk a bit about what is being done proactively, and that is what I intend to do.

As members know, we cannot discover new worlds until we have the courage to not see the shore. Those who know me know that I would rather talk about the “why” than the “how”. I like to clearly define what we are talking about.

Let us start with the word “security”. Security is an absence of worry. It is peace of mind, a form of safety. It is rather easy to define.

### *Government Orders*

Now, what is the definition of the prefix “cyber”? Cybersecurity is a word that is used in all kinds of ways. We want to combat cybercrime with cybersecurity. We want to prevent cyberstalking. Sometimes it can be confusing. What is the meaning of the prefix “cyber” that is used everywhere?

The origin of the word will help us to understand it. It was coined after the Second World War by an American researcher named Norbert Wiener. This brilliant mathematician was hired by the Massachusetts Institute of Technology, or MIT, to work on a research project on new types of weapons. More specifically, he was asked to develop missiles that could take down V-1s and V-2s, the unmanned German aircraft filled with explosives that were causing so much damage in England.

To that end, Professor Wiener had to model the behaviour of a pilot who knew he was being chased in order to better understand the decision-making mechanisms of humans in general. We will use the term human so as not to offend anyone. In 1948, Norbert Wiener named this field of research “cybernetics”, a new area of science that studies the mastery of machines. He was inspired by the Greek term *kubernao*, which means to pilot and from which the terms “government” and “governance” are also derived. It means “to steer”.

In 1949, Wiener's book was deemed one of the most important works of the 20th century. The New York Times praised it and predicted that cybernetics would be a leading branch of science in the future, which has come to pass. This book still contributes practical knowledge to today's world because one of the main concepts underlying this new theory is that of regulation. That is what we are discussing today.

With the Internet, everything becomes cyber, but the societal challenge is huge because in cyberspace we no longer know what is the cause and what is the effect. We are no longer certain who governs and who is governed. We no longer strive to determine if the chicken came before the egg or if the egg came before the chicken. In cyberspace, we cannot make sense of the chickens and the eggs.

When we talk about the Internet, we are talking about space and time. Space and time are concepts that, throughout history, have allowed us to place and understand ourselves. In philosophy it is said that nothing exists without space and time because everything is always somewhere in space and in a given moment, it is situated in time.

However, the Internet is everywhere and nowhere. In fact, when we talk about the web we picture an entanglement of threads without a centre. Humans, with their neurolinguistics, have a hard time placing themselves when there is no centre. We are always looking for the end. The Internet does not have one. In space, there is no centre and time is eternal. The Internet is always, never, and in perpetuity. It is therefore very hard to understand and associate with the cyber point of view.

Bill C-26 is divided in two parts. In the first part, it says that it seeks to reinforce the security of the Canadian telecommunications system. Then there are indications of how it will change this and how it will change that. In the second, it says it will create the new

critical cyber systems protection act to do this or that. I am summarizing the bill.

I noticed when I read Bill C-26 that there is a lot of “how” and not a lot of “why”. What is the “why” behind Bill C-26? In my opinion, there is just one reason why and that is to ensure that citizens can trust in the mechanism that protects them in the area of cybernetics and cyberspace.

Trust is complicated because it is not something that is easily granted. I will use the example given by my colleague from Saint-Hyacinthe—Bagot. I know him and he is conspicuous in his absence, even though I am not allowed to say that. I do not have eyes in the back of my head.

● (1735)

It is pretty easy to build up trust between two individuals. However, trusting an entity, a company or a government is harder. Trust means having peace of mind, without needing supporting evidence. It is difficult to achieve in the public sphere. It is essential, however, and I think that is what Bill C-26 seeks to accomplish.

Trust begins with education and insight. Since this has been explored in speeches throughout the day, I will not dwell on it, but the geopolitical world is changing these days, and the balance of power is shifting. In addition, it is hard to know where the centre is, as I explained a little earlier.

The Canadian government's foreign policy is vague at best. It took years for the government to acknowledge that there was a problem with Huawei. It was the only Five Eyes nation that did not see the inevitable, that did not see the evidence right under its nose.

I am talking about education, but the bill does not contain any provisions for education in cybersecurity. I am talking about education in terms of privacy and facial recognition. Education would help people avoid the temptation to commit the act that we are trying to prohibit here.

We also know that we are stronger together. It is interesting to see who has already thought about these issues. One of our colleagues said that other institutions have thought about this. Yes, there is a concept known as cyber diplomacy, which involves co-operation and dialogue between nations. Moreover, to answer a question that has not been asked, which is the nature of philosophy, the Council of Europe could offer some very interesting answers and solutions in this matter.

This brings me to another question. Despite the many measures, there are quite a few things I do not see in this bill. I do not see measures that would prevent our devices from being taken over by malware, for example, or by a foreign power. Device takeover is something we recently studied at the Standing Committee on Access to Information, Privacy and Ethics. It is not the stuff of science fiction; it is actually happening now.

Also, I do not see how this bill prevents intellectual property infringement. I could name 200 other things I do not see in this bill, but I will mention just one more. I do not see how we are going to regulate what is known as the dark web. However, the bill names six organizations that will have the power to act as regulators.



However, I would like to ask the following question: Do these organizations have the necessary knowledge to do that? It is not always clear. In previous bills on other subjects, we were told, for example, about the CRTC, which was responsible for implementing some provisions. We saw that the CRTC was an outdated organization. The organizations in question now are not much better.

Cybersecurity is not something that is easy to regulate. That is why it is a good idea to look up and try to see a little further. I agree that the bill is well-intentioned, but intention without courage is meaningless.

A poet that I recently met in Montmartre told me that there is no love, only shows of love. It is the same thing here, except that we are talking about shows of courage, and so I hope that the government will show courage with Bill C-26 and turn its intentions into action.

Let us send Bill C-26 to committee as soon as possible.

---

## PRIVATE MEMBERS' BUSINESS

• (1740)

[English]

### FEDERAL FRAMEWORK ON AUTISM SPECTRUM DISORDER ACT

**Hon. Mike Lake (Edmonton—Wetaskiwin, CPC)**, seconded by the member for Don Valley East, moved that Bill S-203, An Act respecting a federal framework on autism spectrum disorder, be read the second time and referred to a committee.

He said: Madam Speaker, it is an absolute pleasure to stand here to discuss Bill S-203, which came to us from the Senate. It was unanimously passed by the Senate before it got to us here.

As members know, I do not speak with the authority of someone who has autism. I do not speak with the authority of a scientist and the folks who do unbelievable work, many of them right here in Canada, leading the world in the science around autism. I speak as a father of an incredible young man, very familiar to people this place, named Jaden, who was 10 years old when I was first elected, and last month he turned 27. He is an energetic young man who brightens up this place when he runs around giving people high-fives, as he is so happy and excited to meet folks.

I will probably share a little more from the heart, but I will start with the technical details and touch on what the bill would do.

As was mentioned in the introduction, this is a proposed act respecting a federal framework on autism spectrum disorder, and I am not going to get into every aspect of it. The bill is just over two pages long, French and English, so it is not super long. Importantly, it leads off with a statement that “The Minister of Health must develop a federal framework on autism spectrum disorder.” It then lays out the measures to be provided, which folks can take a look at on the Internet and see the bill there.

Its real strength, I think, is in its accountability mechanisms, and towards the end it talks about the minister. It says, “Within 18 months after the day on which this Act receives royal assent, the

### Private Members' Business

Minister of Health must cause to be tabled in both Houses of Parliament a report setting out the federal framework on autism spectrum disorder developed under section 2.”

Further to that, later on it says:

4 (1) Within five years after the day on which the report referred to in section 3 is tabled in Parliament, the Minister of Health must cause to be tabled in each House of Parliament a report that sets out

(a) the measures from the federal framework that have been implemented and their effectiveness in supporting autistic persons, their families and their caregivers; and

(b) with respect to any measure included in the federal framework that was not implemented, the reason it has not been implemented and the timeline for its implementation.

I think there is a really strong accountability framework.

For anybody who has been working in this area over the years, there is a real impatience right now. It has been many years that we have been talking about a national strategy. However, here we are today, and I think it is an opportunity to move forward, with some of that impatience, yes, but with real hope for the future for people with autism in this country and the people who care about people with autism.

My other hope is that, in addition to whatever strategy the government comes forward with, and there is indication that the government will be coming forward with a strategy maybe even ahead of the timeline outlined in this bill, it will be both substantial and organic. I think part of the problem over the years is that we have been waiting for perfection, waiting for every box to be checked. Therefore, we have had delay after delay. We have to recognize that we are never going to have unanimity, but there is a lot of common ground. If we work together towards that common ground, we will be able to make some progress. Then, through constant consultation with autistic Canadians, scientists and the broader community of families and caregivers, we can make whatever it is that we come up with stronger and stronger all the time.

I have a few thanks to give that are worth mentioning.

First, this bill did come from the Senate, where it was supported unanimously but largely led by Senator Housakos and Senator Boehm. I offer a huge thanks of appreciation to Senator Housakos and Senator Boehm. Also, I would be remiss if I did not thank Senator Jim Munson, now retired from the Senate, who led the charge on this for years and years.

I also want to thank colleagues from all sides of the House. I have been so fortunate over the years as we have worked on these things to have support from my own colleagues. As well, today, this bill is seconded by a Liberal colleague, whom I have had the chance to work with in his previous life when he was on the provincial side of things, more behind the scenes, trying to find some common ground when we could. My experience is that we have had so many people contributing in that way.

I thank everyone who has contributed to Jaden's life: his sister Jenae, his mom Debi, his grandmothers Helen and my mom Bonnie and her husband Dale, and all of the people who have surrounded him over the years.

*Private Members' Business*

● (1745)

I am going to turn to the second half of my speech, where that common ground, in my experience, lies. It is pretty straightforward. As we have conversations with people across the country and around the world, there are some really common areas where there is a lot of work that needs to be done and is critical to achieving the best outcomes for autistic people. That is diagnosis and early help. Some people say early intervention or early therapy, whatever it might be, but a good common ground word would be help for people. There is education, employment, housing. The sixth thing that is a little more vague but we all are concerned about is this idea of what happens when we, as parents, are gone. Are we going to have people around our loved ones who are going to care for them like we cared for them? That is a critical question.

Two of the things that I have kind of focused on or learned as I have gone down this path, both through my experience with Jaden and in talking to lots of other stakeholders, particularly autistic people themselves, are the ideas of inclusion and autonomy and what those things mean. If I think about autonomy for Jaden, it is a bit tricky because Jaden has real difficulty with abstract things like danger. Jaden could not have full autonomy because he might run into a street. He loves dogs. He might see a dog and run across the street to grab the dog by the side of its cheeks and pull its face into his face so he can smell the dog's breath, feel the dog licking his face and he would not even be aware of traffic as he is running. There are all sorts of danger awareness issues.

I like to think about maximum autonomy. With Jaden, when I think about maximum autonomy, I think about the fact that too often we are impatient, trying to figure out what he wants or presuming we know what he wants. We do not take the time to really listen to him. What I have learned over time and my advice to loved ones of people with autism is to really try to get down to their level, in a sense. We should not force them into our world, but get down in their world and really take the time to try to understand what they are trying to say.

When Jaden grabs my face and says, “Ba, ba, ba, ba, ba, ba” super intently, he is trying to tell me something, and it is incumbent on me, as someone who cares for him, to try to understand what he is trying to tell me. That may be through his body language, his facial expressions. Sometimes his skin tone is a little different. Sometimes he is paying attention to and looking at something that is bothering him, like we forgot to grab something that is important to him, such as his iPhone or something like that. He is always trying to communicate something. It is incumbent on us to try to find out what that is if we are going to maximize people's autonomy.

I will talk about inclusion. I talked about maximizing autonomy for Jaden, but we talk about inclusion as well. Full inclusion is a really tricky concept. Not every fully inclusive situation is perfect in every scenario for every single person, but that goes for us as well. There may be things that we do not prefer or ways that we prefer things to be that are not the same as everybody else wants.

As we look at inclusion, I think about inclusion in Jaden's case. Jaden was included in a regular classroom, but he was not included in the same way as every other kid by himself in that classroom. He had an assistant with him. It is a bit different, a modification to help

him mitigate some of the challenges he had, but he was in a regular classroom from kindergarten to grade 12.

That regular classroom really served him well. He surprised a lot of people. He had kids around him who really saw what he was good at and because they paid attention to what he was good at, they had a chance to realize that oftentimes his abilities surprised them. They were beyond what they might have thought. They had a chance to get to know him because they were in his classroom, and they challenged him.

For him, that was being included in a musical theatre production in grade 10. He was first in a group scene in grade 10, but then he again outperformed expectations, so in grade 11 they gave him a few more scenes. They put him in some sort of dance routines and things like that and taught him to do those things.

● (1750)

Then in grade 12 they did another performance, and one of the girls in the class asked if Jaden could be her partner, her husband, in *Joseph and the Amazing Technicolor Dreamcoat*. She modified all of the routines to make it look like he was doing exactly what everyone else was doing. That is what inclusion looks like. That is what maximum inclusion looks like. It is people getting to know people and then challenging them. It is embracing their skills and abilities and helping them with their challenges, just like all of us need in this place.

We have so many people who are here to help us in that regard. Not all of us can draft perfect policies, so we have people working in the House of Commons who help us with that from time to time. There are all sorts of those things. We have translators who translate, because not all of us are perfectly bilingual. We are all challenged with something. For people with autism, it is no different from that.

I am going to close by telling a story I tell at the end of my presentations. I do presentations around the world about how we define normal.

About 10 years ago, we had a chance to do an interview. My daughter was 13 at the time and Jaden was about 17, and we had this chance to do an interview with Steve Paikin. Anyone who has done an interview with Steve Paikin, and there are a few of those people in this world, know he can ask some tough questions sometimes. He gave Jenae a heads-up that he would ask her a tough question in the interview, but he had not given her a heads-up as to what it was going to be. He asked her if she sometimes wished her brother was “normal”, like every other kid. He said, “quote, unquote”. He knows Jaden and he knows Jenae as we had done interviews with him before.

Jenae, without skipping a beat, at 13 years old said, “Well, honestly, since Jaden was diagnosed with autism before I was born, I don’t exactly know what a normal brother is like, so Jaden kind of is my normal, having autism.” Steve pressed her and asked, “Do you like him just the way he is?” She responded, “Honestly, if Jaden didn’t have autism or was, like, cured or something, he wouldn’t be the same as Jaden is now.” At 13 years old, as a sister, she said that.

When I am talking to students and am talking about this in front of 500 introduction to psychology students, or whatever the case is, I will point out that in Jenae’s case, she did not have a choice. She was born into the family and Jaden was already there, so her normal was kind of set out for her. However, the school they went to from K to 12 had a choice, and it chose to include Jaden in the classroom.

At the time, we thought that was better for Jaden, but every single kid he graduated with, every single kid who was in that school with him, would say their life was immeasurably better because Jaden was included in their class. They learned so much. When they move forward in their lives, the diversity of knowledge they have is so different.

I often like to think of my life and my normal and how we define it. It is almost like, and bear with me here, a video game character. Think of a video game character and imagine a circle as long as we can see, and that is our video game character, and we walk around and experience things in that bubble. Sometimes that is what our life is like. I am 53 years old. My life is like 53 years of walking around in that bubble. Sometimes a TV screen or a computer monitor comes into that world and shows me something from the outside, but that is my normal.

If that circle only included people just like me, first of all, my weaknesses would be the same as other people’s weaknesses, so nobody would be there to compensate. Also, my strengths would not be strengths because everybody would have the same strengths. Our world, our normal, is better when we are surrounded by people who come from different backgrounds and who have different experiences. To the extent that we grasp that and include all Canadians in our experiences, our workplaces, housing, education systems and in everything else, we are all going to be better off for it.

I look forward to hopefully passing this bill and creating this better world for all Canadians.

• (1755)

**Hon. Judy A. Sgro (Humber River—Black Creek, Lib.):** Madam Speaker, I extend sincere congratulations to my colleague. This has been an issue the two of us, and others, have talked about so many, many times. It gives me great pleasure to stand here and congratulate you and ask you about timelines, because I do believe our government is quite supportive. Could you elaborate a bit on your expectations on the timelines you are looking for to move forward with this framework?

**The Assistant Deputy Speaker (Mrs. Carol Hughes):** I want to remind the member to address the question through the Speaker. She might want to use the word “him” as opposed to “you”.

The hon. member for Edmonton—Wetaskiwin.

### *Private Members' Business*

**Hon. Mike Lake:** Madam Speaker, the bill lays out a time frame of 18 months for a report. Hopefully, we are going to move this bill forward faster than would normally be scheduled. I am hoping debate will collapse tonight and we will be able to save some time to get it to committee and then move forward even faster.

As for a timeline, my hope, and she can probably play a role in this as a member of the Liberal caucus, is to encourage the government to move forward with a national strategy, which I know is being worked on right now, as quickly as we can, so we can put all of this energy to work with this collaborative vibe we have going on in the House right now to benefit these folks who really, really can use the help.

[*Translation*]

**Ms. Andréanne Larouche (Shefford, BQ):** Madam Speaker, I thank my colleague for his very moving speech.

In my personal experience, I had the good fortune of being involved with a magnificent youth hostel, and the people who helped us during the day were people on the autism spectrum. What a fantastic experience it was. It opened my eyes to the need to include them.

My question is the following. In Quebec, we have so many good initiatives. Is my colleague open to referring the bill to committee to benefit from all the good things happening for people with autism in Quebec’s health and social services system?

• (1800)

[*English*]

**Hon. Mike Lake:** Madam Speaker, I totally understand the jurisdictional issues that sometimes the members of the Bloc have to grapple with, but I have had great conversations with colleagues from my hon. friend’s party. We look forward to getting it to committee and hearing from experts from across the country.

The whole point of a national strategy is that we benefit from the very best evidence, from the very best experiences that folks are having not only across the country, but around the world. In a sense, we inhale that information and use it to our benefit. Then, as we gather that information, we can almost exhale it to the community for its benefit. It is almost like breathing. We constantly, with every breath, get stronger and better. That is what we want to do, and getting it to committee is a huge part of that process.

**Ms. Laurel Collins (Victoria, NDP):** Madam Speaker, I want to thank the member for his ongoing advocacy for autistic Canadians. I really appreciated his comments.

I was hoping he could expand on two points that he touched on briefly. One is how we ensure this piece of legislation adheres to the principle of “nothing about us without us”. The second is the need for tangible investments to improve the services and supports for autistic Canadians, families, service providers and caregivers.

*Private Members' Business*

**Hon. Mike Lake:** Madam Speaker, I am loving these questions from all sides. They are hitting the nail on the head. They indicate there is a real understanding of what needs to happen.

The “nothing about us without us” conversation is something that I think we continue to get better at, but we have a long way to go. It is a challenge. There is a segment of the autistic population that is able to clearly communicate what it is like to have autism. There are other people on the autism spectrum in Canada for whom it is a bit more difficult to communicate, but I think that we are all learning that we have a long way to go to include those voices.

I have one more quick comment on that. What is very important is that we make sure we are including indigenous Canadians with autism in that conversation as well, because I think they have been under-represented in many of the conversations over time.

**Mr. Ziad Aboultaif (Edmonton Manning, CPC):** Madam Speaker, as the hon. member has been very active on this file for a long time domestically and internationally, what advice can he give from seeing what is happening in other parts of the world to make this bill better and stronger?

**Hon. Mike Lake:** Madam Speaker, I will say this. As I have travelled the world and talked to people, we are doing better in Canada and North America than in many parts of the world. We have a lot to offer in terms of knowledge and we have a lot to learn in terms of knowledge, but if we get this right, we can export the knowledge that we have to other parts of the world, sharing and having conversations about how we make life better for everyone. I think this is a real opportunity for us to take a leadership role at a global level on inclusion.

**Mr. Michael Coteau (Don Valley East, Lib.):** Madam Speaker, I am proud to stand here today on behalf of the residents of Don Valley East to join my colleague in supporting Bill S-203. I was very proud to be asked to join this coalition of great parliamentarians who are working hard in the Senate and in the House of Commons to really move an issue forward that is long overdue. This bill is a great example of parliamentarians coming together to do the right thing. It is a great example of the House of Commons and the Senate working together to push forward a bill that will help so many Canadians and their families.

The bill calls upon the government to develop a national framework to better support autistic individuals in Canada. It is a very ambitious bill. It asks territories, provinces, communities, stakeholders and people to come together to build this framework to better support autistic individuals.

What I really like about the bill is that there is a strong emphasis on people as they transition into adulthood. It puts forward a strategy, if it does pass this House, to better position them in life and look for ways to leverage all the great supports that are out there, some of which are working better than others in terms of coordinating and sharing best practices.

I want to take a moment to acknowledge the colleague who just spoke. He has done great work over the years. I have had the opportunity to work with the member for Edmonton—Wetaskiwin on the autism file over the years, while I was a provincial member. I want to thank him for his advocacy and his work.

I also want to thank Senator Housakos, who is the mover in the Senate of the bill, and Senator Boehm, who has helped move the bill along.

It has been interesting for me over the years. I was a school board trustee from 2003 to 2011. The first time I started to work within the autism sector was when a parent came into my office one day to meet with me. She was so taken back that the school system, the Toronto District School Board, did not have the supports in place to help her child. She specifically spoke about the ABA instructors not being available in the classroom for her child.

Back then, I knew nothing of the subject. I have a couple of family members who are autistic, but beyond that I do not know much about the politics of autism. Over the years at the school board, learning about the history of it and going to the province and learning about the history of the autism sector and its interaction with government services, it really surprised me. It was an awakening.

Back then, in 2006-07, we worked hard to put forward the first ABA demonstration classroom in Toronto, if not the entire province. The parent became an incredibly good friend of mine, but she spoke a lot about how I helped and I listened, and the director of education at the time, Dr. Chris Spence, had listened to help develop this classroom. She would thank me all the time.

I did not realize that she was actually educating me and preparing me for many years later, when I became the minister of children and youth services in Ontario and was responsible for autism services in the province.

My journey back in 2006-07 opened up the door to an incredible sector of individuals working so hard, parents and young people in that sector, who have worked so hard to support the community and provide the best possible services for children. There was no question that I could easily sense the frustration with the history of autism services and how they were delivered in Ontario.

When I first became the minister responsible for the file, there was a protest around Queen's Park. There were probably 10,000 people. There was an age cut-off. Anyone over six no longer qualified for the same services as those under six. I was put on the portfolio and I had months to develop a new plan from scratch.

● (1805)

I had the opportunity to work with many individuals in Ontario from the sector, people such as Bruce McIntosh and so many other parents and advocates, to look for a way to build a new program, the Ontario autism program, the OAP.

We were able to not only double the funding back then and remove the age restrictions but also invest in diagnostic tools and expand on the diagnostic locations where one could go to get a young person to meet with someone, do a diagnostic and figure out if they required services such as ABA services. We also got to invest in research.

What I learned back then was that, in the system itself, not only in Ontario but also across the country, there was a lack of coordination. Organizations were not equipped to work with each other and share information. Governments did things differently everywhere.

This national framework, I think, would help everyone to work with provinces, territories, organizations, parents and advocacy groups. It would bring people together to better position young people and any autistic individual in this country for life.

At the end of the day, this is about basic decency. This is about returning decency to decision-making and to building programs that speak to the values we have as Canadians. The fact that we can come together in the House, remove all partisanship from this issue and do what is best for people who are autistic and their families, demonstrates to me our values and our decency as Canadians.

I am hoping this bill will move through the House as quickly as possible and that we can go forward with a national framework that will better position people in this country.

I do want to also take this moment to acknowledge the “Pay Now or Pay Later” report from back in 2007. That was put forward by Jim Munson. I do not know former senator Munson well. I have heard his name many times, and I know that people speak very highly of him. In 2007, when I was back in Don Valley East working with parents, trying to build a demonstration ABA classroom, the former senator was in the Senate, building a call and an awakening across the country to do better for autistic people in our country to ensure that they have decency, the benefit of programming and the ability to live their lives at their full capacity.

Here we are today, many years later, in the House, and I am hoping that we can come forward with a strategy that will make this country a better place for everyone.

• (1810)

[*Translation*]

**Ms. Andréanne Larouche (Shefford, BQ):** Madam Speaker, I would like to begin by mentioning Mathieu Caron, a man from Sherbrooke whose podcast helped me better understand what it is like to be an adult living with autism. Hi Mathieu.

Today I am talking about Bill S-203, which would provide for the development of a federal framework designed to support autistic Canadians, their families and their caregivers. It directs the Minister of Health to develop a federal framework on autism spectrum disorder. The national framework must identify measures relating to research, culture and tax benefits, among other things. The minister must consult with other relevant federal ministers, civil society groups, and provincial governments and the Government of Quebec, including their ministers of health. Lastly, the bill provides for the tabling of a report in Parliament, as proposed by Quebec senator Marie-Françoise Mégie, who is also a doctor.

### *Private Members' Business*

The Bloc Québécois will vote in favour of the bill at second reading so that it can go to committee and be amended in such a way as to respect Quebec's jurisdiction. In my speech, I will discuss the pros and cons of this bill, share examples from Quebec and conclude with a reminder about the importance of investing in health.

To begin with, in 2019, the Minister of Health's mandate letter directed her to “Work collaboratively with provinces, territories, families and stakeholders toward the creation of a national autism strategy”. On October 27, 2020, the Government of Canada announced \$1.46 million for the Canadian Academy of Health Sciences, or CAHS, to lead consultations on a national autism strategy. The CAHS report was released in May 2022, and the Public Health Agency of Canada hosted a national virtual conference on November 15 and 16, 2022, to inform the development of a national strategy.

As a reminder, autism spectrum disorder is a neurodevelopmental condition. The term refers to a range of disorders characterized by difficulties with social skills, repetitive behaviours, speech and non-verbal communication. Individuals on the autism spectrum may also have co-occurring health conditions that affect their overall physical health, including their mental health.

According to the Public Health Agency of Canada, approximately one in 50 Canadian children and youth, or 2%, have autism. That number has gone up over time. In Quebec, the annual prevalence of ASD in children aged one to 17 has been growing strongly, rising from one per 1,000 in 2000-01 to more than four per 1,000 in 2014-15. This prevalence differs according to the child's sex and age. It was 7.3 and 1.8 per 1,000 among boys and girls, respectively, in 2014-15.

People on the autism spectrum need support in various areas, such as housing, employment, education and, of course, health services. Within its areas of jurisdiction, the federal government can play a role in supporting these people and their families. Autism intersects with other identities such as race, ethnicity, culture, socioeconomic status, gender and sexuality, and that intersectionality creates diversity in experiences and needs that must be taken into account. People with autism do not always feel safe or meaningfully included in their communities. Such experiences can have harmful outcomes to their health, safety and quality of life. We must work harder to include them.

*Private Members' Business*

Stigma and discrimination can be addressed by shifting public attitudes towards autism acceptance and awareness through public campaigns, social contact, training, and education programs. The physical and emotional safety of people with autism can be fostered by promoting autism-inclusive, neuro-affirming and accessible spaces, programs and understanding in local communities. Best practices for suicide prevention can also be adapted to better meet the needs of individuals with autism at risk for suicide.

Improving the accessibility and inclusion of public transportation, recreational facilities, leisure programs, and technology can enable community participation of people with autism. Quebec and every province and territory offer autism diagnostic and support services, yet there is wide variability in what is available, which can contribute to delays and disparities. Some people with autism are particularly disadvantaged, such as those living in rural and remote areas, equity-seeking groups, and adults with autism. Research to develop valid and meaningful strengths-based diagnostic tools and improve access to diagnostic assessments for adults with autism is also suggested.

Adopting family-centred services available across the lifespan can promote the health and well-being of the entire family. It also empowers families to be involved in service delivery.

• (1815)

Young autistic children benefit from early access to supports and services because this is a time of significant development. Equitable access to school and community supports across a range of life domains can promote academic success, life and social skills, and improve mental health.

Implementing health and education transition policies and practices may help manage and prevent mental and physical health challenges and promote better adult outcomes.

However, research about autism in adulthood is limited. More than half of Canadians with autism rely on disability benefits.

Academic supports and accommodations available in post-secondary institutions do not always meet the diverse range of autistic students' needs and abilities, which means that they are still not enrolling to the same extent as non-autistic and other disabled students.

Some ways to create more inclusive workplaces, which is also important, and to improve employment outcomes can involve providing autism-inclusive supports and accommodations, giving access to supported work experience and internships, addressing benefit disincentives, and promoting workplace autism acceptance. Mr. Caron spoke at length about this with me.

With the limited availability of affordable housing in many regions, autism-inclusive housing is in even shorter supply across Canada, and the need will only grow.

Second, with its generous social safety net, Quebec already offers a wide range of services for individuals with autism. The Bloc Québécois hopes that the strategy will recognize these efforts, and that Quebec will not be penalized for its generous social benefits.

We also have some excellent examples in Quebec. Les Grands Ballets Canadiens de Montréal offers a program called "dance for well-being". This great model contributes to the well-being of people living with autism spectrum disorder, their families and caregivers through the benefits of dance.

Quebec offers a wide range of services for people with a physical or intellectual disability or an autism spectrum disorder to develop, maintain and compensate for their disabilities and promote their autonomy and social participation. These services are also intended for family and loved ones. They are divided into three categories. One category is local services that are often offered in the individual's living environments, such as the home, school or workplace. They aim to compensate for functional disabilities and reduce the risk of harm to ensure the safety of activities related to lifestyle. Examples include home support services, residential services, support for meaningful and rewarding activities, and support services for family and friends.

I would like to highlight the work that has been done for the past 45 years by the Fédération québécoise de l'autisme, a provincial group of organizations and individuals who are concerned about the interests of people with autism, their families and friends. This federation defends their rights, supports community life, informs and instructs Quebecers on issues related to autism, and participates in research.

There are 16 regional autism associations in Quebec. Associate members include other associations, early childhood centres, rehabilitation centres, school boards, schools, hospitals and private clinics. Everyone works together. The regional autism associations are community organizations primarily made up of parents, and their shared mission is to promote and defend the rights and interests of people with autism in order to enable them to lead a dignified life and achieve the greatest degree of social autonomy possible.

Third, I certainly must mention the fact that the Bloc Québécois is adamant that delivery of health services is not a federal jurisdiction. It refuses to allow the federal government to impose its standards and ways of doing things on Quebec and the provinces.

As such, the Bloc Québécois wants to emphasize that one component of the national strategy, timely and equitable access to screening and diagnosis for autism spectrum disorder, is not under federal jurisdiction. When it comes to delivering health care services, the best thing the federal government can do is increase health transfers. That is why the Bloc Québécois will seek to amend Bill S-203 to ensure that it respects Quebec's and the provinces' areas of jurisdiction.

In closing, I would be remiss if I did not mention the federal, provincial and Quebec health ministers' meeting, which took place from November 7 to 9, 2022, and ended inconclusively. The only solution is higher transfers.

The Bloc Québécois supports Quebec and the provinces' unified demand that the federal government raise health transfers from 22% to 35%. This permanent increase is what will help people living with autism spectrum disorder. Again, only a 35% contribution from the feds will enable people to live with autism spectrum disorder.

In closing, I thank the Granby association for intellectual disabilities and autism. I had the opportunity to visit this organization recently, and the people there are doing absolutely terrific work. Quebec has plenty of wonderful organizations like this one. I hope the federal government will provide health transfers so that we in Quebec can continue to help them and help people with autism.

● (1820)

[English]

**Ms. Rachel Blaney (North Island—Powell River, NDP):** Madam Speaker, I am honoured to speak to Bill S-203, respecting a federal framework on autism spectrum disorder.

Before I speak about this really important bill, I want to recognize that today is my grandson's birthday. I want to wish Dude a very happy birthday. I wish I could be with him. As so many of us in this place know, we miss a lot of important days. It is hard for me to miss his birthday today, so I just wanted to wish him all the best.

I want to give many thanks to the member for Edmonton—Wetaskiwin. I know about his advocacy. I have certainly seen this bill in this place before. I hope that we finally get it through. It is so important.

I think the basis of this is really about how we look at this whole country and make sure that everyone feels like they belong. One thing that is very clearly a challenge in a country as big as ours is that often different provinces and territories have different services that do not always meet the need. It is really important that when we look at this framework, we understand that by bringing everyone together. We want to see the best supports in place for those living with autism spectrum disorder and for those who love them the most.

Whenever one of our fellow members brings their human experience, their lived experience, to this place to say, as a person who lived through these realities, here is a way we can make life better for everyone, we should all pay attention. We should all listen and

### *Private Members' Business*

make sure that when we speak to this issue, we speak in a collective voice. I certainly hope that is what happens.

This really talks about having a national framework and making sure there is a timely and equitable process for people to access screening and diagnosis so that they are able to access the supports that are there. It is also so much about providing good financial supports. Often folks living within this group have challenges. There are extra needs. We want to make sure that people have the supports they need to do this well and that there is support for caregivers. There is nothing worse than seeing people who are working so hard giving all of that care and they burn out because we do not have the proper supports in place for them. We do not want to see that happen. We want there to be success where there should be success.

This also talks about having meaningful research and the resources there to provide that research so that those services are there. In that way, our communities can do better and we can provide an adequate service, community connection, so that people can succeed.

I often think about this. I think about how we can pay attention to what is happening to all of the people in our communities so that no one gets left behind. I think about how we can take the time to notice where those blocks are and remove those blocks so that we can have that wholesome support.

Public education is part of this framework. That is incredibly important. It is only with education that we draw so much more awareness and allow people to hold this information. It creates an environment of curiosity. That is really important. I cannot say enough from my perspective about how much we need to have curiosity so that when somebody is a bit different from us, instead of us being afraid, we really open doors, ask questions and learn how we can work with people in a more meaningful and profound way.

What we know based on so much research is that people in our communities have been left behind. It is shameful that in this country things fall apart. That really worries me.

I often think of Maya Angelou, who is a great hero of mine. She used to say that when we know better, we do better. That is why public education is important because, hopefully, the more we know, the more opportunity we can see, the more doors can be opened and the more inclusive our communities will become.

● (1825)

We also know that, if there is a co-occurring condition, it is even harder for families to be successful. There is a complexity, and added challenges, that we need to address, which is part of the reason this framework is so important. It brings people to the table to talk about the co-occurring conditions and what they mean going into the future. If we are going to provide and build communities that we can be proud of, a country that we can be proud of, we really need to make sure that that is done.

*Private Members' Business*

We know that resources around knowledge and research are desperately needed. We also know that rural and remote communities are often challenged to provide the services. This is a big concern for me. For myself, representing a rural and remote community, I see all too often that the services that are desperately needed across the board are just not there, and the people who are trying to provide those services are doing their very best. However, often when we look at service delivery, we forget that broad areas with lots of travel for service providers becomes very challenging, and asking families to travel big distances is another challenge.

We need to be looking at this. This is really important. I have spoken to people in my riding who deliver services, who work with families, and they talk about this repeatedly. They need more time. They need the right services in place. We need to find pathways so we are not sending families far away from home to get help because it just adds another burden. It is harder to get ahead. It is harder to do the everyday things of life. It is harder to maintain employment, sometimes, because of the high needs and care that are required.

I really hope that, when we look at this framework, we are really attentive to making sure that the needs that are out there are supported, regardless if people live in a more urban centre or in a more rural centre.

One of the things that is so important about this bill as well is that it talks about that coordinated effort, bringing all levels of government together to make sure we are not seeing overlap, and where there are gaps, identifying them and finding the resources to fill those gaps. This is so important.

I am grateful to be here to speak to this bill. In closing, I just want to say that the most important part for me, and I think we are almost there in this bill, is the concept of “nothing without us when it is about us”. I need to be very clear that is something the NDP will be making sure of. What we do not want to see happen is a framework put into place where people who are not living this every day, who are not supporting it every day, are having more of a say than those who are experiencing it.

The NDP will be supporting this bill. I look forward to seeing it finally getting through this place and out into the country so we can see better supports, and identify those key challenges, to building a better Canada for everyone.

● (1830)

**The Assistant Deputy Speaker (Mrs. Carol Hughes):** There being no further debate, the hon. member for Edmonton—Wetaskiwin has five minutes for his right of reply.

**Hon. Mike Lake (Edmonton—Wetaskiwin, CPC):** Madam Speaker, what a fantastic 45 minutes that was. This is a rare time in the House, because often things are pretty combative in here. I am reminded tonight, as we think about what we are doing here, of words from JFK: Things do not happen. Things are made to happen.

I am so thankful for two senators who did not take for granted that the government is moving toward a national autism strategy. It has signalled as much, and these two senators, and the entire Senate by extension, did not take that for granted. It has been a long time,

and a lot of us on all sides have worked on this for a long time. We are not going to wait for it to happen. We are going to work to make it happen together.

Today was a real example of that. It was a coming together of members from across the House. A few folks mentioned things they might change a bit when the bill gets to committee, whatever the case may be, which is the way it should be. However, let us find a common ground. Let us debate how we can make it stronger. Let us move forward.

One other thing I am thinking of relates to this. When I am talking to university students, I often talk about political labels and how helpful they are. We have the Liberals, the Conservatives, the NDP, the Greens and the Bloc in here. However, let us remember the fact that political labels are constructs. As helpful as they might be for the functioning of our democracy, we are human beings before we are political labels.

As we were having our conversation tonight, it felt more like we were human beings having a conversation about how we can make our country better. We set aside the political labels for a night because we agree on something. Sometimes that is okay if we largely agree on something.

That also extends, I would say, to the labels that science puts on us, as with autism. Autism is a label, if we think about it. There are a lot of labels we use that might be helpful for organizing, understanding or whatever the case may be, but we have to remember that we are human beings first.

I talked about help, and so often it is easy to think about legislation like this as legislation designed to help people. I just want to remind everybody in this place, as we have the conversation, that a big part of getting this right is understanding that we are going to benefit from it. As a society, we are stronger when we are using all of our strengths, all of our skills and all of our abilities. A huge part of what we are doing here tonight is creating an environment where we are operating on all cylinders and using all of our strengths and abilities. There are too many people who have the strengths and abilities we really need in this country whom we are not using to their full capacity because they are simply not included to the extent they ought to be.

I will close by thanking everybody who took part tonight and those who stuck around to support us. We really look forward to having a fantastic conversation at committee and getting this legislation passed through the House as soon as we can so that we can take the steps we need to take to realize the full potential of our country and include everybody.

**The Assistant Deputy Speaker (Mrs. Carol Hughes):** The question is on the motion.



[Translation]

If a member of a recognized party present in the House wishes that the motion be carried or carried on division or wishes to request a recorded division, I would invite them to rise and indicate it to the Chair.

• (1835)

[English]

**Hon. Mike Lake:** Madam Speaker, I request that it be carried on division.

**The Assistant Deputy Speaker (Mrs. Carol Hughes):** I declare the motion carried on division. Accordingly, the bill stands referred to the Standing Committee on Health.

(Bill read the second time and referred to a committee)

---

## ADJOURNMENT PROCEEDINGS

A motion to adjourn the House under Standing Order 38 deemed to have been moved.

[English]

### TAXATION

**Mr. Martin Shields (Bow River, CPC):** Madam Speaker, I appreciate the opportunity to speak in the House tonight and share the time and discussion on this topic with my colleague from Glengarry—Prescott—Russell, who I know works hard on his file and is committed to agriculture, as many people are in this House. I appreciate that he is here this evening for this discussion.

One of the things I have talked about in the House a number of times is the carbon tax and the challenge it presents for a particular part of the ag industry, which has a lot to do with ag production in Canada, but also specifically in the Bow River riding. My question is to do with the topics of exemption, rebate and inflation.

Canadian farmers, as my colleague would know, are among the most efficient, if not the most efficient, in the world. Ag emissions from Canadian ag producers are 70% lower than the average. At times the public does not understand or realize how efficient the ag sector is, but another important aspect is that Canada is the fifth-largest exporter of ag food in the world. Often ag producers feel like they are vilified. They should be applauded, but they feel vilified in our country.

In the Bow River riding, where the majority of irrigation is in Alberta and 4% of the land produces almost 20% of the Alberta ag GDP, the title of our ag minister is Minister of Agriculture and Irrigation. That is how important irrigation is in Alberta and in the Bow River riding, where the majority of irrigation is.

I am going back to the topic of exemption. To run irrigation, we use electricity. Ag producers use electricity. That powers irrigation. Electricity is not one of the exemptions under this government. The government often refers to the exemptions for fuels like natural gas, but electricity is not an exemption. It is very expensive.

The government will also talk about rebates. The rebate is about 1%, or a penny on the dollar, and these days pennies are not even legal tender. That is not much, so I have seen bills from my ag and

### Adjournment Proceedings

irrigation producers of \$7,000 per month for the carbon tax. I have seen irrigation carbon tax electric bills of \$40,000. Those are huge, and although the government says the rebate is 80%, or eight dollars on \$10, it is 1% for our ag producers. That is why they feel vilified.

Inflation has seen a 110% increase. The cost of farm fuel has doubled. Combines can cost \$1 million. If we add all the carbon tax on ag producers, they are feeling like they are vilified in their own industry and that the government is leaving them behind. The ag producers will be an industry that cannot produce food security within our own country. Ag producers are price-takers. They have nowhere else to put these costs, and when we talk about taxation, it is brutal.

Electricity is not exempt.

• (1840)

[Translation]

**Mr. Francis Drouin (Parliamentary Secretary to the Minister of Agriculture and Agri-Food, Lib.):** Madam Speaker, I would like to remind the member for Bow River that our government is making significant investments in Canada's agriculture sector. Our total budget for 2021-22 was approximately \$4 billion, the highest amount in recent years.

These historic investments make it possible to fund innovation, business risk management, market development, and compensation for our supply-managed producers and processors. In July, the federal, provincial and territorial ministers agreed to inject half a billion dollars to fund the new sustainable Canadian agricultural partnership. Of that amount, \$250 million was allocated to the resilient agricultural landscape program to support ecological goods and services provided by the agriculture sector.

[English]

The new agreement includes stronger targets, such as a three to five megatonne reduction in greenhouse gas emissions; an increase in sector competitiveness, revenue and export; and an increased participation of indigenous peoples, women and youth.

To respond to the member for Bow River regarding carbon pollution pricing, we have recognized the special role our farmers play in Canada. I would remind the hon. member that much of the agricultural sector is already exempt from pollution pricing.

Greenhouse gas emissions from livestock and crop production are not included in carbon pollution pricing systems. We also provided exemptions for gasoline and diesel fuel used by farmers for agricultural activities. There is also a partial rebate for commercial greenhouse operations.

*Adjournment Proceedings*

Beginning in the 2021-22 tax year, we are returning a portion of the proceeds from the price on pollution directly to farmers in back-stop jurisdictions through the refundable tax credit. Farmers in Alberta, Saskatchewan, Manitoba and Ontario will be eligible for an estimated \$100 million in the first year. That is expected to increase year to year.

At the same time, we are standing by our farmers who are on the front lines of climate change. Along with the provinces, we delivered over \$1 billion to help farmers get back on their feet after droughts, wildfires and flooding in western Canada and northwestern Ontario last year. We are there for farmers in Atlantic Canada who have suffered damages to their buildings and crops from hurricane Fiona.

I know the member will engage in some discussions after I am done my speech. I do sympathize with farmers who, last year in western Canada, lost 30% of their crops. That means 30% of crops could not make it to market because of the effects of climate change. Failing to act also has a cost to farmers.

We may differ on the ways to get there, but I believe that pricing pollution is the most cost-effective way to get to decarbonizing the processes in our agricultural sector. Otherwise, we would be stuck and bowed down with regulations that would cost farmers even more.

I welcome the hon. member's debate.

**Mr. Martin Shields:** Madam Speaker, I appreciate the comments, as well as the programs that many agriculture producers across the country enjoy.

Again, electricity and irrigation are challenges we have that were not mentioned. There is one other one that we need to mention and we need to be thinking about it now. The Americans do not have the carbon tax, but they are building a bank of vaccines for foot and mouth disease. Canada has not done anything, and it is not a matter of if, but when. We need to start looking at building a vaccine bank for our agricultural cattle industry. It is going to be critical. I hope the member understands that and will lobby for that particular vaccine bank.

**Mr. Francis Drouin:** Madam Speaker, I do want to emphasize one point again. I mentioned the federal backstop. The reason there are no specifics to irrigation systems or electricity in Saskatchewan is because the Saskatchewan government refuses to put a price on pollution.

If tomorrow the Saskatchewan government chose to respect the Greenhouse Gas Pollution Pricing Act, along with Alberta, Manitoba and Ontario, they could realize those specifics in each region. That is why it is incumbent on the provinces to act. Otherwise, we are going to keep facing these major disasters, which cost our communities and farmers extreme amounts of money.

On the foot and mouth disease vaccine bank, obviously he is making some good lobbying efforts. I know the cattle producers have made those same representations to me, and we are looking at this right now.

• (1845)

POST-SECONDARY EDUCATION

**Mr. Richard Cannings (South Okanagan—West Kootenay, NDP):** Mr. Speaker, science and research are the basis of our modern life. All the technological marvels and comforts we enjoy come from that. In the research ecosystem, it is graduate students and post-doctoral fellows who do most of the work. They do the heavy lifting, and they work full time on their research. It is a full-time job.

They are paid through postgraduate scholarships through the federal funding councils: the Natural Sciences and Engineering Research Council, the Social Sciences and Humanities Research Council and the Canadian Institutes of Health Research. The values of these scholarships were at one time enough to allow young researchers to live reasonable lives. I had one of these scholarships when I was doing my masters studies at the Memorial University of Newfoundland in the 1970s, and it paid for my housing and food, with a bit left over. By sheer coincidence, I am wearing my MUN tie tonight.

However, that is not the case today. The scholarship amounts have not changed since 2003. That is almost 20 years ago. Masters students now receive \$17,500 annually, and Ph.D. students get \$21,000 annually. That might have been enough 20 years ago, but we know how housing and food costs have skyrocketed since then. On top of that, these students have to pay their tuition, and that adds thousands of dollars to those annual costs. In fact, the average postgraduate tuition in Canada is over \$7,000 a year.

These are poverty wages. This is below minimum wage, yet this is what we are expecting our best and brightest to live on. We are depending on these students for our future, and we have to keep them here in Canada, but many of them are lured out of the country to find research and educational opportunities in countries that value them more than we do.

A group of students, scientists and other concerned citizens formed a group called "Support our Science" recently. They sponsored a petition here in the House of Commons that garnered over 3,500 signatures. They were asking the government to increase the value of graduate scholarships by 48% to match inflation over the past 20 years, and to index that to the consumer price index so it does not fall behind again. They also asked that the number of scholarships be increased by 50% to match the demand for graduate students and the demand for these graduates in the innovation workplaces of Canada.

Once these students complete their doctoral degrees, they seek out post-doctoral fellowships. It is the traditional route to finding work in academic institutions and in research and development companies across the country, but the number of post-doctoral fellowships does not line up with the number of doctoral students. About 3,000 masters students receive these scholarships, and almost 2,000 Ph.D. students receive the scholarships, but there are only about 450 post-doctoral fellowships offered. Because of that, a huge number of recent graduates leave Canada for post-doctoral work elsewhere in the world. In fact, 38% of them leave the country. They are drawn by good salaries and good lab support, both aspects in which Canada does not compete well.

At its most basic, valuing these students means paying them enough, so I urge the government to do the right thing and the obvious thing, and pay these young researchers a living wage.

**Mr. Andy Fillmore (Parliamentary Secretary to the Minister of Innovation, Science and Industry, Lib.):** Madam Speaker, I am happy to respond to the comments made by the hon. member for South Okanagan—West Kootenay regarding federal investments in science for our graduate students, scientists and researchers. In fact, I agree with just about everything he said. I must say it is good to see him flying the MUN school colours.

Canada is a leader in science and research, and the government is committed to ensuring that this continues. Every day, Canadian researchers stand at the forefront of new scientific discoveries and research breakthroughs. The Government of Canada has continued to invest in Canadian researchers, the key drivers of innovation who are helping to build a healthier and more prosperous future.

Enhancing the opportunities available to researchers has been a priority that the government has backed up with significant investments in successive budgets. Since 2016, Canada has committed more than \$14 billion to support the valuable contributions that scientists and researchers make to the health, well-being and prosperity of all Canadians. For example, budget 2018 announced historic new investments in science and research of over \$1.7 billion over five years, including \$925 million to the three granting agencies to support fundamental science, and \$462 million per year to establish permanent, stable funding to the Canada Foundation for Innovation to support research infrastructure in our country.

In terms of targeted investments to support students and post-doctoral fellows, the government recognizes the critical role that federal scholarships and fellowships play in nurturing and sustaining Canada's top talent, through support for career progression and increased financial security and independence. Budget 2019 provided \$114 million over five years, with \$26.5 million per year, ongoing, to create 500 more master's level scholarship awards annually, and 167 more three-year doctoral scholarship awards annually through the graduate scholarships program.

The government also recognizes that students and researchers are facing financial challenges that could be a barrier to pursuing higher education. During the COVID-19 pandemic, the government made \$450 million available through the Canada research continuity emergency fund with a view to helping our scientists and trainees get through a very difficult period.

### *Adjournment Proceedings*

Looking forward, to deliver an equitable, accessible and effective suite of scholarships and fellowships, the Government of Canada continues its work to promote equity, diversity and inclusion. Budget 2019 invested \$37.4 million over five years, and \$8.6 million per year, ongoing, to expand parental leave coverage from six months to 12 months for students and post-doctoral fellows to help young researchers better balance work and family.

Budget 2019 also invested in bursaries and scholarships for first nations, Inuit and Métis students through a \$9-million investment in Indspire, while the granting agencies have partnered with indigenous people to develop a national research program to advance reconciliation. Furthermore, through budget 2022, we invested \$40.9 million to support targeted scholarships and fellowships for Black student researchers.

We want to promote science in this country, and we will continue to invest in science across our nation.

• (1850)

**Mr. Richard Cannings:** Madam Speaker, the fact is that, for almost 20 years, there has not been any new money for these scholarship programs I have been talking about. These are our best and brightest young researchers, and they are living in poverty.

I appreciate that the government has increased spending in some aspects of science. It supports science. However, it needs to support these students. More and more of them are leaving Canada for the United States, the United Kingdom, Germany and Australia. Many countries are providing better living conditions and studying environments than Canada.

This brain drain costs our economy almost \$1 billion a year, just in lost training dollar investments. The solution is simple: Increase the scholarship amounts and increase the number of scholarships. It would be a relatively small investment that would have an immense payback for our country and for the young researchers our future depends on.

**Mr. Andy Fillmore:** Madam Speaker, I will conclude my remarks the way I started them by saying that I agree with the member in what he is saying. The government has heard the calls from the research community to increase the value of the scholarships and fellowships, and I am happy to say that we will continue to work with the federal granting agencies and the research community to explore ways to better support our next generation of researchers and top talent.

*Adjournment Proceedings*

The Government of Canada recognizes that for Canada to achieve its full potential, support for science and research must evolve. We are committed to ensuring that Canadian researchers are positioned for even more success now and in the future, and to better respond to the needs of the modern research enterprise. This is why the government recently announced the launch of the advisory panel on the federal research support system.

This panel will provide independent expert policy advice on the structure, governance and management of the federal system supporting research and talent. In a rapidly evolving global science and technology landscape, this panel will advise on how the govern-

ment can be more effective in fostering research excellence and support downstream innovation to support economic growth, drive breakthroughs and address complex societal changes.

• (1855)

[*Translation*]

**The Assistant Deputy Speaker (Mrs. Carol Hughes):** The motion that the House do now adjourn is deemed to have been adopted. Accordingly, the House stands adjourned until tomorrow at 10 a.m. pursuant to Standing Order 24(1).

(The House adjourned at 6:55 p.m.)

---





# CONTENTS

Thursday, December 1, 2022

<b>ROUTINE PROCEEDINGS</b>		<b>Questions on the Order Paper</b>	
<b>Government Response to Petitions</b>		Mr. Lamoureux .....	10256
Mr. Lamoureux .....	10253		
<b>Committees of the House</b>		<b>Points of Order</b>	
<b>Canada–People’s Republic of China Relationship</b>		<b>Requirement of Royal Recommendations for Bill C-285—Speaker's Ruling</b>	
Mr. Hardie .....	10253	The Speaker .....	10256
<b>Finance</b>			
Mr. Fonseca .....	10253		
<b>Bankruptcy and Insolvency Act</b>			
Mr. Angus .....	10253		
Bill C-309. Introduction and first reading .....	10253		
(Motion deemed adopted, bill read the first time and printed) .....	10253		
<b>Petitions</b>			
<b>Taxation</b>			
Mr. Kmiec .....	10253		
<b>The Environment</b>			
Ms. Blaney .....	10254		
<b>Climate Change</b>			
Mr. Johns .....	10254		
<b>Persons with Disabilities</b>			
Ms. Zarrillo .....	10254		
<b>Housing</b>			
Mr. Morrice .....	10254		
<b>Seniors</b>			
Mr. Rogers .....	10254		
<b>Charitable Organizations</b>			
Mr. Viersen .....	10254		
<b>Firearms</b>			
Mr. Viersen .....	10254		
<b>COVID-19 Mandates</b>			
Mr. Viersen .....	10255		
<b>Military Chaplaincy</b>			
Mr. Viersen .....	10255		
<b>Persons with Disabilities</b>			
Mr. Genuis .....	10255		
<b>Freedom of Speech</b>			
Mr. Genuis .....	10255		
<b>Consular Affairs</b>			
Mr. Genuis .....	10255		
<b>Charitable Organizations</b>			
Mr. Genuis .....	10256		
<b>Human Organ Trafficking</b>			
Mr. Genuis .....	10256		

Mr. Lamoureux .....	10281
Mr. Lemire .....	10281
Mr. Maguire .....	10282
Ms. Michaud .....	10282
Ms. Gladu .....	10283
Ms. Zarrillo .....	10283
Ms. Pauzé .....	10284
Mr. Lemire .....	10284
Mr. Lamoureux .....	10285
Mr. Carrie .....	10286
Mr. Johns .....	10286
Ms. Gladu .....	10286

## STATEMENTS BY MEMBERS

### Gender-Based Violence

Mr. Morrice .....	10288
-------------------	-------

### Retirement Congratulations

Mr. Badawey .....	10288
-------------------	-------

### Oil and Gas Industry

Mr. Kram .....	10288
----------------	-------

### Canada-Taiwan Relations

Ms. Sgro .....	10289
----------------	-------

### Félix Blackburn

Mrs. DeBellefeuille .....	10289
---------------------------	-------

### Uterine Cancer Screening

Ms. Koutrakis .....	10289
---------------------	-------

### Cost of Living

Mr. Barrett .....	10289
-------------------	-------

### International Day for the Abolition of Slavery

Mr. McKay .....	10289
-----------------	-------

### Gender-Based Violence

Ms. Saks .....	10290
----------------	-------

### Public Safety

Mr. Calkins .....	10290
-------------------	-------

### Crime Prevention

Mr. Chiang .....	10290
------------------	-------

### Indigenous Affairs

Mr. Vidal .....	10290
-----------------	-------

### Carbon Tax

Mr. Williamson .....	10291
----------------------	-------

### Laviolette Poultry Farm

Mr. Drouin .....	10291
------------------	-------

### Housing

Mr. Desjarlais .....	10291
----------------------	-------

### 350th Anniversary of Berthierville

Mr. Perron .....	10291
------------------	-------

### The Economy

Mrs. Kusie .....	10292
------------------	-------

### Gender-Based Violence

Ms. Sudds .....	10292
-----------------	-------

## ORAL QUESTIONS

### Firearms

Mr. Poilievre .....	10292
Mr. Mendicino .....	10292
Mr. Poilievre .....	10292
Mr. Mendicino .....	10292
Mr. Poilievre .....	10292
Mr. Mendicino .....	10292

### Housing

Mr. Poilievre .....	10293
Mr. Hussen .....	10293
Mr. Poilievre .....	10293
Mr. Hussen .....	10293

### Democratic Institutions

Mr. Blanchet .....	10293
Mr. Mendicino .....	10293
Mr. Blanchet .....	10293
Mr. Mendicino .....	10293

### Health

Mr. Boulerice .....	10294
Mr. van Koeverden .....	10294

### Indigenous Affairs

Mr. Angus .....	10294
Ms. Hajdu .....	10294

### The Economy

Mr. Hallan .....	10294
Ms. Bendayan .....	10294
Mr. Hallan .....	10294
Ms. Bendayan .....	10294

### Carbon Pricing

Mrs. Gray .....	10295
Ms. Saks .....	10295
Mrs. Gray .....	10295
Ms. Bendayan .....	10295
Mrs. Vien .....	10295
Ms. Bendayan .....	10295
Mrs. Vien .....	10295
Mr. Duguid .....	10295

### Official Languages

Mr. Beaulieu .....	10296
Ms. Petitpas Taylor .....	10296
Mr. Beaulieu .....	10296
Ms. Petitpas Taylor .....	10296
Mr. Beaulieu .....	10296
Ms. Petitpas Taylor .....	10296

### Diversity and Inclusion

Ms. Lantsman .....	10296
Mr. Alghabra .....	10296
Ms. Lantsman .....	10296





**PRIVATE MEMBERS' BUSINESS**

(Bill read the second time and referred to a committee) .. 10331

**Federal Framework on Autism Spectrum Disorder Act**

Mr. Lake .....	10323
Bill S-203, Second reading .....	10323
Ms. Sgro .....	10325
Ms. Larouche .....	10325
Ms. Collins (Victoria) .....	10325
Mr. Aboultaif .....	10326
Mr. Coteau .....	10326
Ms. Larouche .....	10327
Ms. Blaney .....	10329
Mr. Lake .....	10330

**ADJOURNMENT PROCEEDINGS**

**Taxation**

Mr. Shields .....	10331
Mr. Drouin .....	10331

**Post-Secondary Education**

Mr. Cannings .....	10332
Mr. Fillmore .....	10333



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>