HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

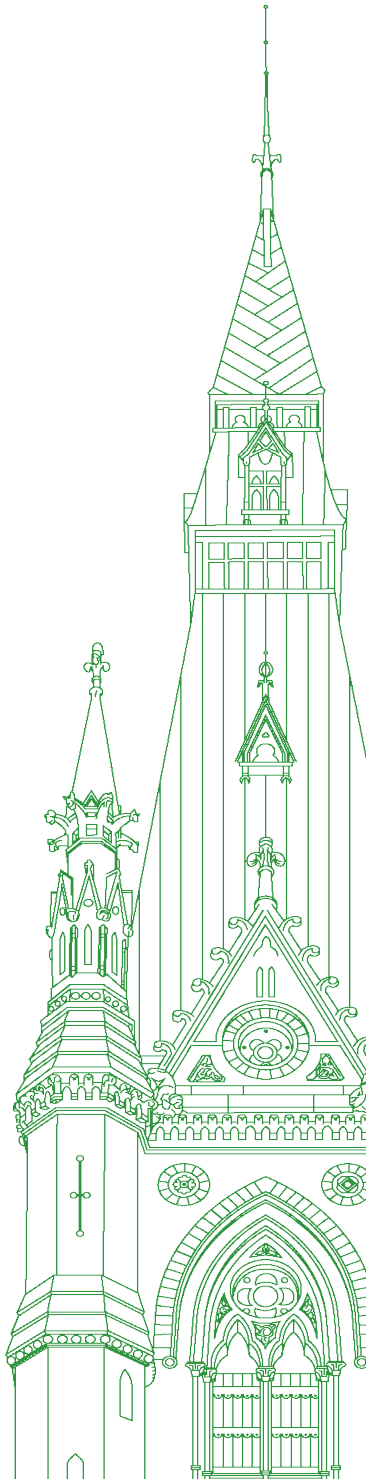
44th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 021

Tuesday, May 3, 2022



Chair: The Honourable Jim Carr

Standing Committee on Public Safety and National Security

Tuesday, May 3, 2022

● (1135)

[*English*]

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

I give my apologies to the witnesses for the delay in starting. We had a vote, as you all know. This is the time of the year when there are many of them. They're unpredictable, and we just have to go with the flow.

We're ready to start now.

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

We will start by acknowledging that we are meeting on the traditional, unceded territory of the Algonquin people.

Today's meeting is taking place in a hybrid format, pursuant to the House order of November 25, 2021. Members are attending in person in the room and remotely using the Zoom application. Members and witnesses participating virtually may speak in the official language of their choice. You will see at the bottom of your screen that you can choose floor, English or French.

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

With us today, not by video conference but in person, we have Dr. Charles Burton, senior fellow, Centre for Advancing Canada's Interests Abroad at the Macdonald-Laurier Institute, appearing as an individual. We have Jennifer Quaid, executive director of the Canadian Cyber Threat Exchange, who is appearing virtually, I believe. We also have, in person, Michael Doucet, executive director, office of the chief information security officer at Optiv Canada Federal.

Each of our guests will have up to five minutes to give us an introductory comment. Just so everybody knows, this is the 30-second warning. I am really strict. When we get to the end of the time allotment, either in opening statements or in rounds of questioning, I'll give you the 30-second warning. I'm afraid that is all the warning you will get.

I will now invite Dr. Burton to take the floor for up to five minutes.

The floor is yours, sir. Welcome.

Dr. Charles Burton (Senior Fellow, Centre for Advancing Canada's Interests Abroad, Macdonald-Laurier Institute, As an Individual): Thank you, Chair.

The threat posed by Russia to Canada's public safety and national security has increased significantly since the western democracies responded to Russia's invasion of Ukraine with measures designed to cripple Russia's economy and with weapons support for the Ukrainian resistance. Whatever the outcome of the suffering in Ukraine, Russia will remain shunned by the west and blocked from financial transactions and trade with lucrative European markets. Putin, I think it's fair to say, is seethingly angry, tormented and resentful, with dangerous capabilities to lash out at Canada in response. He is likely to make common cause with China, which will magnify the threat to us.

Canada is inadequately prepared for the range of threats posed by Russia, including threats to Canada's critical infrastructure, espionage and sabotage. We are less prepared than our allies.

A considerable concern in this regard is whether the RCMP, CSIS and CSE have been sufficiently accountable to the public safety and national security concerns of Parliament as represented by this Commons committee. We know that the RCMP, CSIS, CSE and DND gather a lot of information on Russian malign activities, but when Parliament asks for a briefing to inform the parliamentary development of legislation to protect public safety and national security, those agencies too often stonewall you, suggesting that the information is too sensitive or that disclosing it would reveal operational details that would be helpful to our enemies.

It would be reasonable to assume that Five Eyes, including Canada, were aware of Mr. Putin's megalomaniac ambitions regarding Ukraine. Nothing has changed in Russia. It's simply our perception of it that has become heightened. They know what he has in store for future invasions and what he has in store for threats to Canada, but how can Canada prepare if the RCMP, CSIS and CSE will not hand over their intelligence assessments on what we should prepare for? Too often, Canadian police and security agencies see their primary function as to simply curate information, which they can trade with the counterpart agencies. Again, this issue is more pronounced in Canada than for our allies.

For example, how badly does Canada need a foreign agents registry act, or something like the Australian Foreign Influence Transparency Scheme Act, as a national security measure? I judge this as very urgent for Canada, especially now, but CSIS would know better which Canadians influential in Canada's policy process have received benefits from a foreign state that put them in a conflict of interest that threatens Canadian security and sovereignty. How many of these are there? How high does it go? If CSIS has this data, they should give it to you.

What about the RCMP's Cameron Ortis? What should we be learning from his arrest? What about the Winnipeg labs matter? Was there a failing in protection of Canadian national security that should be addressed by Parliament? Then there's the Quentin Huang matter. Why is it that, unlike our allies, Canada does not successfully prosecute and send to prison people who transfer military technologies from Canada to agents of a foreign state?

Let me add one last point. As the Commons Special Committee on Canada-China Relations has examined, the Chinese-language media in Canada is strongly dominated by elements that support the Chinese Community Party's agenda in Canada. Since the outbreak of hostilities in Ukraine, Chinese domestic media and its proxies in Canada have been repeating the Russian conspiracy theories and associated disinformation day after day, week after week and more or less word for word. This Russian disinformation has the effect of discrediting the integrity of Canadian democratic and judicial institutions and debasing the loyalty to Canada of a significant fraction of Chinese Canadians.

Canada needs to take all of this much more seriously, in my view, and allocate the resources and the restructuring of our public safety and national security agencies to address it much more effectively than we have up to now.

Thank you, Mr. Chair.

● (1140)

The Chair: Thank you very much.

I would now like to invite Ms. Quaid to give us her opening comments.

The floor is yours for five minutes.

Ms. Jennifer Quaid (Executive Director, Canadian Cyber Threat Exchange): Thank you, Mr. Chair.

My name is Jennifer Quaid. I'm the executive director of the Canadian Cyber Threat Exchange, the CCTX.

The CCTX is a pan-Canadian, member-based, not-for-profit organization focused on enabling Canadian companies to build cyber-resilience through collaboration. We represent 170 members across 15 sectors. We were founded by some of Canada's largest companies, but our mission is to enable organizations of all sizes to reduce financial and operational risk through access to relevant and timely threat intelligence. Members choose to participate, because they recognize that being aware of the cyber-threat environment and its ever-changing landscape is the first step to ensuring the cyber-resilience of their organizations.

As Canada's Minister of National Defence recently said, “Cyber security is one of the most serious economic and national security challenges we face.” As you know, cyber-threats are becoming more sophisticated and are increasingly pervasive. Driven by the growth and global adoption of innovative technologies, cybercrime pays. Who does it pay? Cyber-threat actors can be grouped into roughly a couple of categories: nation-states who are conducting espionage and statecraft through the Internet, and criminals who are engaging in cybercrime for financial gain.

It's this criminal element that has commercialized cybercrime. It's now an industry unto itself. It's an industry where the barriers to entry are lower than ever. Technical expertise is no longer a requirement. Cryptocurrency makes collecting your fee easier, and the chances of getting caught are low. Several countries allow cybercriminal groups to operate within their borders, but we also have hacktivists, cyber-attackers designed to target social injustice, and the ever-present insider threat.

The ongoing geopolitical tension in Russia and Ukraine has created an opportunity for an increase in hacktivism and criminal activity. The threat actors are targeting critical infrastructure on both sides, taking down banking websites and disrupting government service. The Conti criminal organization is acting in support of Russia. Anonymous claims to be waging a cyberwar on Putin. Network Battalion 65 stole and used Conti's code to lock up files inside government-connected Russian companies.

Canadian organizations have been following events unfolding in Ukraine and are operating under a heightened sense of alert. CCTX members, in collaboration with the Canadian centre for cybersecurity, are working to ensure that Canadian businesses can better defend themselves from these attackers.

This is a good example of public-private partnership in action. Through the CCTX, the cyber centre has the opportunity to disseminate information to businesses of all sizes in all sectors. We can then enable our members to collaborate, leverage and use that information in a meaningful way, but collaboration is more than sharing threat information. It's professionals sharing best practices and working together on cyber-problems that are impossible to undertake within a single organization or sector.

It's engaging with others to improve your cyber-resilience—the resilience of your supply chain, your customers and the Canadian economy. It's an effective way to expand your team's capacity, which is increasingly important in an economy where there are 25,000 open positions. According to CIRA, 25% of organizations have reported a data breach, and the attacks aren't stopping.

What more can be done? The government can make sharing easier for many organizations by the simple act of creating “safe harbour” legislation, laws designed to encourage businesses and organizations to voluntarily share information by protecting them from legal repercussions, sharing beyond statutory requirements. You can also enable more companies to join a collaboration organization by making membership as an ITB—anything to encourage sharing information.

Collaborating on cyber-threats and building our collective resilience are critical to prevent, detect and contain cyber-attacks in the private sector. Our success increases significantly when we work together.

Thank you.

● (1145)

The Chair: Thank you very much.

I would now like to invite Michael Doucet to give his opening comment. He will have the floor for up to five minutes.

Go ahead whenever you're ready, sir.

Mr. Michael Doucet (Executive Director, Office of the Chief Information Security Officer, Optiv Canada Federal): Thank you very much.

Good morning. I'm honoured to be here this morning speaking on behalf of my organization, Optiv.

Our level of preparedness to the wide range of threats posed by Russia deserves this dialogue, our collective engagement and our commitment to focus on hardening our systems, preparedness and response. Optiv is pleased to be part of this dialogue.

As a practitioner who has contributed to national security in various roles in government for 30 years and now with the pure-play cybersecurity integrator for close to four years, I'm keenly interested in our approach to understanding and countering the cyber-threats facing us from Russia and other nation-states that wish to do us harm. This threat knows no national, provincial, territorial or municipal boundary.

Cybersecurity is a team sport that requires mature governance, focused attention, measurement and exercising. Continued diligence must be the standard.

I'll say a few words about Optiv.

Optiv is a world-class leading cybersecurity integrator. We work alongside clients and public, private and not-for-profit sectors to manage cyber-risks and equip organizations with perspectives and programs to accelerate business for program progress. We cover the wide range of cyber-products and services including but not limited to threat intelligence, threat hunting, incident response, managed services, and identity and data management.

In my role at Optiv as executive director of the office of the chief information security officer, I have pan-Canadian responsibility to engage all sectors and verticals in understanding, quantifying, exercising and enhancing their cyber-posture. Typically this is performed on a risk-based approach.

What do I mean when I talk about a risk-based approach? You begin by understanding your cyber-program. You then measure your cyber-program and identify gaps that must be closed to reduce risks to the organization. This is done on the backdrop of a changing environment requiring diligence and constant improvement. In the world of cybersecurity, your job is never complete. Organizations cannot take a day off. Digital transformations in cybersecurity are fast-paced, mission critical and increasing in complexity. It is incumbent upon all stakeholders and citizens to positively impact our digital environment.

Let's move to the weighty question of our level of preparedness on the threats posed by Russia, with a focus on continuity of government and critical infrastructure. Of course, government is part of critical infrastructure, but I'll speak specifically to the federal government.

At a high level, what is the threat posed by Russia? Let's take a look at the initial threat.

Prior to the ground offensive, Optiv's global threat intelligence centre widely distributed an advisory summarizing cyber-incidents related to ongoing tensions in Ukraine, as well as previous cyber-activity attributed to the Russian government and supported military operations in eastern Europe. Cyber-activity and Russian influence operations against Ukraine and NATO supporting Russian military shaping operations include denial of service attacks, psychological operations and disinformation campaigns as pretexting for military operations.

Let's move on to the question of preparedness. How do we measure our level of preparedness? We strive for a horizontal approach to cyber when threats and needs vary by critical infrastructure vertical. Cyber-programs should be right-sized to the organization; however, they can still be reported in a consistent manner. Every organization should know the health and status of their cyber-program. I can't put too fine of a point on that: every organization. You need to measure this. Then you need to determine the end state of your cyber-program. If there's a gap between those two, you need to endeavour to close that gap.

Practically, what does this mean? It means assessing your cyber-program, metrics, assessing gaps and developing a cybersecurity strategy. From the strategy, build programs and plans to address the gaps. You must evolve an incident response plan and business continuity plans to ensure continuity of operations. With this, you can support it by metrics and a dashboard. You need to exercise those plans to ensure that you are ready to respond to an incident. Then you need to continuously measure and improve the program.

I'd be happy to provide the committee with concrete recommendations during our discussions.

I will leave my opening comments at that, and I'll be pleased to take questions during the further discussion.

Thank you very much.

● (1150)

The Chair: Thank you very much.

You won't have long to wait for questions. I'm going to open the floor to questions right now.

Leading us off is Ms. Dancho.

You have a six-minute block, whenever you are ready.

Ms. Raquel Dancho (Kildonan—St. Paul, CPC): Thank you, Mr. Chair.

Thank you to the witnesses for being here.

Mr. Burton, my first questions are for you concerning Russia's relationship with China, and in particular how they both together signed a security pact, largely viewed as against America and the west. That was back in February. I'm just wondering if you could tell the committee, given your extensive experience and academic background with China, when we're looking at the security of Canada, and we're talking about Russia specifically in this study, how you view the security pact influencing how Canada should approach its own security.

● (1155)

Dr. Charles Burton: I think it is a cause of great concern. Essentially, because of Mr. Putin's badly advised or probably not advised invasion of Ukraine, Russia will be considerably weakened, both militarily because they're losing a lot of stuff—they lost the *Moskva* in the Black Sea—and they're also going to have their economy crippled. This will force Russia to have to rely more on China for export of the commodities that sustain Russia's prosperity, oil and minerals, and also to rely on China for bucking the sanctions that we've imposed. China has facilitated North Korea in effectively avoiding the sanctions that we attempted to impose on that regime.

We'll be in a situation where China I think will certainly extract a price for this, which will be that they will expect Russia to collaborate with China in China's overall global agenda, and that could include seeking Russian military support for action taken against Taiwan in the future, and combining with Russia with regard to claims in the Arctic.

Russia, as you know, claims pretty much everything under the Canadian continental shelf, and China has the resources and ability to actually start to exploit those Arctic resources. China referred to itself recently as “a near-Arctic state”. I think it's about as near to the Arctic as Yemen, but in any event, they want access to our northern resources for strategic purposes, ports and so on, and to our natural resources.

With the strategic positioning of Russia, if they go together, this is really very bad news for Canada. As I've argued elsewhere, unlike some of the other witnesses to this committee, I really feel that we need to start thinking about what sort of protection we can have for our northern regions. It's not really about do we give 2% or less or more. It's really about how much is it going to cost to overcome decades of neglect of our Arctic, particularly as Russia and China combine together and actually start to pose an effective threat in the light of global warming opening up those waters to navigation by Chinese and Russian vessels of various kinds.

Ms. Raquel Dancho: I appreciate that.

I wanted to ask you specifically as well about the Canadian ambassador in Russia and the Russian ambassador here in Canada, who has been widely seen to spread considerable misinformation in Canada.

The Liberal government right now is saying we can't expel the Russian ambassador from Canada because they'll do the same to our Canadian ambassador in Russia and, therefore, we won't have eyes on the ground. Can you comment on that? Do you agree with the Liberals' position on this?

Dr. Charles Burton: I wouldn't want to politicize it in terms of a political party, but I do think that if we do not make diplomats in Canada accountable for activities that are not consistent with their diplomatic status, whether this is menacing and harassment of people in Canada, or attempting to influence discourse in Canadian newspapers, particularly Chinese-language media, by coercing advertisers and the persons who may have relatives back in China to not report on things or to report them in a certain way.... I think those diplomats should be made accountable and we should PNG them, declare them *persona non grata*, and bear the consequences of reciprocal expulsions.

Our passive attitude towards this simply emboldens these regimes to do more. I think we have to put a stop to it. I anticipate that we'll see more of this in collaboration with our allies, particularly in Europe, in the months ahead.

Ms. Raquel Dancho: Thank you, Mr. Burton.

My next question is for Ms. Quaid.

I'd like to get your perspective on the weakest link in our cybersecurity in Canada. To my knowledge, our very large corporations have relatively strong cyber-defence, but what about down the supply chain for some of our larger corporations who rely on small and medium-sized enterprises. Can you comment on where you think we need to bolster our cybersecurity defences?

Ms. Jennifer Quaid: Thank you again for the question, Ms. Dancho.

You're absolutely correct. The small and medium-sized enterprises make up 98% of our economy, so in fact they're not just the supply chain for the large corporations but for the entire economy. They undoubtedly represent our weakest link, although I hate to use that term, and they represent that because, according to recent stats, 44% of them do not have any defences in place against a possible cyber-attack.

Many of our smaller organizations don't have the data. They don't feel that they're under attack or that they're a target for an attack. What they're not realizing is that data of any kind makes you a target.

You're quite correct. Forty-four per cent don't have any form of cyber-defence and 60% have no insurance, and we need to do more.

● (1200)

Ms. Raquel Dancho: Thank you very much.

The Chair: Thank you.

Now I would like to invite Mr. Chiang to take his six-minute slot.

Sir, whenever you're ready, the floor is yours.

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

I thank the witnesses for your time today in providing us your expertise.

My question is for Mr. Doucet.

From your perspective, what are some of the largest cybersecurity threats facing Canada's national security related to Russia? What are some proactive steps that can be taken to avoid threats to Canada's national security and our critical infrastructure? What should Canada be prepared and able to do in the event of a large-scale cybersecurity attack from Russia?

Mr. Michael Doucet: Thank you for your question. There are quite a few elements to that question.

Number one, historically—or when I began my career in government—when we looked at these threats, we certainly looked to nation-states, to the Russian threat and so on. It was handled in government, but it was not as pervasive in the private sector. Today, that threat against Canadians is not only a national security concern for governments themselves, but also a national security concern for critical infrastructure. We know that most critical infrastructure is not owned by government and, in a lot of cases, not necessarily regulated by government.

The weakest link is sitting back and thinking you're okay by not having a program, by not measuring risk, whether you're a small, medium or large enterprise.

I enjoyed Jennifer's comments on small and medium-sized enterprises, but I'd also like to highlight that larger enterprises are potentially a more lucrative target for our attackers. Therefore, an advanced persistent threat, such as Russia's, or other state-sponsored threats, is really tough. We have to be 100% vigilant, not only internally to the organization but across our suppliers when we're thinking of third party threats as we're moving to different platforms and so on. It's very important.

Now, the million-dollar or potentially billion-dollar question is, really, what do we do about this? I'd like to highlight some work the National Security and Intelligence Committee of Parliamentarians put together and was tabled not very long ago. They had a framework and activities to defend systems and networks of government. It was tabled in February. It's an extensive report. It's worth reading. By the way, all of the recommendations were accepted.

It raises a couple of issues, one being—and this is a direct quote from the report—"Who is protected depends upon who you ask". We need to fix that, quite frankly. We need to fix that from both a responsibility and an accountability perspective, but we also need to fix "who do you ask?" That's really important to us.

Another quote is, "The threat posed by...gaps is clear." We know we have gaps. This is not an effort to blame people or organizations for gaps, but we know we have them and we must be diligent in closing them. We must be doing so in a programmatic way, where we're hitting the high-threat items.

Cybersecurity, in my opinion, is not about dollars spent, because you can spend immeasurable amounts of money on this; there's no question. Cybersecurity is, once again, about team sport and spending your dollars in the right areas that are going to have the best effect on government systems, on critical infrastructure systems or on shared systems.

Sir, does that help?

Mr. Paul Chiang: Thank you very much.

To follow up on your answer, should there be regulations to ensure cybersecurity in Canada, in terms of government regulations for government, for the private sector and the public sector? Do you think there should be regulation?

In your opinion, how would you suggest we close these gaps you mentioned?

● (1205)

Mr. Michael Doucet: We can talk about the responsibility for regulation.

My preference is not to overly regulate. Once again going to small and medium-sized businesses, do they have the resources to respond to regulation? It is potentially more of a supportive environment, communication environment. Whether you're a small or large organization, or a home owner with a network in your house, which we all have, there are immeasurable resources out there, from Public Safety Canada, RCMP and others, to help us secure our systems. For a small business, those can be very useful.

On closing the gaps, quite frankly, the gaps can be closed, but you need to understand them. You need to understand the gaps, the impacts of those gaps, and you need to understand who wants to do you harm.

I'll give you an example. If you look at the financial sector versus the agricultural sector, there may be different threat actors going after each one of those. The disruptive actors who just want to create disruption will go after anybody. You need to identify your gaps and you need to close them.

The bad news there is that the world is changing around you. The environment is changing around you as you're doing all of these things. If I assess a system today, or a system of systems, and I'm down a two-year road to close those gaps, which is not unreasonable, what other gaps are presenting themselves during that period of time, and how can I be relevant and move the program forward at all times?

The Chair: Thank you very much.

I would now like to invite Ms. Michaud for a six-minute block.

It's very good to see you back. I hope you're feeling better. Welcome.

[*Translation*]

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

I am happy to be back, even though my voice is still a bit hoarse.

I thank the witnesses for being with us today. It's really nice to see them in person.

Mr. Burton, you are clearly an expert on China. I will put some questions to you about that later.

In your opening remarks, you said that Canada was inadequately prepared to respond to security or cybersecurity threats and that it was less prepared than its allies.

What do you think explains that? Is it a lack of investments over the years?

What can we do to catch up?

Considering what is happening in Ukraine, is it too late or do we have enough time to prepare adequately?

[*English*]

Dr. Charles Burton: Compared to other countries, Canada has been less proactive in prosecuting or outing elements that have engaged in cyber-espionage. The United States has identified a number of agents of the Chinese People's Liberation Army who have been involved in this kind of activity.

We tend to be reluctant to engage, particularly with the Chinese, with regard to activities like cyber-espionage, suppression of Chinese language media or indeed harassment of people who might wish to speak out. They are harassed either by Chinese agents directly or through various kinds of harassments over the Internet.

This has been because our government has given priority to the promotion of prosperity in our relations with China and is prepared to tolerate these sorts of activities, because the cost to Canadian business and Canadian prosperity would be high.

The Chinese government has made it clear that if Canada does crack down on these sorts of activities of agents of the Chinese state in Canada or cyber-disruptions, we will lose business. You may recall the hack of NRC aerospace data or the earlier hack of the Treasury Board and other related government departments. From what I've heard, they were attributable to the Chinese state, but there have been no consequences to China for doing these sorts of activities.

It really is a question of political will, and it would be great if your committee could start to compare the policies of other like-minded countries, particularly the United States, the U.K. and Australia, with regard to this sort of activity. Our cyber situation is really so grave that, arguably, it looks like the Five Eyes is being reduced to three eyes.

When you look at the Quad, it doesn't include Canada. When you look at the Australia, U.K., and U.S. activity in the Indo-Pacific, to the best of my knowledge, the United Kingdom is not an Asia-Pacific country. Canada is, so why have the United States and Britain decided not to include us in the recent consultations between the United States and the U.K. on Taiwan, along with Japan? Part of our country is geographically closer to China than Australia. Why are we being excluded?

I think it's because we have not been pulling our weight in terms of addressing threats to public safety and national security, and our allies just don't see us as reliable partners anymore, along with New Zealand, which is for different reasons. I feel very sorry about this, but I do feel it is not too late. This is the Parliament of Canada. We can turn this around.

● (1210)

[*Translation*]

Ms. Kristina Michaud: You mentioned the United States, Australia and the United Kingdom.

Have other countries implemented best practices Canada could use for inspiration to protect critical infrastructure and prevent cyber-attacks?

[*English*]

Dr. Charles Burton: Yes, if you look at the United Kingdom last year, it expelled three spies posing as journalists working in the U.K. It revealed that there was an agent of the Chinese state, Christine Lee, who was giving generous donations to certain politicians who then, one presumes in response, would be representing the interests of China over the interests of their own country.

We've seen in the United States much more concern about the leak of high-tech technologies that would facilitate a dual-use military technology or technologies that would facilitate cyber-espionage out of universities. Canada has not responded to things like the Australian Strategic Policy Institute's report that revealed that there were researchers of the People's Liberation Army working in sensitive areas of high tech at Canadian universities. They had entered Canada under false pretences by not revealing their status as military officers, and it goes on.

Why didn't we do more about the Michael Chan matter in Ontario? CSIS said he had frequent contacts with the Chinese consul general, but we don't know what they were talking about. It's important for Parliament to know.

The Chair: Thank you very much.

I would now like to invite Mr. MacGregor to begin his six-minute slot.

Sir, the floor is yours.

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

I'll echo my colleagues' thank you to our witnesses for appearing before our committee and helping us with the course of this study.

Dr. Burton, I would like to start with you.

You had spoken in your opening remarks about the relationship between CSIS, the RCMP and CSE, and about the fact that the Parliament of Canada sometimes doesn't have a very good analysis of what those individual national security agencies are up to.

I want to put this in the context of the fact that the act that authorized the National Security and Intelligence Committee of Parliamentarians is due for a statutory review this year. I think that review lends itself to our current study because, as you said, we are woefully unprepared to meet many of the security threats.

Do you have any recommendations for what you would like to see that review cover? Is the current model of parliamentary oversight working? What would you like to see done differently? Are there any models, say, in the United States Congress or in the U.K. Parliament that we should be looking at as examples?

Dr. Charles Burton: The answer is yes. Particularly Australia, the U.K., the U.S. and also Scandinavian countries have a lot to teach us in terms of drawing the appropriate line between not revealing information that would be threatening to Canada's national security and where the security agency is not, in effect, protecting its own inadequacies in the performance of its duties as described in the mandates to the ministers that oversee them.

In Canada, I think we have far too much polite agreement with security agencies that say that they can't tell you this or that. I think it's a cultural issue. To some extent, frankly, I feel that they disdain parliamentary committees and do their best to tell you as little as possible for fear that if you find out something, it might reflect negatively on them or on past assessments that may not have been accurate.

I do think there needs to be more trust of parliamentarians to maintain secrecy. We need to be looking at the kinds of parliamentary or congressional committees that exist in other countries. We need to try our best to see if we can make Canadian committees more able to inform decisions about what legislation needs to be made based on a full understanding of what is going on.

I really don't think that in any other country the Cameron Ortis matter would be suppressed for so long, or that Quentin Huang, who was alleged to have transferred military technologies to the Chinese state—

● (1215)

Mr. Alistair MacGregor: I'm sorry to interrupt, Dr. Burton, but I have limited time and I want to get to Ms. Quaid.

Ms. Quaid, in your opening remarks, you made mention of the fact that cybercrimes pay and that cryptocurrency allows for easy payment. I'm sure you're aware that cryptocurrency has been a hot topic in Canadian politics over the last number of weeks.

Professor Robert Huebert appeared before our committee. He said that financial crimes in Canada are difficult to assess because there's a lack of transparency and visibility in financial transactions in Canada. In his view, more transparency is needed.

Do you have any specific recommendations you would like to see this committee make in the context of that remark and also in the context of cryptocurrency? What does the federal government need to be doing more of to include more transparency and visibility?

Ms. Jennifer Quaid: I would suggest that we start with the safe harbour legislation. Make it easier for organizations that have been attacked, through any of the methods, to not just report that they were attacked but to tell the world what happened. That creates transparency on the threat and helps other organizations. Echoing what Michael was saying, it's a team sport. If we are telling each other what has happened and how people got into our systems, it will prevent further attacks.

I think that is the easiest thing to do, the safe harbour legislation.

On the cryptocurrency side, you would have to really speak with the banks to find out. There is no transparency on cryptocurrency. That's the nature of it. Who has been paid what, by whom and when is very difficult to speak to.

Mr. Alistair MacGregor: Finally, Mr. Doucet, you made mention of the fact that cybersecurity is not about dollars spent. It's very much a team sport and there are resources.

With the increase for CSE announced in budget 2022—a significant chunk of money—what recommendations would you like to see our committee make on how that money should be spent? Are you satisfied with where it's being allocated? Do you want to see any more specifics? I'm interested in anything you can tell us.

Mr. Michael Doucet: Thank you for the questions.

On the amount of money that has been provided to CSE, I would look for specific outcomes in cybersecurity and in Canada—specific outcomes in the fields in which they play, which is just about everywhere in Canada.

The Chair: I'm sorry, sir. You have just 10 seconds left.

Mr. Michael Doucet: I think we want to be very outcomes-based on the spend. I also think we want to be very careful to build our organization for today's and tomorrow's threats, not last year's threats.

The Chair: Thank you very much.

Mr. Michael Doucet: Thank you.

The Chair: Colleagues, we now move into the second round of questions. We'll have enough time for each party. There will be four slots, and we'll begin with Mr. Van Popta.

Sir, you have five minutes whenever you're ready.

● (1220)

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

Thank you to the witnesses for being with us today and sharing their wisdom and knowledge.

Dr. Burton, I'll start with you.

In your testimony, and in response to an earlier question, you mentioned that the RCMP, CSIS and CSE, the Communications Security Establishment, have information, but they tend to stonewall us. You ask how we can prepare for threats as parliamentarians if they don't provide us with the information.

We've been told in Parliament that this is why we have the NSICOP—the National Security and Intelligence Committee of Parliamentarians. I wonder if you could comment on the efficacy of that committee.

Dr. Charles Burton: I'm of the opinion that it would be better if these matters were addressed through a committee of Parliament—people with security clearances—with perhaps some sessions held in camera, not publicly. I would rather see it as part of the regular parliamentary process. I'm not aware of any other country in the world that has anything comparable to our process, and I am concerned about whether it can be as effective as the committees of other parliaments in terms of ensuring that our public safety and national security agencies are being fully accountable to Parliament and that they are providing parliamentarians with the information they need to draft or change legislation to better meet the threats.

One example I can offer is our legislation on the transfer of classified technologies to agents of a foreign state. I have had the honour of working for the RCMP in preparing some cases on these. When the cases were sent to the Department of Justice—the two I know about—they were not acted on because our legislation is too weak and it was felt that the people alleged to have been traitors to our country by transferring classified technologies to agents of a foreign state would not be made accountable for it.

Our legislation does not compare favourably to that of other nations more successful in this. The British and the Americans are doing dozens of cases a year. When was the last time you heard of anybody prosecuted for this in Canada? To the best of my knowledge, never. This is a problem. It means we are considered a good sort of place for people who want to tap into our high tech through various legitimate or illegitimate means, and that just shouldn't be the Canada that we are.

Mr. Tako Van Popta: Thank you for that, Dr. Burton.

Mr. Doucet, I'm going to put the same question to you and see if you have a different perspective on the efficacy or the usefulness of the NSICOP as a replacement for other sorts of committees receiving reports.

Mr. Michael Doucet: Absolutely, and thank you. I was afraid you were going to ask me that question. I may give a bit of a different perspective on this, having spent most of my federal career within that community.

With all due respect, I wouldn't necessarily accuse the community of stonewalling. However, I would potentially accuse them of overclassifying information. I think this comes down to the culture and the culture of those organizations.

When I joined CSE on April 2, 1988, I wasn't allowed to tell my family how many people worked there. There were so many things that you.... You were behind that iron curtain. We had this...call it a cloak of secrecy or “need to know”. Call it what you want. The community needs to mature on that front.

If we are going to really engage critical infrastructure, critical infrastructure players can get security clearances. We can provide them with classified information. The government can do that. That is available. We need to declassify when we need to declassify. Having valuable threat information but not being able to act on it is not a good place to be. Those are my thoughts on that.

As it relates to the national security committee of parliamentarians, I can tell you that I personally did a happy dance when it was formed. I thought that was a tremendous step forward. It was good on us and good on Canada for doing that. Does it require some tweaking as it matures? Potentially, but it is a very good construct for Parliament.

The Chair: You have 10 seconds, sir. You're giving them back to the committee. Your generosity is warmly received.

We'll move right to Ms. Damoff.

You will have five minutes whenever you're ready to go.

● (1225)

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you so much, Chair.

Thank you to all our witnesses.

Dr. Burton, it's always lovely to see you, so thank you for being here today. You mentioned in your testimony about the relationship between China and North Korea. The isolation of Russia is not going to end any time soon. I think you mentioned, as well, that Russia and China will become even closer, and Russia will become dependent on China.

What recommendations would you have for the Canadian government to ensure that we're keeping our critical infrastructure safe as that relationship gets closer between Russia and China?

Dr. Charles Burton: I think we have done one good thing. I was very pleased with the government's budget with regard to critical minerals. As the situation develops, and as I believe that Russia will move more into alliance with China, it will be challenging for us to engage in secondary sanctions against China if China does with Russia what it's been doing with North Korea: facilitating the breaking of the sanctions that we are imposing on Russia to try to induce Russia to come into compliance with the norms of the international, rules-based order. It will be harder.

If the world is going to split into two camps of the autocracies and the countries that Russia and China are able to bring into alliance in various ways.... China has quite a successful ability to rally support in the UN from nations that have received benefits under their belt and road infrastructure program. If we're going to be in that kind of situation, it's important that we ensure our supply chains as a matter of national security, so that we cannot be subject to coercion by countries that will say, “We will give you the element that you need, but if you're not nice to us in complying with our political agenda in your country, we'll cut you off.” We saw that with the Chinese sanctions against canola seeds and meat at the time of the fiasco with Meng Wanzhou and the completely unjustified and brutal incarceration of Michael Kovrig and Michael Spavor.

We have to look at the situation seriously. We have to look at the CSIS assessments, which are critical for you to understand what Canada has to do. It's not going to be without cost. There's no point in our pretending that this is not happening, because it is, and we have to make the hard choices necessary to protect our nation and the other nations of our like-minded allies as a consequence.

Ms. Pam Damoff: Thank you, Dr. Burton.

Mr. Doucet and Ms. Quaid, the U.S. is looking at mandatory reporting for attacks on critical infrastructure sectors, and I'm wondering whether or not you think that Canada should look at that.

Before you answer, Mr. Doucet, you said you had a number of recommendations for the committee that you hoped you would get out in testimony. If you could provide those in writing if you don't provide them during your testimony, that would be great.

Maybe, Mr. Doucet, we could start with you.

Mr. Michael Doucet: Sure. I would certainly support mandatory reporting for select critical infrastructure players, and what I mean by that is when you look at the 10 sectors within critical infrastructure, they're very large, agriculture being one of them. Are we going to ask for mandatory reporting from a dairy farmer with 60 head of cattle? We need to approach that with caution.

That being said, if we are moving to a regime of mandatory reporting, we need to absolutely ensure that the reporting is safeguarded, that the source of that reporting is safeguarded, that the after actions on that reporting are safeguarded, and so on and so forth, and that we find a way to share that knowledge nationally, because the last thing we want to do is have organizations report on breaches and have that disseminated where we don't want it disseminated. When you aggregate all that information, that's a lot of information.

Ms. Pam Damoff: I only have about 20 seconds left. I'm sorry, Ms. Quaid.

Could you perhaps jump in there?

Ms. Jennifer Quaid: Absolutely. Mandatory reporting is a good concept. It certainly assists the government to understand the size of the threat, but if the information that we learn from that mandatory reporting is not disseminated to the greater economy to help it defend against the same threat, then really we're just going to be seeing the same thing happen over and over again. There's no point in—

● (1230)

The Chair: Thank you very much.

I now will invite Ms. Michaud to follow her line of questioning.

You have two and a half minutes. The floor is yours.

[*Translation*]

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

Mr. Doucet, we know that cyber-attacks have been on the rise over the past few years and that the situation has been exacerbated by the conflict in Ukraine. That is what the Canadian Security Intelligence Service has told us.

You talked about recommendations you would like to make to the government, not only to protect our government institutions, but also to protect private companies that may have a significant impact in Canada.

What recommendations could we make to the government?

[*English*]

Mr. Michael Doucet: The first recommendation would be to the government, as a player within critical infrastructure, to get it right, to take the series of reports on this subject and to tiger team those reports and look at how we're going to better protect the government infrastructure.

As I mentioned earlier, there was a report by the committee that was accepted very broadly. It covers 169 federal organizations. I think the first step would be to understand the threats that are prevalent in each one of those 169 organizations to ensure that they are reporting on those threats, identifying gaps and identifying how they're going to lower those gaps.

I think it's very difficult to go out to providers of critical infrastructure and tell them what they must do, if you're not doing it yourself. I think the funding, the teams and the people are there to accomplish this. Teaming across government departments is not always easy. They come with different cultures. They have different mandates, but I believe we really have to ensure that we can do so.

Number one would be for the government to get it right.

Then, of course, we need to look at how we are providing, how the government is providing, advice and guidance to critical infrastructure providers and others. I would really want to look at the number of organizations out there that are supporting cyber-environments, such as CCTX and others, and how can we harmonize that level of support to Canadians and Canadian infrastructure.

The reason I say that is there is a wealth of organizations. Some security officers are really looking at who they should talk to, amongst this wealth of organizations. Where will they get that valued information and who can be that trusted partner? Those are some of my recommendations.

The Chair: Thank you very much.

Mr. MacGregor, you will take us to the end of this panel. You have two and a half minutes, whenever you're ready, sir.

Mr. Alistair MacGregor: Thank you very much, Mr. Chair.

Mr. Doucet, I'd like to continue with you. You had made mention of agriculture. That's actually my other critic role. I know the technological advances in agriculture are going ahead at breakneck speed. There are many machines used in modern agriculture, precision agriculture. There is the use of blockchain technology. The machines now have the ability to communicate with the parent company, and farmers have access to real-time data not only on how their crops are growing but also on the correct applications of pesticides and fertilizers.

Continuing on with what you said to Madame Michaud, can you talk about some of the vulnerabilities that exist in Canada's agricultural fields? Maybe there are some recommendations that we can make with respect to that, because that is a massive part of our economy, and we have big plans to grow it. We are a major agricultural player on the world stage.

Mr. Michael Doucet: Absolutely. Thank you for that question.

Having a son in Saskatchewan, I really light up to the agricultural sector, because when you drive around rural Saskatchewan it's evident. It's evident when you're looking at modern-day farming.

I would say that modern-day agriculture on the scale that Canada is doing...and obviously you have a number of sensors out there. A farmer now is running operational technology as opposed to your traditional tractor and plow. There's data, there's critical data, and there is also data that, if manipulated, could really affect the outcomes of the farming operation.

Really, I think for the sophisticated Canadian farmer, you are partnering with the suppliers of agricultural goods and services. You're looking at what we refer to as third-party risk and how that could impact your organization, how that could impact your farm.

What do you look for? I believe you look for value. You look for asking exactly the questions you're asking of your suppliers. For large farmers, you look for potentially partnering with others who are going to help you make those decisions, because you are highly vulnerable from what we refer to as an operational technology perspective.

● (1235)

The Chair: Thank you very much. That takes us to the end of the panel and the end of our session. Again, you have our apologies for the late start. This is our world at the moment. We're very grateful for your wisdom and your commitment of time to this committee. It's very important work.

On behalf of all of Parliament, thank you very much for your testimony and for being a part of this democratic process.

Colleagues, it will be a very quick turnaround to the next panel. I'm told by the clerk it's even less than five minutes. I'll see you very soon.

● (1235)

_____(Pause)_____

● (1240)

The Chair: We are ready to go. We will organize our rounds the same way we did with the first number of witnesses, with a full round and then the first four of the second round.

I'm very happy to call the meeting back to order. In this second hour we will hear from Dr. Frédéric Cuppens, professor, Polytechnique Montréal; Dr. Nora Cuppens, professor, Polytechnique Montréal; and Dr. Jonathan Paquin, full professor, department of political science, Université Laval, for up to five minutes of opening comments each.

We can get started right away. I will ask Dr. Cuppens to begin. You might ask, which one. How about Dr. Frédéric Cuppens with a five-minute opening statement?

Go ahead, whenever you're ready.

[*Translation*]

Dr. Frédéric Cuppens (Professor, Polytechnique Montréal, As an Individual): Ms. Cuppens will begin.

Dr. Nora Cuppens (Professor, Polytechnique Montréal, As an Individual): Good afternoon, everyone.

I will begin, as my colleague Frédéric Cuppens and I prepared a shared presentation.

Thank you all for inviting us to appear before this committee. I will provide some context, and Mr. Cuppens will give you a few recommendations.

We all know what the context is. On the one hand, there is the Russian Federation's invasion of Ukraine and, on the other hand, there is the assistance provided by western countries and the North Atlantic Treaty Organization, or NATO, to Ukrainians to deal with this invasion. We are now wondering whether we should worry about reprisal through cyber-attacks. In other words, will the war on the ground shift into cyberspace?

Russia has shown its ability to engage in cyberwarfare with highly organized cyber-attack groups. We know about and have identified a number of them. There is APT28, which carried out a cyber-attack on TV5 Monde, APT29, another mostly Russian organization, known for its interference in the 2016 U.S. election, the 74455 Russian military intelligence unit, which carried out cyber-attacks on critical infrastructure using BlackEnergy and Industroyer software, as well as the Conti group, which is known for its affiliation with the Ryuk ransomware.

We want to remind you that, well before the military attack against Ukraine, tensions between the United States and Russia were extremely high. Following the attack on the SolarWinds company, President Biden called President Putin a killer. He has used other terms to describe him since. Therefore, Russian cyber-attacks may multiply and intensify, targeting especially those who are helping Ukrainians, such as western countries, including Canada. What are the targets and the threats? That is the question we are asking ourselves. This cyberwarfare can take very diverse forms, with the most well-known being data exfiltration, denial of service attacks, fraud and, of course, sabotage.

The most visible form of cyberwarfare today is information warfare, consisting of disinformation. We should expect this information warfare to continue and fake news to proliferate. However, a number of experts agree that the impact of those cyber-attacks is limited for the time being. Shortly after the conflict in Ukraine began, the Conti group, which I mentioned earlier, claimed responsibility for the cyber-attack on the Alouette aluminum smelter, which you have probably heard about. Last week, there was also the attack on Rideau Hall, which had a very symbolic impact, but for the time being, Russia's involvement in that attack has not really been confirmed.

We may ask ourselves the following question: why hasn't Russia launched any major cyber-attacks yet?

We don't have an answer, but we can make two assumptions. The first is that, like a traditional war, a cyber war has to be prepared for. We have seen that the preparation on the ground is somewhat chaotic. Russia may not have prepared for a cyber war, or it may be waiting for the right moment to launch it. The second assumption is that either of the two camps starting a massive cyber-attack would without a doubt be seen as a crossing of the famous red line, which would inevitably lead to conflict escalation.

Therefore, critical infrastructure is a priority. We may worry specifically about attacks sabotaging that infrastructure. It goes without saying that our geographic distance is irrelevant when it comes to cyber threats. Some experts have not hesitated to compare cyber weapons to nuclear weapons as a deterrent, comparing the power of cyber-attacks to the power an atomic bomb could have.

In this context, two untruths that are often spread can be highlighted. The first is that infrastructure that is not connected to the Internet is protected from cyber-attacks through what is generally referred to as physical isolation. That is false, and we have known it full well since the Stuxnet worm attacks, which targeted nuclear power plants.

The second untruth is a *Die Hard 4* liquidation scenario, whose objective would be to destroy a country's economy—

● (1245)

The Chair: You have 10 seconds left.

Dr. Nora Cuppens: Okay.

That's a movie, but it is also false. So all the steps of the scenario are possible and feasible.

[*English*]

The Chair: Thank you very much.

[*Translation*]

Dr. Nora Cuppens: I now yield the floor to Mr. Cuppens, who will present our recommendations.

[*English*]

The Chair: Thank you.

I now would like to invite Dr. Frédéric Cuppens to give us an opening statement of up to five minutes.

Sir, whenever you're ready, the floor is yours.

[*Translation*]

Dr. Frédéric Cuppens: A liquidation scenario like the one in the movie is unfortunately entirely possible. We are talking about attacks on road traffic, air traffic, telecommunications systems, the media, power distribution systems, financial systems, the stock market. There are already examples around the world illustrating the possibility of those cyber-attacks. We think it is just a matter of preparation and means to unleash those types of large-scale attacks. Naturally, it is complicated for isolated individuals, but it unfortunately becomes entirely possible at country level.

We have some recommendations in that context. There are of course basic recommendations. The first recommendation is to stop using software from Russia, especially security software. A number of countries have already recommended that a famous Russian antivirus developer no longer be used.

According to the second assumption, cyber-attacks can come from anywhere in the world, not only from Russia. For example, it was recently shown that the Conti group was led by a 12-year-old girl living in Mans, France.

It is also absolutely necessary to raise the overall security level across Canada. That goes through the general mobilization of all resources to be able to address cyber-attacks and urgent needs in terms of federating and coordinating cybersecurity expertise in industry, academia and government.

We also suggest that the sovereign power take over anything related to the cybersecurity of critical infrastructure. That is what a number of countries have done, and that is what France did with its Military Programming Law 2019-2025.

At Polythechnique, our efforts are focused both on research and on education. When it comes to education, it is extremely important to develop a program for basic education—bachelor's and master's degrees—but also for continuing education by establishing certificates and micro-programs, as well as a professional development program for short one to five day training.

Concerning research, we really believe there is a need to expand the work on cyber weapons as a deterrent. That goes through the development of solutions to meet the needs I will list on a priority basis.

First, there is attribution, the ability to find the true source of an attack. This is not a trivial problem; attribution is a key problem if we want to develop a doctrine for using cyber weapons.

Second, there is the internal threat. A lot of work today is focused on detecting and protecting against external threats. However, a large-scale cyber-attack, like the one we just brought up, will very likely require internal relays in the infrastructure targeted by the attack. So it is very important to develop solutions for monitoring internal threads to manage not only cases of malicious intent, but also cases of negligence. Unfortunately, internal threats are often related to negligence.

Third, parameters for measuring the real impact of a cyber-attack scenario are absolutely necessary to develop a cyber deterrence doctrine in line with the principles of response proportionality.

Fourth, there is cyber resilience, the ability to resist cyber-attacks. Polytechnique has worked on a number of critical sectors, such as finance, the supply chain, defence, the marine sector and aerospace.

In closing, I would say that, to meet those various needs, one of our priorities is the development of tailored solutions based in particular on artificial intelligence.

Thank you for your attention.

● (1250)

[*English*]

The Chair: Thank you very much.

I would now like to invite Dr. Paquin to give us up to five minutes of opening comments.

Go ahead, sir, whenever you're ready.

[*Translation*]

Dr. Jonathan Paquin (Full Professor, Department of Political Science, Université Laval, As an Individual): Ladies and gentlemen committee members, it is a privilege and an honour to testify before you today.

Evidence suggests that Moscow is a threat to our country's security. Over the past 15 years, Russia has carried out cyber-attacks on critical infrastructure of countries that are hostile to its interests. Since Canada is currently very hostile to Moscow's interests, it is potentially a prime target for the Kremlin. Russia's Minister of Foreign Affairs Sergey Lavrov recently told Italian media that Americans and especially Canadians played a leading role in preparing ultra-radical, openly neo-Nazi subdivisions for Ukraine. That says a lot about how the Russians see our role in the conflict.

Moscow funds information manipulation, or disinformation, campaigns against democratic institutions in the west. Its objective is clear, as it has been said over and over again, and it is to misinform and divide our fellow citizens in order to weaken our democratic institutions. Those activities have been well documented in recent years.

Since the invasion of Ukraine began, Putin's regime has repeatedly threatened to use tactical or strategic nuclear weapons because it feels that NATO is engaging in a proxy war against Russia.

As a result, since February 24, we have had to be very aware of various threats to our security. Our vigilance must be even greater now that western countries have expanded their objectives in the Ukrainian conflict and have openly sought to degrade Russia's capabilities. That more offensive posture has been contributing to escalating tensions with Russia. Since Canada is fully on board with that, the Kremlin is becoming a growing threat to our security.

I think the best security measure Canada should have with regard to Russia is a combination of deterrence through retaliation, which is possible, considering article 5 of the North Atlantic Treaty, the legal basis of an organization whose member Canada has been for many years, and deterrence through denial—in other words, cyber resilience—through education on disinformation and renewed continental defence.

I also feel that the principal threat to Canada are cyber-attacks on our critical infrastructure. The Government of Canada must increase its investments to enhance the security of that infrastructure and to make us even more resilient to Russian attacks. The idea is to discourage the Kremlin from carrying out such attacks because it would know that the probability of success is low. That is deterrence by denial.

As for Moscow's information manipulation campaigns, their impact is less immediate and more diffuse than that of cyber-attacks. I am of the opinion that Canada is pretty well-equipped to deal with that disinformation because it is relatively invulnerable. It would be my pleasure to elaborate on this.

Finally, despite Putin's alarming statements, Russia's use of weapons of mass destruction carries a lower risk for Canada then cyber-attacks. Nevertheless, since the progress of the war in Ukraine is unpredictable, the Canadian government has a responsibility to invest more in modernizing command and control through the North American Aerospace Defence Command, or NORAD. We must have an excellent monitoring system to quickly detect Russian missiles and, more importantly, hypersonic missiles. The Minister of National Defence has already talked about this, and announcements should be made soon, which is a very good sign.

I think it is also time to reconsider our participation in the North American missile shield, as Washington is not required to defend Canada in case of Russian missile attacks.

I will stop here, but I will do my best to answer your questions.

● (1255)

[*English*]

The Chair: Thank you very much.

We now will move to a full round of questions. We will begin with a six-minute slot from Mr. Lloyd.

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

Thank you to the witnesses for coming out today.

My first question will be for Dr. Nora Cuppens.

Something you said really piqued my interest. You said that the Russians had claimed a cyber-attack on Rideau Hall, but that you can't confirm at this time whether they were actually behind the attack.

Do you believe that the Russians will sometimes claim responsibility for attacks they don't actually carry out in order to sow confusion in Canada?

[*Translation*]

Dr. Nora Cuppens: Thank you for the question.

Attribution is a big problem because it isn't easy to trace the source. These groups of attackers, even if they are identified and even if we manage to find out who they are, rarely claim responsibility for their actions. When they do, they try to provoke. When they decide to claim responsibility for their actions, they expect a reaction. In terms of the attack on Rideau Hall, they won't claim responsibility, but they leave enough doubt that it is assumed to have come from there. We have to be careful when it comes to this type of attack.

● (1300)

[*English*]

Mr. Dane Lloyd: With what you're saying—and what I'm trying to confirm—do you think that the Russians, in order to create disinformation, fear and confusion, will sometimes claim responsibility for attacks even if they weren't involved in the attack? Is that a form of disinformation that we need to watch out for?

Do we just take it at face value when they say that they've done an attack, or is it still important to do an attribution to confirm whether or not they are indeed the source of the attack?

[*Translation*]

Dr. Nora Cuppens: It's the same thing for the terrorist attacks. As soon as there's an attack, the terrorists claim it, whether it's linked to their movement or not. I think I've answered your question, but I will answer it more positively.

Yes, they can claim responsibility for an attack or make it appear that they are behind this or that attack, precisely to create fear. They want to send the message that if we do something, they can do something in response that will have a very significant impact. This attack is an example, even though it wasn't the Russians behind it. As you just said, this creates a climate of fear. It's said that you can have a significant impact through a reaction or a cyber-attack.

[*English*]

Mr. Dane Lloyd: Thank you for that.

Dr. Frédéric Cuppens, one of the things that seem to be a strategic strength in western democracies are a strong ecosystem in the information technology sector, which I would hope would carry over into both cyber-offensive capabilities and cyber-defensive capabilities.

What are some recommendations that you would make so that Canada can maintain and build upon its strategic strengths in these areas? Is it more investment in education, in terms of developing engineers who are capable of building this infrastructure? Is it a tax credit to encourage the private sector to invest in cybersecurity capabilities in Canada?

What are your recommendations on what the government could do to facilitate a strong private-public sector response and an ecosystem for cybersecurity?

[*Translation*]

Dr. Frédéric Cuppens: The first recommendation relates to information, which is indeed a central element. More expert engineers need to be trained in cybersecurity, whether it's for protection, detection or the use of more offensive weapons. As part of our research, we are working more on defensive postures. We talked about cyber-resilience and solutions for detecting internal threats. It is indeed—

[*English*]

The Chair: I'm sorry, sir, but could you please move your microphone down closer to your mouth?

Yes, that's probably better.

[*Translation*]

Dr. Frédéric Cuppens: We are working more on defensive posture to build cyber-resilience and develop tools to detect external and internal threats. To work on that, you have to—

[*English*]

Mr. Dane Lloyd: I'm sorry to interrupt. Since I have only a minute left, could you please follow up with a written submission with your recommendations? I'd appreciate that.

My final question is this. There was a pipeline outage in the United States in the past couple of years. I believe it was the continental pipeline. It completely blew up the energy infrastructure, and gas prices were going through the roof. We're in a time of high inflation right now. Oil supplies and energy supplies are very tight.

What can the government do to strengthen our energy transportation infrastructure to protect it from a similar attack?

[*Translation*]

Dr. Frédéric Cuppens: I don't know who the question is for.

[*English*]

The Chair: Whom was it directed to?

Mr. Dane Lloyd: That was to Mr. Cuppens.

The Chair: Dr. Cuppens, unfortunately you have only 10 seconds to answer.

● (1305)

[*Translation*]

Dr. Frédéric Cuppens: When it comes to transportation, the key is to work on the supply chain, which is done using multimodal transportation. In fact, vulnerabilities tend to occur at the border of two modes of transportation, for example, from marine to rail or rail to road. It's at these stages of transition in the multimodal transport chain that vulnerabilities are found, and it's these that need to be addressed as a priority.

[*English*]

The Chair: Thank you very much.

Mr. McKinnon, it's over to you now for a six-minute round. Begin whenever you're ready, sir.

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

I'm going to start with Dr. Paquin. You made a remark about NATO and article 5 that I'd like to clarify. It seems to me—perhaps I heard you incorrectly—that you said article 5 could be used to justify a response to an attack on us. My understanding of article 5 is not that it would justify a response by us for an attack on us, but it would require us to respond to an attack on one of the other NATO members.

Are you suggesting that, by a cyber-attack on one of our NATO allies, we would be required to respond via article 5?

[*Translation*]

Dr. Jonathan Paquin: That's a very important question.

There is growing concern within NATO about the consequences of cyber-attacks, because we know that cyber-attacks can be significant. Indeed, under NATO's growing position, a large-scale cyber-attack within a country against its facilities or critical infrastructure could be considered an attack against one of the members of the organization.

Furthermore, article 5 of the North Atlantic Treaty does not provide that all members of the alliance will automatically enter into a military confrontation against the state that has perpetrated the threat. Rather, it provides that each member will be responsible for taking whatever means are deemed appropriate to assist the state that is the victim of a cyber-attack.

The main problem with cyber-attacks and NATO is attribution, as my colleagues Dr. Nora Cuppens and Dr. Frédéric Cuppens mentioned. That means being able to prove beyond a shadow of a doubt that a major cyber-attack was perpetrated by the Kremlin, for example, in Canada, by the government, and not by hackers who act autonomously or independently on Russian territory. This is not an easy thing to prove.

It could have the effect of causing member states to debate whether that's really the case, and therefore loses much of its relevance.

[*English*]

Mr. Ron McKinnon: Thank you, Dr. Paquin.

I'm going to switch now to Dr. Nora Cuppens. Some of our previous witnesses have identified that one problem in Canada is the lack of a central agency to coordinate and manage, across our society, possible attacks. CSE has a very narrow role in that respect.

Is that a role that CSE should be undertaking, or do you have any comments on the fundamental premise?

[*Translation*]

Dr. Nora Cuppens: Thank you for the question.

I come from Europe, and it's true that in France, in particular, there is the Agence nationale de la sécurité des systèmes d'information, which plays an observatory role as well as a sovereign role, as Dr. Frédéric Cuppens mentioned earlier. So we need a similar institution that would operationalize, if you will, the protection of our systems and infrastructure. It could be the Communications Security Establishment.

We have all kinds of rules on computer hygiene and rules that tell us how to protect ourselves or react to attacks, but there is no obligation to enforce these rules on protection, detection and response to intrusions. It seems to me that establishing such an institution that would play a role as a cyber-surveillance and observatory, that would push for regulation and verify that the rules are being applied, is of paramount importance to ensure that we are moving in the right direction.

Some might say that it's complicated for small- and medium-sized businesses to apply certain rules. However, they could be associated with an entity that is conducting cyber-surveillance to help them gradually acquire that protection. We talked about the supply chain earlier. Attacks aren't directed at entities head-on; they always come from third parties, particularly in the supply chain. So they tend to be the least secure entities.

● (1310)

[*English*]

Mr. Ron McKinnon: You mentioned, of course, small enterprises and so forth. For the dairy farmer or the garage down the street, they are connected to the Internet and they're possibly either vulnerable themselves or perhaps a gateway to someone else's vulnerability. This kind of protection, the detection of an attack, is a very specialized and arcane skill set.

How are those kinds of companies and organizations going to protect themselves and, therefore, the network from attack?

[*Translation*]

Dr. Nora Cuppens: I can answer the question in two ways. The first is a classic answer that everyone is familiar with—

[*English*]

The Chair: I'm sorry. There are two ways, but only 10 seconds.

[*Translation*]

Dr. Nora Cuppens: It involves taking action on cyber hygiene.

The second is outsourcing. When you don't know how to do it, you ask for help from experts. The approach is to outsource that work to entities that know how to do it. The company is then an entry point.

[*English*]

The Chair: Thank you.

Madame Michaud, we now turn to you for six minutes.

[*Translation*]

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

I'd like to thank the witnesses for accepting our invitation to appear before the committee.

Dr. Paquin, I suspect you were my professor at Laval University in another life. You taught me a lot about American foreign policy, and I'm sure that your expertise on Canadian security, among other things, will be of great benefit to the committee.

At the beginning of the conflict in Ukraine, you mentioned that since World War II, there has been a desperate desire to avoid a conflict between two nuclear superpowers, and that's why western powers didn't want to go beyond economic sanctions, for example.

How might Russia react to these economic sanctions, and how should Canada prepare?

Do you think Canada is sufficiently prepared for any kind of attack?

Dr. Jonathan Paquin: Thank you for the question, Ms. Michaud. It's a pleasure to see you again in a context other than academia.

To answer your question, I would say that it's very important for Canada to do everything in its power to limit the conflict in Ukraine to Ukrainian territory. As long as we focus on economic sanctions and remember that our goal is to help Ukrainians liberate their territory in the name of international law and liberal values, things will work out relatively well, in my view.

The problem I see is that in the last week or two a new Western strategy has emerged in relation to Ukraine. The goal is no longer just to help Ukrainians defend themselves, it's also to weaken Russia.

Canada's Deputy Prime Minister and Minister of Finance Chrystia Freeland said when she tabled the federal budget on April 7 that democracies, including Canada, would only be free when the Russian tyrant was defeated.

Of course, we can see this kind of rhetoric as being legitimate, but the signal it sends is that our strategy is not to liberate Ukraine, but that we really have taken a more offensive strategy focused on weakening Russia. This could lead Russia to counterattack. We know that Russia feels humiliated and that is certainly true for a number of reasons with regard to President Putin, and it has been for at least 30 years. Because of our actions in Ukraine, including the delivery of heavy artillery—and that's what Canada is doing right now with its allies—if Russia were to lose the war or if Russia were unable to win in eastern and Southern Ukraine, it's a safe bet that there will be retaliation and that, essentially, the Russians will not maintain the status quo.

I think there could be cyber-attacks, not against small or medium-sized businesses, which are not integrated, as it were, into large value chains, but rather on critical infrastructure. That's why I feel governments absolutely must increase investment not only to secure Canada's digital space, but also to increase coordination with key Canadian businesses, provinces and territories as well as our key partners, including the United States and the United Kingdom.

● (1315)

Ms. Kristina Michaud: Thank you very much.

You touched on a pretty important point in your opening remarks when you spoke of Canada's role in this conflict and the perception of that role.

We know that China and India, in particular, have not denounced the Russian invasion of Ukraine.

What impact might this diffusion of Russian perception have on other world powers in terms of Canada's role? In what ways do you feel this could come to throw the world order off kilter?

Are we safe from this kind of global disinformation campaign?

Dr. Jonathan Paquin: Thank you for the question.

Before February 24, many observers wondered whether Western countries, including Canada, were willing to go far enough to defend the values they hold. Many doubted it. President Putin and Chinese President Xi Jinping doubted it.

In my view, the situation in Ukraine shows that Western countries, Canada and other NATO members in particular, are able to be more cohesive in terms of their actions as well as their cooperation when danger is in the air, in a sense. That's important. This is a decisive moment because the message we're sending to countries like China, in relation to Taiwan, is that we're ready to do whatever it takes, that we are even ready to wage a proxy war to defend our allies, our democratic partners. The Canadian government's message is very clear. Canada's approach is quite dichotomous, if not Manichean, when it comes to good democracies versus autocracies, which are not good.

Canada has a very clear position on this situation. That's not always been the case. For a long time people wondered where Canada stood.

[*English*]

The Chair: You have 10 seconds, please.

[*Translation*]

Dr. Jonathan Paquin: Canada was struggling to move forward with clear and assertive positions. Now it's made its bed, and the world knows where Canada stands on these issues.

[*English*]

The Chair: Thank you very much.

Mr. MacGregor, the last slice of this round goes to you. You have six minutes, sir, whenever you're ready.

Mr. Alistair MacGregor: Thank you very much, Mr. Chair.

Thank you to all of our witnesses for helping guide our committee through this study.

Dr. Nora Cuppens, I would like to start with you.

In your opening remarks, you were talking about the information war that exists and Russia's responsibility in that. Here in Canada, during the month of February, we noticed a switch at the end of that month from a lot of groups that were involved in anti-vaccine protests. Suddenly, with the war beginning in Ukraine, there was a noticeable shift to a pro-Russian stance. They started echoing Russian propaganda and really trying to promote that. It was almost overnight from the beginning of the war in Ukraine.

Dr. Nora Cuppens, what can we learn from that?

I guess it speaks to the level of Russian involvement in developing that misinformation and spreading misinformation in Canada. I think many of us rightly perceive that as a threat to our democracy, if we can't even agree on a common set of facts.

Moreover, what programs and policies can the federal government effectively enact to combat that when we have a state actor that is very hostile to Canada's interests meddling in our internal affairs and exploiting those divisions in our democracy?

● (1320)

[*Translation*]

Dr. Nora Cuppens: Thank you for the question.

It's true that we keep coming back to this issue, which all three of us have brought since the beginning of this meeting: the attribution aspect.

In our cybersecurity efforts, we often correlate to try to see if there is an intrusion or an attack going on, what the target is, and what the security objective is. The reasoning is the same. It starts in cyberspace and ends up in the everyday space on the ground, therefore protests and so on.

So it's hard to say whether the motivations or reasons that led to the protests are necessarily related to the Kremlin, the Russians or other such events. There are also isolated initiatives, even pro-Russian ones, where people personally take action to help move things in Russia's direction.

It's not easy to determine whether it was a Russian initiative that led to protests like these. It's also difficult to correlate when the Russian invasion started on February 24 to some events that happened on the ground in connection with the protests or with attacks on energy sector infrastructure in Ukraine, operators or satellites, because we mustn't forget the space element.

We are looking into this issue, and we haven't yet found the answer when it comes to this attribution aspect, which allows for investigations. Once we determine attribution, that will bring in other legal aspects and responsibilities—

[*English*]

Mr. Alistair MacGregor: Thank you, Dr. Cuppens.

I'm sorry to interrupt, but I only have two minutes left. I want to get to Dr. Frédéric Cuppens.

Sir, you mentioned France's cybersecurity law. I think you're referencing the critical infrastructure information protection. France has identified 12 sectors, which include food, health, water, telecom and broadcasting, space and research, industry, energy, transport, finance, civilian administration, military activities and justice. You used that as an example. Canada needs to take the lead at the federal level on establishing cybersecurity.

What kind of recommendation would you, sir, like to see this committee make to the federal government? Would you like to see us take the France model and introduce federal legislation here to really have that basic level of requirement across those sectors?

If you could elaborate on that, it would be helpful, sir.

[*Translation*]

Dr. Frédéric Cuppens: I don't have the answer to the last part of the question.

Having said that, there are indeed some great things about the proposed approach in the Military Programming Act 2019-2025, including the concept of operators of vital importance, or OVIs.

In France, once it has been designated as an OVI, a company whose activities are related to a critical sector is required to meet a certain number of obligations to comply with the military programming law. This isn't a spontaneous declaration by the company; it's a requirement imposed by the state once the company has been designated as an OVI. This naturally applies to large companies, but it also includes small or medium-sized ones if they engage in activities related to a critical sector.

[*English*]

The Chair: You have 10 seconds.

[*Translation*]

Dr. Frédéric Cuppens: With respect to the security of activities of vital importance, or SAVI, each sector reports to a government department. It's the department's responsibility to ensure that all the OVIs in its purview remain in compliance with the law.

[*English*]

The Chair: Thank you very much.

Colleagues, we're now within three or four minutes of the end of our time. We don't have time to go into another round. Some of us have a hard stop within two minutes from now. I would like to thank the witnesses and to apologize for the rushed nature of the discussion. It's because of a vote that was required at the beginning of this session. I apologize for that.

On behalf of all members of the committee, I want to thank those of you who have come today for your experience, your expertise and your wisdom in shedding light on such an important part of Canadian public policy.

Thank you for all of your contributions.

Colleagues, we'll see you on Thursday. This meeting is adjourned.