HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

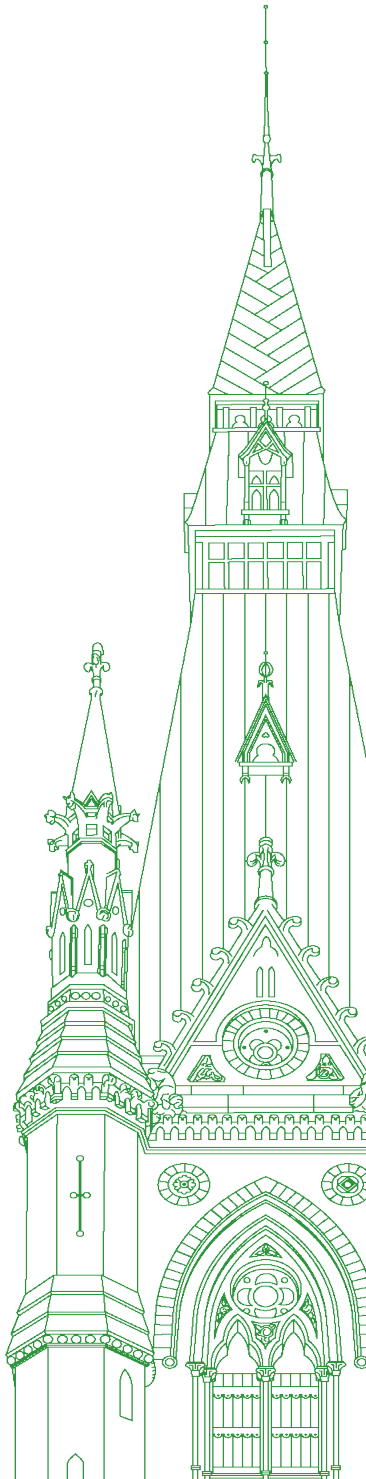
44th PARLIAMENT, 1st SESSION

Standing Committee on Transport, Infrastructure and Communities

EVIDENCE

NUMBER 009

Thursday, March 24, 2022



Chair: Mr. Peter Schiefke

Standing Committee on Transport, Infrastructure and Communities

Thursday, March 24, 2022

● (1530)

[*Translation*]

The Chair (Mr. Peter Schiefke (Vaudreuil—Soulanges, Lib.)): I call this meeting to order.

Welcome to meeting No. 9 of the House of Commons Standing Committee on Transport, Infrastructure and Communities.

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.

I would like to take this opportunity to remind all participants in this meeting that screenshots or taking photos of your screen is not permitted.

Given the ongoing pandemic situation, I encourage all committee members and witnesses to follow the recommendations of the health authorities, as well as the Board of Internal Economy directive of January 28, 2022.

[*English*]

As chair, I will be enforcing these measures as best I can for the duration of the meeting, and I thank members in advance for their co-operation.

Pursuant to Standing Order 108(2) and the motion adopted by the committee on Thursday, March 3, 2022, the committee is meeting to study Canada's preparedness to respond to Russian threats to Canadian waters, ports and airspace.

Colleagues, appearing before us today we have from the Canada Border Services Agency, Denis Vinette, vice-president, travellers branch; from the Communications Security Establishment, Rajiv Gupta, associate head, Canadian Centre for Cyber Security; and from the Department of Public Safety and Emergency Preparedness, Ryan Schwartz, acting director general, critical infrastructure directorate, national and cybersecurity branch.

For the second part of our meeting, we have from BlackBerry, Dr. John de Boer, senior director, government affairs and public policy, Canada.

I would like to welcome all of our witnesses to the committee today. Thank you for your time.

I will turn the floor over to our witnesses for their opening remarks.

Mr. Denis Vinette, the floor is yours.

Mr. Denis Vinette (Vice-President, Travellers Branch, Canada Border Services Agency): Thank you, and good afternoon to all of you.

[*Translation*]

Good afternoon Mr. Chair, and members of the Standing Committee on Transport, Infrastructure and Communities.

Thank you for inviting me to participate in the discussion today.

I am pleased to be here to answer your questions about the role of the Canada Border Services Agency, or CBSA, with respect to the arrival of Ukrainian nationals in Canada and sanctions against Russia.

The CBSA is responsible to facilitate the flow of legitimate travel and trade into Canada. Its role is to assess the security risk and admissibility of persons coming to Canada. All persons, including Canadian citizens, seeking entry to Canada must present to the CBSA and may be subject to a more indepth exam. Admissibility of all travellers is decided on a case-by-case basis and based on the information made available at the time of entry.

The CBSA is committed to protecting the health and safety of Canadians and will examine, detain or seize goods entering Canada if they pose a health, safety or security risk.

Further and beyond the screening of travellers, the CBSA also uses a number of automated advance information sources from carriers and importers to identify goods and conveyances that may pose a threat to Canada.

The Agency uses a risk-management approach to facilitate legitimate trade while focusing on higher or unknown risks. This approach involves screening goods at several points along the trade continuum: at the earliest opportunity overseas, in transit, and upon arrival at the Canadian border.

● (1535)

[*English*]

The agency's focus is on getting the right information at the right time in order to know when, where and how to target its enforcement efforts. CBSA targeting officers work in collaboration with border services officers who are trained in examination, investigative and questioning techniques. Together they are the agency's greatest assets when it comes to identifying, detecting and intercepting contraband or other goods at the border.

As it pertains to commercial sanctions, the CBSA is supporting the whole-of-government response to the Russian invasion of Ukraine and is assisting Global Affairs Canada in the administration of the Special Economic Measures Act, the United Nations Act, the Justice for Victims of Corrupt Foreign Officials Act, the Export and Import Permits Act and other associated regulations at the border.

The CBSA is also an active partner in the marine security operations centres and supports Transport Canada with relevant and timely customs information.

The CBSA works closely with the RCMP to deliver the broad range of border services with the CBSA mandate focused on delivering services at ports of entry.

Border services officers also review import and export documents, including bills of lading, invoices and certificates of origin to determine if the goods or shipments and transactions are subject to sanctions or control measures. Shipments that appear to be in contravention of the legislation, regulations or sanctions are detained and referred to Global Affairs for further assessment. Upon direction from Global Affairs, the CBSA may detain the shipment or seize it to make sure that all the applicable regulations and sanctions are applied at ports of entry.

The CBSA also conducts risk assessments on travellers and goods seeking entry to the country. We work with our partners in the intelligence sector to conduct security screening on foreign nationals seeking entry to the country. Both the screening and risk assessment processes include the collection and analysis of information from a variety of sources and partners to determine the admissibility and the risk.

The agency also regularly shares, under strict legal parameters, relevant information on border and national security issues to our partners, as well as other government departments in Canada to ensure the health, safety and security of Canadians.

All goods, conveyances and people may be subject to an in-depth exam. The CBSA risk assesses 100% of all vessels and their cargo in order to identify potentially higher-risk vessels and the goods they are carrying.

Our officers exercise their professional judgment in a highly complex environment and are well supported in their training to apply these measures. We further work closely with other partners, including Transport Canada and the RCMP, to ensure that security and sanctions are applied appropriately.

I will be happy to answer questions from committee members.

[*Translation*]

Thank you.

[*English*]

The Chair: Thank you very much, Mr. Vinette.

Next we have Mr. Gupta.

Mr. Gupta, you have five minutes for your opening remarks. The floor is yours.

[*Translation*]

Mr. Rajiv Gupta (Associate Head, Canadian Centre for Cyber Security, Communications Security Establishment): Good afternoon.

Thank you, Mr. Chair and members of the committee for the invitation to appear today to discuss Canada’s preparedness to respond to Russian threats to Canadian waters, ports and airspace.

[*English*]

My name is Rajiv Gupta and I am the associate head of the Communications Security Establishment's Canadian Centre for Cyber Security, which we more commonly refer to as the cyber centre.

CSE, reporting to the Minister of National Defence, is one of Canada's key intelligence agencies and the country's lead technical authority for cybersecurity. The cyber centre is a branch within CSE and a single point of expertise on technical and operational cybersecurity matters. We defend the Government of Canada, share best practices to prevent compromise, manage and coordinate incidents of importance and work to enable a secure digital Canada.

Canadian cyber systems inside and outside of government hold information and personal data that is critical to Canada's prosperity, security and democracy. Canadian cyber systems are also essential to critical infrastructure operations. It is critical that these systems are protected, and I can assure you that CSE and its cyber centre recognize this importance.

While I can't speak to our specific operations in this setting, I can confirm that we have been tracking cyber-threat activity associated with the current Russian invasion of Ukraine. We know that Russia has significant cyber capabilities and a demonstrated history of using them irresponsibly. The NotPetya destructive malware of 2017 is an example of this behaviour and illustrates how a cyber-attack on Ukraine can have international consequences.

As the situation evolves, CSE continues to monitor the cyber-threat environment in Canada and globally, including cyber-threat activity directed at critical infrastructure networks and operational and information technology systems.

For Government of Canada networks, we have the tools in place to monitor, detect and investigate potential threats and to take active measures to protect and defend against them. For Canada, we have issued unclassified threat bulletins urging Canadian critical infrastructure operators to be aware of the risks and to implement mitigations against known Russian-backed cyber-threat activity.

We strongly encourage all Canadian organizations to take immediate action, increase organizational vigilance and bolster their online cyber-defences. We also encourage all Canadians to visit getcybersafe.gc.ca, and all businesses to visit cyber.gc.ca to learn more about our best practices that can be applied to protect them from cyber-threats.

Ransomware poses a significant threat to Canadian organizations. Its impacts can be severe, including business downtime, permanent data loss, intellectual property theft, privacy breaches, reputational damage and expensive recovery costs. We are calling on Canadian organizations to implement the best practices specified in the ransomware playbook put out by the cyber centre.

In addition to public advisories and guidance, the cyber centre continues to share valuable cyber-threat information with Canadian critical infrastructure partners via protected channels. This information includes indicators of compromise, threat mitigation advice and confidential alerts regarding new forms of malware and other tactics, techniques and procedures being used to target victims.

Within government, CSE has been sharing valuable cyber-threat intelligence with key partners supporting Ukraine. CSE continues to support the Department of National Defence and the Canadian Armed Forces on measures to support enhanced intelligence co-operation, cybersecurity and cyber-operations.

● (1540)

[*Translation*]

Members, as geopolitical tensions continue to rise, I want to assure you that CSE is constantly working to help address foreign and cyber threats facing Canada,

[*English*]

and we will continue to do so.

I'll be happy to answer any questions you may have.

Thank you.

The Chair: Thank you very much, Mr. Gupta.

Acting Director General Schwartz, the floor is yours. You have five minutes for your opening remarks.

Mr. Ryan Schwartz (Acting Director General, Critical Infrastructure Directorate, National and Cyber Security Branch, Department of Public Safety and Emergency Preparedness): Good afternoon, Mr. Chair and members of the committee. I'm very pleased to be here.

Thank you for the opportunity to discuss the Government of Canada's approach to critical infrastructure security and resilience.

I will start by going back in time a little bit, to 2009, when federal, provincial and territorial ministers responsible for emergency management approved the national strategy for critical infrastructure. It established a collaborative approach to CI resilience that's based on building partnerships, all-hazards risk management and sharing information.

The strategy set direction for enhancing CI resilience against current and emerging hazards. It also established the classification of CI in Canada on the basis of 10 sectors, including transportation as well as networks for each sector.

These sector networks are led by a responsible federal department. For example, Transport Canada leads the transportation sector. Public Safety Canada leads federal efforts to strengthen CI resilience. We add value to partnerships between the public and private sectors by bringing stakeholders together through the national cross-sector forum and other engagement mechanisms.

Public Safety also leads federal cybersecurity policy development, which includes the national cybersecurity strategy first published in 2010 and updated in 2018. This was followed by a December 2021 mandate letter commitment for a renewed cyber-strategy.

In this context, we work with international partners to promote the rules-based international order calling out malicious cyber-activity where warranted. Canada did just this in January in the prelude to Russia's invasion of Ukraine, condemning the cyber-attack on Ukraine's government systems and fear campaign against the Ukrainian people.

The Government of Canada, including Public Safety, has taken steps to help make sure Canadians, and especially CI owners and operators, are aware of cyber-threats, including those posed by Russian-backed actors.

Public Safety and other departments and agencies work closely with allies and partners to ensure a common understanding of the threat posed by malicious cyber actors and to ensure that we are prepared to respond if Canadian cyber-systems are targeted. This is particularly important considering the interconnectivity of today's CI.

Public Safety also leads work with federal partners on national security policy, including countering hostile activities by state actors as well as economic-based threats to national security.

In terms of specific programs and initiatives, Public Safety delivers CI resilience and impact assessments, conducts physical and cyber exercises and works with the Canadian Centre for Cyber Security to share information with industry partners on cyber-risks and mitigation measures.

Our CI impact assessments support decision-making and situational awareness on hazards and risks. They consider cascading impacts that can disrupt or degrade the distribution of goods and services via Canada's supply chains, for which ports are a key dependency across CI sectors.

The regional resilience assessment program undertakes all hazards assessments across Canada. This is a tangible way governments and industry work together to examine vulnerabilities, implement corrective measures and improve resilience. Since 2012, we have conducted hundreds of assessments at Canadian CI facilities, including electricity grids, major transit hubs and ports.

In June 2020, Public Safety, working with the Canadian Centre for Cyber Security, launched the Canadian cybersecurity tool in response to an increasing number of cyber-incidents targeting the health sector. Designed specifically for Canadian CI owners and operators, this virtual self-assessment tool is a short survey that provides a picture of an organization's operational resilience and cybersecurity posture.

Malware, particularly ransomware, has hit physical infrastructure such as pipelines, power plants, water treatment and manufacturing plants and transportation and logistics systems. As my colleague mentioned, the NotPetya malware crippled logistics companies in 2017 with ripple effects across key ports and other transportation nodes globally, leading to billions in damages.

With these types of events in mind, Public Safety has launched a cyber-physical exercise series that saw nearly 600 participants attend launch events in February and March. I would also note that we're hosting one of our quarterly industrial control systems security symposiums on March 29 and March 30, for which 900 people have registered.

I would be remiss if I didn't say that CI stakeholders also bear responsibility for protecting their assets and systems. This includes ensuring basic cybersecurity hygiene and business continuity and emergency response planning. Indeed, CI security and resilience is a shared responsibility.

Looking ahead, Public Safety is committed to working closely with provinces and territories, the federal community and the private sector to develop a new strategy and approach to CI resilience. This work is under way with the goal of developing a forward-facing strategy and approach by the end of next year.

I would conclude by noting that we are committed to working with partners to enhance and improve CI security and resilience in Canada, including addressing cyber-threats against our most vital assets and systems.

Thank you very much for your time. I'm happy to answer any questions you may have.

● (1545)

The Chair: Thank you very much, witnesses, for your opening remarks.

We will begin the line of questioning today with Mr. Jeneroux.

Mr. Jeneroux, you have six minutes. The floor is yours.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, Mr. Chair.

Thank you to the witnesses for taking the time on a Thursday afternoon to join us.

I'm going to take you up on your offer, Mr. Gupta, of expanding perhaps a bit more on the comments you made on sharing information with government and understanding how that happens. Does an incident occur and then you connect with the minister directly? Is it through a connection within the specific department that it pertains to?

If you could outline that a little bit more for me, it would be helpful.

Mr. Rajiv Gupta: Absolutely.

I will make the assumption that we're talking about incidents that happened within government, but please clarify that after if you want.

Mr. Matt Jeneroux: For sure, yes.

Mr. Rajiv Gupta: Within the government, the Canadian Centre for Cyber Security does monitor government departments. We have a variety of sensors. We look at networks, hosts, the cloud. We gather all this information. We have analytics that run. We take automated actions to defend the government.

Occasionally something gets through and there is an incident. In that case, we have a shared inbox, basically, for all government departments to notify us of the incident. Otherwise, we are typically notifying the departments of incidents that have happened. We assess the severity of the incident.

If the incident is looking like it's going to expand beyond the simple control of a single department, then we escalate through a process called the GC CSEMP, which is the cybersecurity event management plan led by TBS. That involves a variety of stakeholders, mainly the tripartite, which is CCCS—the cyber centre—Treasury Board and Shared Services Canada. There's a very structured process in which we escalate through that program by calling on different levels of communications and whatnot involving different departments.

● (1550)

Mr. Matt Jeneroux: Does that happen rather immediately, then? An incident occurs and that—

Mr. Rajiv Gupta: It depends on the assessment. If it's serious, it can happen within an hour of understanding it—

Mr. Matt Jeneroux: That's interesting.

Are the ministers of these departments notified as well, or is it through this command system and it's up to them to then notify their minister?

Mr. Rajiv Gupta: It's through the command system, so basically the GC CSEMP, and that will specify the levels of notification as you progress through the levels, depending on the severity of the incident.

Mr. Matt Jeneroux: Have there been any Russian attempts at cyber-infilitration on Canadian waters, in ports and airspace in 2022?

Mr. Rajiv Gupta: Not that we are aware of in terms of incidents.

Mr. Matt Jeneroux: Are there any under investigation right now that you can let us know about?

Mr. Rajiv Gupta: We don't speak to operational specifications here. That's where I'll leave it.

Mr. Matt Jeneroux: Sure.

Your agency has urged organizations to report any incidents of unexpected or unusual network behaviour. How many reports has your agency received since Russia invaded Ukraine, so essentially in the last month?

Mr. Rajiv Gupta: I'm not sure of the exact number. We total them each week and we gather them together. We receive all sorts of reports as Canada's national cyber centre—

Mr. Matt Jeneroux: Are we talking of thousands, hundreds, millions?

Mr. Rajiv Gupta: It's probably in the hundreds or less than a hundred per week in terms of our typical intake. That's typically the scope. Then we categorize them by sector and severity.

One thing to notice is that yes, we have the front door for the country. We're always encouraging more and more organizations across Canada to reach out to us. We are here to help. We really do want them to report these incidents into this so that we get a very good picture as to what's going on. To some extent, the numbers that I would provide for you are not necessarily representative of what's actually going on, because we believe everything to be under-reported.

Mr. Matt Jeneroux: Of these, let's say, hundreds, what industries are you most receiving these reports from? What types of places are reporting these?

Mr. Rajiv Gupta: It's across the sectors that we've seen.

Mr. Matt Jeneroux: Can you give me some examples?

Mr. Rajiv Gupta: Do you mean in terms of the sectors, going into the specific results?

Mr. Matt Jeneroux: Yes, sectors.

Mr. Rajiv Gupta: The sectors would be anything from, obviously, government. We have financial...we have the various sectors that are mentioned by Public Safety as well right across the board in terms of the—

Mr. Matt Jeneroux: They'd have to be Canadian-based, Canadian-connected. Are they...? I guess, where—

Mr. Rajiv Gupta: Yes, absolutely, you're right. We look for incidents being reported from Canadian organizations within Canada. That's what we focus on and who we support through the cyber centre.

Mr. Matt Jeneroux: In the last month you've had hundreds reported. Is that higher than in the last three years, or is this consistent with what you've seen?

Mr. Rajiv Gupta: I'm not sure of the last three years, but we're not seeing anything unusual in terms of the numbers. Cyber-threats have been consistent for years and years, and they have always been here, which is one thing we do want to stress. We have put out cyber-threat assessments talking about the threats to Canada from 2018, 2020.... This is something that we've dealt with on a regular basis. The threats tend to change over time.

The reporting is something we don't control, so I would hate to put too much emphasis on what is reported in terms of the general trend, but we're not seeing anomalous activity at this point in time, which I think is the—

Mr. Matt Jeneroux: In my last 30 seconds—just to indicate I only have a short amount of time—this is for CBSA and Public Safety.

How many employees have been relieved of their duties due to perceived or actual involvement in foreign interference since 2015? If that number is zero, how many active investigations are ongoing?

Mr. Denis Vinette: I'm happy to start.

I'm not aware of any. I would have to verify on that front. Those are investigations that are normally undertaken by the RCMP. They'd probably be better positioned to speak about any insider threat type of activity that would have been investigated at the CBSA.

The Chair: Thank you very much, Mr. Vinette.

Mr. Chahal, the floor is yours. You have six minutes.

Mr. George Chahal (Calgary Skyview, Lib.): Thank you, Chair.

I first want to thank all the witnesses for their testimony and for joining us today.

I'll start my questions with you, Mr. Gupta. To your knowledge, where do most of the cyber-attacks or attempted attacks against Canada originate from?

● (1555)

Mr. Rajiv Gupta: Cyber-attacks can originate from anywhere in the world. Wherever they originate from doesn't necessarily represent where they're coming from. Threat actors are always trying to hide where they're coming from.

From our cyber-threat assessments in 2018 and 2020, we talked about the major threats facing Canada, the number one being cybercrime. There are many different cybercriminals out there, and that is the one that we identified as major. In addition to that, we highlighted the state-sponsored programs of China, Russia, North Korea and Iran. These are the threats we had indicated in terms of being the most significant threats to Canada.

Mr. George Chahal: Which countries are the best at defending against cyber-attacks, and what can we learn from them? Do you have any specific examples that you can provide?

Mr. Rajiv Gupta: I don't know if there's a real assessment as to which country is the best. I know that in terms of the Government of Canada, we have a fairly significant cyber-defence program. It has been modelled in other parts of the world. We have divested technologies from Canada to other countries, such as the U.K. They have publicly stated that they've taken some of our host-based technology and implemented it.

I think we have a good program here. We certainly work closely with our Five Eyes partners to share notes and make sure that we are amongst the best in the world here.

Mr. George Chahal: Do you see us as a global leader in defending against cyber-attacks?

Mr. Rajiv Gupta: I think across the Government of Canada, yes.

Mr. George Chahal: Great. Thank you.

Mr. Schwartz, in your testimony you talked about public safety assessments and the impacts to our transportation, ports, and electrical grids. Have you seen Russian-backed hackers attack, or have you seen attempted attacks on our transportation infrastructure before, either here in Canada or in other countries?

Mr. Ryan Schwartz: Mr. Chair, given the operational nature of the question, I would probably have to defer to my colleague at the Canadian Centre for Cyber Security, just based on the type of activities they monitor and the role they have there.

I'm afraid I can't speak to that in any detail.

Mr. George Chahal: Can you talk a little bit—you did touch on these topics—about the assessments and the work you've done with regard to those sectors?

Mr. Ryan Schwartz: Absolutely.

We have two programs. One that I mentioned is the regional resilience assessment program, or RRAP, as we call it. There is a physical security and a cybersecurity component to that. These are programs that, in the case of the RRAP, go out to all 10 CI sectors across the country in all regions of the country. It has done, as I mentioned, a number of assessments at various CI facilities. There is a very robust physical security assessment, which looks at the typical “guards, gates and guns” type of approach. It's a 1,500-question set that we use to sit down with CI owners and operators.

That is supplemented by what we call the Canadian cyber-resilience review. It's a cyber-based question set focusing on cyber hygiene and cybersecurity posture. In addition to that, we've onboarded a new tool this year called the network security resilience assessment, which is able to plug into the facility's networks and look for weaknesses and vulnerabilities. That's also being used by the Canadian Centre for Cyber Security. We are collaborating and liaising in that respect.

In addition to that, we undertake critical infrastructure impact assessments that look at cascading impacts across sectors. Again, we take an all-hazards approach to our work. If there is an earthquake, a flood or some other type of disruption—blockades are a good example from the last few weeks—we will look at the nature of the threat or the hazard and then look at other sectors where there will be a domino effect, if you will, in terms of interdependencies and impacts that might happen in other sectors with ultimately impacts on Canadians resulting from the disruptions to CI that deliver services to them.

Mr. George Chahal: Thank you.

Mr. Gupta, would you like to have an opportunity to answer? Have we seen Russian-backed hackers attack or attempt to attack transportation or port infrastructure before, either here or abroad?

● (1600)

Mr. Rajiv Gupta: I'm not aware of the port activity that you talked about.

Mr. George Chahal: What about transportation infrastructure?

Mr. Rajiv Gupta: Transportation infrastructure is fairly broad. I would have to dig into my memory there to see exactly what has happened.

Mr. George Chahal: Thank you.

Chair, I believe that's the end of my time.

The Chair: Thank you very much, Mr. Chahal.

[*Translation*]

I now give to floor to Mr. Barsalou-Duval.

You have six minutes.

Mr. Xavier Barsalou-Duval (Pierre-Boucher—Les Patriotes—Verchères, BQ): Thank you, Mr. Chair.

My first question is for Mr. Vinette from the Canada Border Services Agency.

The government has announced a series of sanctions against Russia following its invasion of Ukraine. Have any of these sanctions had an impact on your work? How have you adjusted your approach since then?

Mr. Denis Vinette: Thank you for the question.

We always check whether individuals or commercial goods coming into the country are covered by the sanctions already in place against Iran, North Korea and other countries. We take into account the new Foreign Affairs sanctions that have been added to the existing sanctions.

We have issued guidance to our officers to ensure that they are aware of the new sanctions imposed. This will allow them to determine whether any ship, aircraft or goods coming into Canada are subject to them. If they are, we will contact Foreign Affairs to determine whether they should be seized or refused entry into Canada.

We have put measures in place, but the immediate effect is not great, as there are few goods, ships or other aircraft coming into the country because of the current Transport Canada restrictions.

Mr. Xavier Barsalou-Duval: This week our committee met with NAV CANADA and the minister of Transport Canada to discuss, among other things, the ban on Russian aircraft from Canadian airspace.

We understand that there has been some confusion as to what was being said. It would appear that humanitarian flights were included, but that this was not clear from what Transport Canada had originally said. This allowed a fake humanitarian flight—at least, one that is claimed to be fake, as the investigation is not complete—to fly over our space despite the ban.

Did you have to deal with unclear directions? Would you need more details following the new measures taken by the government?

Mr. Denis Vinette: We regularly monitor all planes, trucks, and other vehicles coming into the country. We work with the other intelligence services in Canada to do further research, when we suspect that planes that are about to arrive in the country might be targeted by the sanctions. This is something that falls under the purview of Transport Canada, but we support the department in its efforts by conducting a more thorough check. When we have suspicions, we advise them that they need to investigate the incident in question.

Mr. Xavier Barsalou-Duval: If I understood you correctly, you did not receive any indications or instructions that were not clear to you.

Mr. Denis Vinette: You are correct. We work very closely and communicate with the people in that department on a daily basis.

Mr. Xavier Barsalou-Duval: Did the CBSA play a certain role when people were forced to land in Yellowknife? What happens when Russian citizens who are not authorized to be on Canadian territory are forced to land there? How are they returned to their country, since there are no flights to that destination? How are they treated? I imagine that they are not kept in prison forever.

Mr. Denis Vinette: There are two parts to the answer.

First, in this case, it was a small plane. It was a commercial plane, but smaller than a Boeing 737. When we were informed that it might be subject to sanctions, we notified Transport Canada, which took over the file on the aircraft.

As for the passengers, our role was to determine whether they had all the necessary documents to be allowed to enter the country. I should point out that there is no ban on Russians entering the country at the moment. So their eligibility is assessed on the basis of their background and the documents and visas they need. If someone has to leave the country, we make sure that our officers follow up.

In a case like Yellowknife, for example, passengers who would be denied entry would be redirected to Calgary or Toronto, perhaps, to leave the country, and we would confirm their departure to ensure that they have indeed left the country.

● (1605)

Mr. Xavier Barsalou-Duval: Could the influx of refugees from Ukraine—which I hope will arrive soon—pose a challenge in terms of identification of individuals and threats related to [*Technical difficulty—Editor*]?

How do you verify the identity of the person in front of you?

Mr. Denis Vinette: Thank you for your excellent question.

We are able to receive Ukrainians and people who leave their country to come here because of what is happening at home. Our security checks include checking their biometrics, including their fingerprints, and their documents. We do all the checks before they receive their permit to stay in Canada. We do this in support of the efforts of the Department of Immigration. So we take all the security measures.

There's always a risk that people will try to infiltrate a humanitarian process like this, and we make sure we have all the measures in place to identify them.

The Chair: Thank you very much, Mr. Vinette and Mr. Barsalou-Duval.

[*English*]

Next we have Mr. Bachrach.

Mr. Bachrach, you have six minutes. The floor is yours.

Mr. Taylor Bachrach (Skeena—Bulkley Valley, NDP): Thank you, Mr. Chair.

Thank you to all of our witnesses for their interesting testimony this afternoon.

I'll start with questions for Mr. Gupta.

Mr. Gupta, the CSE's 2020 national cyber-threat assessment found that state-sponsored cyber-activity poses the greatest strategic threat to Canada and that this is likely intended to disrupt critical infrastructure in our country.

Would you say that this assessment from two years ago is still accurate?

[*Technical difficulty—Editor*]

A voice: We've been hacked.

Mr. Taylor Bachrach: And is it happening right now?

Voices: Oh, oh!

The Chair: Do we have everyone?

Mr. Gupta, can you check your microphone again to make sure we have your connection?

Mr. Rajiv Gupta: Yes, I lost connectivity for a bit. I'm not sure everyone else did as well.

The Chair: It's interesting that it happened as we're discussing cybersecurity threats.

Mr. Bachrach, I'll stop the time and let you pose that question again so that Mr. Gupta can hear it.

Mr. Taylor Bachrach: Mr. Gupta, I'm not sure if you caught the question, but I was referring to the 2020 national cyber-threat assessment. The question was whether that assessment is still accurate, particularly the point where it indicated that the greatest strategic threat to Canada is state-sponsored cybersecurity, particularly that disrupting critical infrastructure.

Mr. Rajiv Gupta: I'll mention two things.

Within that report we mentioned the greatest long-term strategic threat to Canada as being the state-sponsored activity, which is typically things that work against economic prosperity, national security, as well as our democratic values. When you lump all those three things together, that's where we're talking into the long-term strategic threat.

What we also highlighted in that 2020 cyber-threat assessment was the threat from ransomware, and particularly the threat from ransomware against critical infrastructure, which we said would have the biggest impact on Canadians. Unfortunately, that has come true since the 2020 threat assessment. I think in the past year we've seen ransomware being the threat that had the biggest impact on Canadians.

In terms of the question, Mr. Chair, with respect to the long-term strategic threat, it's still the threat posed by the nation-states when you bundle in economic prosperity, national security, as well as our democratic values.

● (1610)

Mr. Taylor Bachrach: Thank you, Mr. Gupta.

Following the assessment in 2020, has the CSE conducted any analysis of specific threats to marine or air transport infrastructure? I'm trying to ground this in the purpose of the transport committee and infrastructure.

Have there been any specific analyses done of specific threats?

Mr. Rajiv Gupta: No. We've worked our way through different sectors, but unfortunately, we do not have the specific threat assessments for those two sectors.

We have done some on threats to operational technologies in ICS, which we believe are relevant. The transportation sector is a combination of IT and OT. In terms of the underlying technology, we've looked at these sorts of things, but we've not done a specific threat assessment for those sectors themselves.

Mr. Taylor Bachrach: In March, the U.S. President issued a statement that warned against the potential that Russia could conduct malicious cyber-activity against the U.S. in response to the unprecedented economic costs that they've imposed on Russia alongside their allies, which of course includes Canada.

Could you describe or characterize how the global cyber-threat environment has changed since Russia's invasion of Ukraine?

Mr. Rajiv Gupta: Sure.

Going back to the 2020 cyber-threat assessment as well, we mentioned that nation-states had been developing capabilities to disrupt critical infrastructure. We knew they had been doing reconnaissance in countries like Canada. We did say in that 2020 cyber-threat assessment that, in the absence of hostilities or conflict, the threat would be low.

Given the escalating tensions in Ukraine and Europe, we had started warning Canada back on January 19. That's when we posted our first escalated tensions bulletin urging critical infrastructure operators to be vigilant, to move to heightened tensions and to actually implement some of the recommendations we had put forth, in terms of preparation. We reinforced that further in February with yet another bulletin.

We had put out other sorts of threat bulletins with respect to destructive malware in Ukraine and others to continue to warn Canadians and inform them of exactly what was going on. Just recently in the U.S., as you've referred to, Biden upped the urgency once again. On our website on Tuesday we reinforced that, saying we were in agreement with the statement that organizations in Canada need to be on a heightened vigilance and that the threat landscape for Canada is certainly one of heightened vigilance and awareness.

Mr. Taylor Bachrach: I think this has been dealt with to some degree in the previous questions, but based on the available information, would you say there's been an increase in the number of attempted cyber-attacks targeting critical infrastructure, including transportation infrastructure, in the U.S. or in western allied countries since Russia's invasion?

Mr. Rajiv Gupta: At this point we have not seen an increase. We have knowledge of the cyber-threats happening, but they are threats we would have already forecasted.

Mr. Taylor Bachrach: Moving along here, you mentioned the 2017 NotPetya cyber-attack earlier. I think that we heard from Public Safety about some of the steps they've taken since then to protect Canadian marine and shipping infrastructure.

My question is for you, Mr. Gupta. How vulnerable is marine shipping, in Canada specifically, to an attack similar to the 2017 NotPetya attack?

The Chair: You have time for a very quick response, Mr. Gupta, please.

Mr. Rajiv Gupta: NotPetya was attributed to Russia. That answers an earlier question as well in case we're aware of these.

In terms of the vulnerability, I would turn that over to my Public Safety counterpart. We helped them develop the tool, but really the assessments, knowledge and information that's sent back from that would not be in our hands within the cyber centre.

Mr. Ryan Schwartz: Mr. Chair, I can elaborate on that to some extent.

We've done work on ports with respect to some of the resilience assessment tools that we have. We've done physical security assessments at 14 facilities in Canada. We've only done cyber-assessments at four facilities. If you're wondering if that's low, I would say it is. I think part of the reason for that is that the programs we offer are not mandatory. They are voluntary programs whereby Public Safety administers these on a free-of-charge basis. We basically rely on CI stakeholders coming to us to actually undertake these services.

In this case, it is a low sample size and we can't really draw any specific comparisons from that based on the overall vulnerability.

Of course, we don't share that information broadly, except with the owner and operator under confidentiality agreements that we sign with them. We do have non-disclosure agreements that we sign with CI owners and operators and—

● (1615)

The Chair: Thank you very much.

I'm sorry, Mr. Schwartz. I just want to make sure we're giving approximately equal time to all members.

Colleagues, for those of you who are having challenges with the connection, I apologize. It seems to be happening at numerous committees across the parliamentary precinct right now. I encourage you to keep trying to log back in.

Next we have Mr. Muys.

Mr. Muys, you have five minutes. The floor is yours.

Mr. Dan Muys (Flamborough—Glanbrook, CPC): Thank you, Mr. Chair, and thank you to all the witnesses for taking time out.

Given the increase in serious cyber-threats, and certainly within the context of the overall deficiencies in defence spending by this government, would you say there is a shortfall in what we should be spending on cybersecurity, particularly given the context of what's going on in the world right now?

Mr. Ryan Schwartz: I'm sorry, Mr. Chair. Is that a question for Public Safety or the cyber centre?

Mr. Dan Muys: It's for whoever wishes to take it. Maybe we'll start with Mr. Gupta.

Mr. Rajiv Gupta: In terms of resources, I think that might be more of a policy question. At the same point in time, one thing I would highlight is that cybersecurity is an all-of-society consideration.

As mentioned earlier, there are obligations on the providers themselves, as well as on government, to provide certain elements of cybersecurity. It's a balance. Government needs to provide the advice and guidance and the tools and information to help organizations equip themselves. At the same point in time, organizations need to invest in implementing the foundational cybersecurity and cyber-resilience elements they need to defend themselves.

Mr. Dan Muys: Does anyone from CBSA or Public Safety want to comment on that?

Mr. Ryan Schwartz: Sure.

Mr. Chair, I would add that budget 2019 allocated about $508 million, I think, for efforts to advance the updated or renewed cybersecurity strategy, which was shared among a number of departments and agencies for their respective cybersecurity efforts. I would also say that there would be—I don't have a number for this—other resources that are applied there. I would use the example of my own group here, where efforts are undertaken to deliver programs that aren't counted or lumped in as part of that $508 million.

I'll leave the question at that. Thank you.

Mr. Dan Muys: Sure.

Would you say you have the resources you need now, or do you need more?

Mr. Ryan Schwartz: I guess the answer would be that this is a growth industry. I say that facetiously in the sense that the scope of the challenge is growing. Significant investments have been made.

As my colleague at the cyber centre said, cybersecurity and critical infrastructure security and resilience is definitely a shared responsibility. I am encouraged by the fact that a number of stakeholders in both the public and private sectors are working together, sharing resources and pooling information to address this.

I think the nature of the commitments that have been signalled in most recently the mandate letter for the Minister of Public Safety to renew a strategy signals the intent to do more work here, but I can't speak to whether we need more money or not at this point in time.

Mr. Dan Muys: All right.

Moving to energy infrastructure, as we look at critical infrastructure that needs to be protected, we know in May of last year the Colonial pipeline in Texas, which provides half of the gasoline for the eastern United States, was shut down for nearly a week due to a ransomware attack. You talked about how the ransomware threat is certainly the one that has the biggest impact on Canadians. In terms of our critical transportation infrastructure but also our energy infrastructure, are we prepared if we are subjected to a potential future attack?

● (1620)

Mr. Rajiv Gupta: I can start, Mr. Chair.

Absolutely, as you've pointed out, highlighting that Colonial pipeline is important. We certainly took that incredibly seriously as well, and it was aligned with what we had predicted in our cyber-threat assessment.

In December we went on a ransomware campaign to educate Canadians and to push out the information, and tools and resources that would be necessary for Canadian organizations to help equip themselves.

It started with an open letter from four different ministers [*Technical difficulty—Editor*].

The Chair: I'm sorry, Mr. Gupta. We're having a little bit of trouble hearing you. Could you perhaps repeat the last two or three sentences?

Mr. Rajiv Gupta: Okay.

In terms of countering ransomware, we did put forth a ransomware campaign in December, which was started by a joint open letter from four different ministers, as well as a ransomware playbook and a ransomware threat bulletin to help equip critical infrastructure and Canadians with the tools [*Technical difficulty—Editor*].

In addition to that, we continually share threat information related to ransomware with the various sectors. You mentioned energy, which is very important and certainly dependent for transportation. We work closely with the energy sector and we have established two programs, one called Lighthouse and one called Blue Flame, with the Canadian Gas Association and the gas industry across Canada, to exchange cyber-threat information in near real time and to help protect them.

These are two pilots we think are very important to protecting the energy sector, not just for ransomware, but for cyber-threats in general.

The Chair: Thank you very much, Mr. Gupta.

Mr. Muys, are you satisfied with the response that was provided? There were a couple of words that were cut out there.

Mr. Dan Muys: Yes, I think he circled back between the gaps in technology.

The Chair: Perfect. Thank you.

Next we have Mr. Iacono.

Mr. Iacono, the floor is yours. You have five minutes.

[*Translation*]

Mr. Angelo Iacono (Alfred-Pellan, Lib.): Thank you, Mr. Chair.

I thank our guests for being here.

My questions are for anyone who wants to answer them.

What is the nature of these attacks? Are they denial-of-service attacks or are they ransomware attacks?

[*English*]

Mr. Rajiv Gupta: I will start, Mr. Chair.

In terms of the nature of attacks, we were describing ransomware. Ransomware is a threat where a threat actor will gain access to your network and then encrypt your valuable data and hold it hostage until a ransom is paid. This threat has evolved to the point where the ransomware threat actors will actually take your data as well as encrypt it sometimes, and actually threaten to extort you in terms of threatening leakage of the information to cause further pain and to further incite you to pay the ransom.

Obviously, they're financially motivated. They will do whatever it takes to get that money. As we've seen, with targeting against various sectors, including health care and others, there is definitely a significant impact on lives and whatnot. These threat actors are interested in money and that's pretty much it.

There are different types of threats, obviously. There are DDoS attacks that do happen and sometimes those are linked to ransomware as well. Someone will basically try to overwhelm an organization with traffic and say that they won't turn it off until you pay a ransom. Those are less common than the traditional ransomware that I described.

Then of course there is traditional espionage and theft of intellectual property or sensitive company data as well, which results in data breaches because this is also worth money on the dark web in terms of selling health information, tax information or credit information and financial information, which can all be sold on these markets for money, and of course—

[*Translation*]

Mr. Angelo Iacono: Thank you.

Mr. Vinette, is it true that Russia often uses non-state actors, such as criminal networks, to carry out its attacks, so that it can better deny them?

● (1625)

Mr. Denis Vinette: This is a very good question, but I think my colleagues Mr. Schwartz and Mr. Gupta are better equipped to answer it.

[*English*]

Mr. Rajiv Gupta: I can answer, Mr. Chair.

In our ransomware threat assessment we did highlight the links between Russia and some criminal organizations in saying that they were able to operate with relative impunity in the countries in which they operate.

[*Translation*]

Mr. Angelo Iacono: Thank you.

What do you think are the vulnerable elements of our own transport networks? What do we need to protect ourselves from?

[*English*]

Mr. Ryan Schwartz: I can attempt to answer that one, Mr. Chair.

From the perspective of public safety and critical infrastructure resilience, one of the main vulnerabilities that we see across CI sectors are what I referred to in my opening remarks as the industrial control systems or the operational technologies that run power plants, regulate water pressure in valves or even operate traffic lights. These are some legacy systems that were not necessarily intended to be connected to the Internet but now are, just given the Internet of things and the increasing connectivity across critical infrastructure sectors. A key vulnerability from our perspective is industrial control systems in general.

That wouldn't just apply to the transportation sector. I would say that applies across health, as my colleague from the cyber centre mentioned. The impact there is the interdependencies. If something happens in one sector, there will be a domino or knock-on effect in other sectors. We're concerned with cascading impacts. To that end, that's why our program, with colleagues from the cyber centre, focuses on industrial control system security exercises. Preparing and planning for such events are helpful as well.

In terms of the energy sector, in the previous question, there are a number of exercises that we undertake with the private sector. Natural Resources Canada is the lead federal department for the energy and utilities sector. There are a number of exercises with Canada and the U.S., for example, energy command and GridEx.

We are focusing on those vulnerabilities, namely industrial control systems.

[*Translation*]

Mr. Angelo Iacono: Thank you.

The Chair: Thank you very much, Mr. Iacono.

[*English*]

Thank you very much, Mr. Schwartz.

[*Translation*]

Mr. Barsalou-Duval, you have the floor for two and a half minutes.

Have we lost Mr. Barsalou-Duval?

Mr. Barsalou-Duval, can you hear us?

Since he is not responding, I will give the floor to Mr. Bachrach.

[*English*]

Mr. Bachrach, if you're ready to go with your line of questioning, I can go to Mr. Barsalou-Duval afterwards.

Mr. Bachrach, the floor is yours for two and a half minutes.

Mr. Taylor Bachrach: Thank you, Mr. Chair.

I will continue with my questions for Mr. Gupta from the CSE.

In 2016, Transport Canada issued a best practices advice paper on cybersecurity for the maritime sector. I imagine you're familiar with this. I note that it hasn't been updated since 2016. Have the cyber-risks in the last six years evolved at all when it comes to the marine sector? If so, why has that best practices paper not been updated?

Mr. Rajiv Gupta: I'd note that it's not a product of the cyber centre. I'm not entirely aware of it.

I'm certainly up to speed on the products that we put out from the cyber centre. We put out our cyber-threat assessment and we update our advice and guidance regularly within the cyber centre's web pages.

Much of our advice and guidance applies across the sectors. I would recommend that people visit cyber.gc.ca to get the latest and greatest information.

● (1630)

Mr. Taylor Bachrach: Do I have time for one more, Mr. Chair?

The Chair: You do, indeed.

Mr. Taylor Bachrach: I'll ask a question of our guest from Public Safety.

Transport Canada publicly released proposals to modernize the marine security clearance program in 2021. These proposals adjust the existing risk base requirements for individuals based on their access to critical systems. It adjusted them to include extending security vetting to anyone who is involved in the movement of marine cargo.

Do you believe that the current profile of cybersecurity threats necessitates a significant expansion of security clearance requirements?

Mr. Ryan Schwartz: Unfortunately, I'm not able to answer that question. I believe that's a question that's better directed to Transport Canada. That's not an area that falls under my purview.

Mr. Taylor Bachrach: Okay.

Thank you, Mr. Chair.

The Chair: Thank you very much, Mr. Schwartz and Mr. Bachrach.

[*Translation*]

Mr. Barsalou-Duval, you have the floor for two and a half minutes.

Mr. Xavier Barsalou-Duval: Thank you, Mr. Chair.

I hope that I can be heard clearly and that there are no technical problems. Today, I had a lot of trouble connecting to the meeting. I think I was disconnected five times from the Zoom meeting.

My question is for Mr. Gupta. I hope I am not repeating what has been said, but I may have missed a few things that have been highlighted so far.

Canada's national cyber security index is 66.23 out of 100, which ranks 36th in the world in terms of cyber security. If we take Germany, which has an index of 90.91, or France, which has an index of 84.42, Canada pales in comparison, not to say that it looks like an amateur.

I'd like to know what we need to work on to raise that score. As the head of the Canadian Centre for Cyber Security, could you tell me why our score is so low compared to the benchmark countries?

[*English*]

Mr. Rajiv Gupta: Mr. Chair, I'm unfamiliar with the index that the member is referring to, unfortunately.

[*Translation*]

Mr. Xavier Barsalou-Duval: You can still talk about the elements on which we need to work more.

[*English*]

Mr. Rajiv Gupta: Most importantly to me is that we start implementing the basics of cybersecurity right across the country. It's foundational, and it applies to every type of threat there is, whether it's Russia, ransomware, cybercrime or hacktivism. We've put out baseline advice and guidance just to make our country solid.

Obviously, yes, I would like to see our country as number one and 100% there as well, but I think working on those types of basic elements of cybersecurity is critical to making sure we're ready and resilient to respond to any type of threat.

We put out advice and guidance for a small business that I think is critical. It's 13 controls that we believe are achievable in terms of implementing, and we'd very much recommend that organizations look to these as a bar to implement as well as—

[*Translation*]

Mr. Xavier Barsalou-Duval: My time is almost up, but I would like to ask you another question.

Are you working on implementing or strengthening cybersecurity for provincial or municipal governments, or are you simply focusing on the federal government?

[*English*]

Mr. Rajiv Gupta: We work very closely with our provincial partners. I recently met with all of the provincial CISOs, chief information security officers, across Canada. We have good, collaborative efforts, and we really see this as a collaborative effort to be able to increase the cybersecurity in Canada.

The Chair: Thank you very much, Mr. Gupta.

[*Translation*]

Thank you very much, Mr. Barsalou-Duval.

[*English*]

Next we have Mr. Dowdall.

Mr. Dowdall, the floor is yours. You have five minutes.

Mr. Terry Dowdall (Simcoe—Grey, CPC): Thank you, Mr. Chair.

I want to thank Mr. Gupta and Mr. Schwartz for taking time to be here today. This question will probably go to Mr. Gupta, but Mr. Schwartz may want to comment as well.

During a media briefing on February 24, 2022, Daniel Rogers, who is the associate chief of the Communications Security Establishment, said that in light of the Russian invasion of Ukraine, the CSE "strongly encourages all Canadian organizations to take immediate action and bolster their online cyber-defences." While Mr. Rogers said that the CSE was "not aware of any specific threats to Canadian organizations related to events in and around Ukraine," he pointed to "a historical pattern of cyber-attacks [against] Ukraine and other countries." In particular, Mr. Rogers said that the CSE was monitoring cyber-threats "directed at critical infrastructure networks, including those in the financial and energy sectors."

This is particularly concerning to Canadians, as so much of our personal and financial information is now stored in the cloud, on our computers or on our phones.

I know some of these questions might have been asked before, but have we seen an uptick in attacks by either Russia or China since the invasion actually began?

● (1635)

Mr. Rajiv Gupta: Within Canada from the cyber centre perspective, we have not seen that uptick in attacks against Canadian infrastructure.

Mr. Terry Dowdall: In your opinion, do you think Canadian energy and financial companies are putting in all the necessary levels of security that they should be at this time to combat cyber-attacks and to keep our personal information safe?

Mr. Rajiv Gupta: We engage these sectors regularly. We work with them. They are incredibly engaged in terms of the briefings we are giving. I feel they are definitely working and listening to the threat advisories we're putting out in terms of the enhanced vigilance and the effort to secure their systems as much as possible, given the hostilities in the current geopolitical situation. From what we see in a collaborative effort, we do see the engagement from these sectors.

Mr. Terry Dowdall: In your professional opinion, on a scale of one to 10, 10 being extremely secure, where would you rate the preparedness of Canada's financial and energy sectors against cyber-attacks as of today?

Mr. Rajiv Gupta: It's very difficult to rate from one to 10. I wouldn't be able to do that. What I will say is that they are engaged; they're competent; we know they're working on it.

We're not a regulator, so I don't know exactly how they're mitigating their risks. What I do know is that they tend to clearly understand the advice and guidance and they are engaged in terms of working with us. That's probably all I can say about that.

Mr. Terry Dowdall: Okay. Thank you.

Last week, as I'm sure you know, U.S. Congress passed a new cybersecurity law that requires critical infrastructure entities to report material cybersecurity incidents within 72 hours and ransomware payments within 24 hours to the Cybersecurity and Infrastructure Security Agency.

Is this something we should be doing here in Canada?

Mr. Rajiv Gupta: I can start, Mr. Chair.

We work on a voluntary basis. We certainly encourage all Canadian entities to report immediately to us. We're here to help and we're very happy to hear of them.

In terms of what has happened in the U.S., we're definitely going to be working with our colleagues and counterparts in the U.S. to learn how it's working there and then basically educate ourselves in terms of their experience.

Mr. Terry Dowdall: At this particular moment in time, do you think it would be something you'd recommend, though, that perhaps we need to be a little more diligent on this particular issue?

Mr. Rajiv Gupta: I'd probably turn that over as more of a policy question.

Mr. Terry Dowdall: Okay.

Mr. Ryan Schwartz: Mr. Chair, maybe just to quickly go back to the previous question on whether certain sectors are prepared, further to my colleague's comments, this is top of mind for industry associations, such as the Canadian Forum for Digital Infrastructure Resilience, as well as Electricity Canada, formerly the Canadian Electricity Association. We have a lot of engagement with different industry association groups.

With respect to greater diligence and the proposal or the initiative you mentioned from the U.S., I would flag that budget 2019 did provide some funding to support new legislation aimed at protecting Canada's critical cyber-systems in four sectors: finance, telecommunications, energy and transport. This is something that continues to be developed by key departments and agencies around town. Certainly I would say that this is a top-of-mind issue both for our industry partners but also in terms of some continued policy work that we develop in-house to the federal government.

The Chair: Thank you very much, Mr. Schwartz, and thank you very much, Mr. Dowdall.

To conclude the questioning for the first panel, we have Ms. Koutrakis.

Ms. Koutrakis, you have five minutes. The floor is yours.

[*Translation*]

Ms. Annie Koutrakis (Vimy, Lib.): Thank you, Mr. Chair, and thank you to all the witnesses who are with us this afternoon.

I invite any of our witnesses to answer my questions this afternoon.

Is there any reason to believe that foreign states might try to work with domestic groups to encourage the blocking of critical infrastructure like border crossings, as we saw earlier this year?

● (1640)

Mr. Denis Vinette: I would be happy to answer the member's question, Mr. Chair.

I thank the member for the question.

In fact, we are constantly exchanging information and listening to what is going on and what could jeopardize our presence and border fluidity because of its importance to the economy and to the security of Canada.

To answer your question directly, I don't have any information at the moment that demonstrates that, but it goes without saying that as a result of the sanctions that have been imposed, we are making sure that those cargoes, which are targeted, don't cross the border.

In terms of security, we have radiation detection portals in our seaports to make sure that containers coming in from overseas are checked for radiation and chemicals that might be in them.

We are always on guard, but I have no information at the moment that there are efforts to block the infrastructure.

Ms. Annie Koutrakis: Does anyone else want to add anything?

[*English*]

Mr. Ryan Schwartz: Mr. Chair, I wouldn't mind chiming in, if you'll indulge me.

Looking back at the example of the recent blockades in February, I would preface this by saying that I also have no intel further to Mr. Vinette's response, but I think another area worth examining is the effects of misinformation and disinformation, which can cascade across social media platforms and be used to incite certain responses, shall we say, that have negative and disruptive consequences on Canadian critical infrastructure, notably in the context of transportation critical infrastructure.

Misinformation and disinformation is something that can have very strong destabilizing effects from a critical infrastructure stability and reliability perspective, but also in terms of social cohesion. That's something as well that I would like to flag to the committee.

[*Translation*]

Ms. Annie Koutrakis: Thank you for your answer.

Is Canada's aerospace and maritime domain knowledge sufficient to detect threats to its ports, waters, and airspace?

Mr. Denis Vinette: Thank you for the question.

In fact, the CBSA works in partnership with Transport Canada, which is responsible for regulating security at airports, at our seaports, and elsewhere.

We always work very closely with Transport Canada to make sure that whenever there are threats or information comes to one of the partners, it's shared and then assessed to see if a response is required. In the maritime units, which monitor our coasts and are integrated teams of CBSA, RCMP, Coast Guard and our military colleagues, we work together to have an overview of what is happening in the maritime domain at all times. This is an example of our efforts to ensure the security of our ports of entry when there are ship movements. We deploy a similar effort on the airport side as well.

Thank you.

Ms. Annie Koutrakis: Thank you very much.

[*English*]

This will be my last question, if I have time, Mr. Chair.

Do we have our own offensive capabilities we can use against Russia as retaliation if they try attacking our critical infrastructure?

Mr. Rajiv Gupta: From a CSE perspective, we have [*Technical difficulty—Editor*] in defensive cyber-operations that we have both legislation and the capability to perform.

[*Translation*]

The Chair: Thank you very much, Ms. Koutrakis.

[*English*]

Thank you very much, Mr. Gupta.

That concludes panel one for today. I would like to thank all of our witnesses on behalf of the committee for their presence here today.

I will now suspend the meeting for five minutes to allow our witnesses to log off.

Colleagues, when we resume, we will hear opening remarks and testimony from Dr. John de Boer, senior director, government affairs and public policy for BlackBerry.

This meeting is now suspended.

● (1640)

(Pause)

● (1650)

The Chair: I call this meeting back to order.

Colleagues, for the second panel today, we have Dr. John de Boer, senior director of government affairs and public policy in Canada for BlackBerry.

Mr. de Boer, I believe you've prepared opening remarks. I turn the floor over to you. You have five minutes.

Dr. John de Boer (Senior Director, Government Affairs and Public Policy, Canada, BlackBerry): Thank you, Mr. Chair.

On behalf of BlackBerry, I'm delighted to speak with you and committee members today.

For over 35 years, BlackBerry has invented and built trusted security solutions to give people, governments and businesses the ability to stay secure and productive. Today, our software is used to protect all G7 governments, is embedded in more than 195 million cars and secures more than 500 million other devices, including mobiles, laptops, and transportation, aerospace and defence systems.

Drawing on our unwavering commitment to safety, security and data privacy, I would like to speak today about the gap between the cybersecurity preparedness of Canada's transport sector and the sector's growing exposure to cyber-threats.

Every organization in every industry sector runs the risk of a cyber breach; however, few carry the same real-world risk from cyber-attacks as those in the critical infrastructure sector. As was highlighted by this committee earlier this week, ransomware attacks on the transportation sector in North America increased by 186% between June 2020 and June 2021. In the past year, Canadian transit systems in Toronto, Montreal and Vancouver experienced cyber-attacks. Rightfully, Canadians are worried. According to the Edelman trust survey, falling victim to a cyber-attack now ranks second behind job loss on the things Canadians worry about most.

Currently, apart from PIPEDA-related obligations, Canada has no regulations in place to govern, much less obligate, rail, air and surface transit operators and owners to report, prepare for and prevent cybersecurity incidents. While there is a regulatory obligation for port administrations and marine and ferry facilities to report cyber incidents to law enforcement and Transport Canada, there is no specific reporting period nor guidance on the cybersecurity measures that they should put in place.

Stepping back to the larger geo-competitive picture, Canada is falling behind our G7 peers on cybersecurity. On a per capita basis, Canada invests half of what the U.S., U.K. and France invest in cybersecurity. The U.S. and European governments are also taking regulatory measures to raise the bar on critical infrastructure cybersecurity, like transportation systems. For example, in the wake of successive attacks on U.S. critical infrastructure, including the Colonial pipeline and the New York subway system last year, the U.S. government took meaningful steps to address cyber vulnerabilities.

In May 2021, President Biden issued an executive order on improving the nation's cybersecurity, which required his government to modernize its cybersecurity defences. In July 2021, President Biden directed the U.S. government to develop cybersecurity performance goals for critical infrastructure owners and operators.

In December 2021, the U.S. Department of Homeland Security's Transportation Security Administration [*Technical difficulty—Editor*] for all freight railroad carriers, passenger rail and rail transit operators to designate a cybersecurity coordinator, report cybersecurity incidents to the U.S. government within 24 hours, develop a cybersecurity incident response plan and conduct cybersecurity vulnerability assessments.

Just two weeks ago, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 requiring covered critical infrastructure entities to report cybersecurity incidents to government within 72 hours and ransomware payments within 24 hours.

Europe has similar requirements and is currently expanding these requirements to include intelligent transport systems, such as connected cars and smart infrastructure. It also plans to levy fines of up to 10 million euros or 2% of annual revenue, whichever is greater, to those who are found non-compliant.

● (1655)

While Canada recently joined the U.K. and the U.S. in calling on critical infrastructure entities to “bolster their awareness of and protection against...state-sponsored cyber-threats”, we are still far behind.

BlackBerry stands ready to work with this committee to strengthen the cybersecurity of Canada's transportation systems from this growing and evolving threat.

Thank you for time today. I look forward to your questions.

The Chair: Thank you very much, Dr. de Boer.

To begin our round of questioning for this panel, we have Ms. Lantsman.

Ms. Lantsman, the floor is yours. You have six minutes.

Ms. Melissa Lantsman (Thornhill, CPC): Dr. de Boer, thanks for joining us via Zoom, and thank you for your opening comments.

I want to start by asking you if there is enough data in Canada. We seem to be getting mixed messages of we don't know, or we don't know how much of a threat this is in this sector or that sector. Do you think we collect enough data to make a proper assessment of the cybersecurity threats that we face?

Dr. John de Boer: Ninety per cent of cyber incidents go unreported.

Furthermore, as I mentioned, there are no mandatory requirements for critical infrastructure operators or private sector entities to report cyber incidents.

You put your finger on a critical issue. The Canadian government and many entities simply do not have full visibility on the scale of the threat or the persistent nature of the threat. That is one of the key issues, and that is one of the reasons why President Biden moved to require mandatory cyber incident reporting for critical infrastructure.

● (1700)

Ms. Melissa Lantsman: Thanks for that.

I wonder, then, how governments make decisions about how much money to allocate to cybersecurity, if they don't know the scope of the threat.

We just heard from an official at Public Safety, Mr. Schwartz. He mentioned that $500 million was allocated in the 2019 budget. Given what we've seen over the last number of weeks in this country and the incredible shortfalls in our own security and defence funding, he suggested that this was sufficient, albeit with the caveat that the threats are growing.

Can you talk a little bit about where Canada falls in terms of our funding towards cybersecurity? How do we know how much money to spend if we don't know the scope of the problem, and why are we spending so much less than our allies?

Dr. John de Boer: Last year's budget, budget 2021, allocated $791 million Canadian to cybersecurity. That was somewhat of an increase from budget 2019. On a per capita basis, as I mentioned earlier, Canada spends $20 on cybersecurity. When you compare that to what the U.K. spends on cybersecurity, which is $52 Canadian, and the U.S. spends $34 and France spends $37, we are well behind.

In terms of whether we are spending enough, the short answer is no. The Canadian business sector spent $7 billion on cybersecurity last year. That's clearly also not enough, because the Insurance Bureau of Canada indicates that 47% of our small and medium-sized businesses spent zero dollars on cybersecurity last year. So there is much room for growth.

We need to catch up to our allies in order to boost our defences. Part of that is mandating it. Part of that is for the government to fill, perhaps, a market failure, which is that cybersecurity is looked to as a cost centre and not prioritized. This needs to be prioritized at the highest level.

Ms. Melissa Lantsman: I'm cognizant of the fact that you mentioned in your opening statement that, I think 186% was the number you used, in terms of increased incidents over a year. I think I mentioned that earlier in this committee. Given that number and given what you know, I'm a little perplexed by the fact that our last round of officials didn't have any kind of assessment on critical transportation. I'm wondering if that's a gap that we have.

What is your risk assessment of a foreign threat, in the case of this study, by Russia? What is your assessment of the threat it poses to critical transportation infrastructure at the present moment?

We heard a lot about financial institutions. We heard a little bit about our critical infrastructure when it comes to oil. In terms of transportation, is there any way of knowing, if we've never studied it and we have no assessment?

Dr. John de Boer: I would rely on some of the assessments that have come out of the U.S. government. The U.S. government has publicly indicated that this threat is real and persistent. President Biden issued a strategy, a maritime cybersecurity strategy, last year, which documented significant gaps in the port system, as well as in ship systems. Many of these systems, whether it be ships, trains or planes, are built to last 30 years. What that means is that they contain legacy systems, outdated IT systems that have not been patched. The vulnerability is vast; it's deep, and the threat is persistent and real.

The U.S. Justice Department in October 2020 charged six Russian intelligence officers affiliated with the NotPetya malware attack that crippled the shipping giant Maersk and also attacked TNT—now FedEx.

There is evidence out there that some of these attacks, some of the largest, most impactful attacks, are state-based.

● (1705)

Ms. Melissa Lantsman: Thank you, Dr. de Boer.

The Chair: Thank you very much, Dr. de Boer.

Thank you, Ms. Lantsman.

Next we have Mr. Rogers.

Mr. Rogers, the floors is yours. You have six minutes.

Mr. Churence Rogers (Bonavista—Burin—Trinity, Lib.): Thank you, Mr. Chair.

Welcome to our guest.

Mr. de Boer, it's mind-boggling when you talk about all this cybersecurity. Just this past year in Newfoundland and Labrador we had a major attack on the health care system, which was crippled for a number of days. It created all kinds of problems for the health care system in the province. Some serious gaps occurred. Medical records went missing, and there were all kinds of problems that the health care professionals had to deal with. It took a considerable amount of effort and time on behalf of the provincial and federal people to resolve many of the issues. It was such a serious event that the premier and people in Ottawa wouldn't even talk about it publicly for security reasons.

I'm not sure even now if it's totally resolved, although it seems to be, and there's not much discussion in the public realm anymore.

In your view, how could this be prevented in the future? What's done is done, but in the future, how could this be prevented, or can it be prevented from happening again?

Dr. John de Boer: It's a great question, and the answer is, yes, it can be prevented.

We have technologies out there in the market today that are prevention-first technologies. Essentially, they leverage AI and machine learning to predict and prevent attacks before they are executed. We have moved beyond traditional technology, which basically adopted what is called a signature-based approach, similar to how we dealt with a COVID-19 vaccine. You need a patient zero, and then you model it and trace it, but now we've moved ahead of that. We have technology that, if put in place, can prevent that.

Second, mandatory cyber incident reporting for critical infrastructure will automatically create an incentive—or a stick, if you will—for entities to put in place better defences. They don't want to have to report their cyber incidences, but if they do, and if it's time-bound, at least we can move quickly to contain it.

Another key vulnerability that can be addressed, and it's being done in the U.S., is actually to get developers of software that's embedded in critical infrastructure and government systems to produce what we call a software bill of materials or an ingredients list that will list all of the components that are in that software so that they can quickly determine the provenance or origin of that software, where it comes from, identify whether vulnerabilities exist and be able to remedy them.

The reality right now is that people who buy software have no idea what's in it. There's no way to verify whether or not that software was built using cybersecurity practices.

Mr. Churence Rogers: I'm not sure you can answer this in the time I have left, but I have a follow-up question.

I get the impression from your comments that you took a lot of examples and illustrations from what the U.S. is doing and what they plan to do moving forward. How would you characterize Canada's preparedness to deal with issues of cyber-attacks on our transportation networks? Which ones would be the most susceptible to attack? Would it be airlines, marine or rail service traffic? How do we better protect against these cyber-attacks?

● (1710)

Dr. John de Boer: All of them, unfortunately, are susceptible. All of them contain legacy IT systems that are not protected and have open-source software that could contain back doors. They depend on supply chains where they are trusting those suppliers, those vendors to implement secure practices, but they perhaps do not verify them.

All of them are susceptible. That's why we need to move quickly to get these critical infrastructure operators, transit operators, to take action to report cyber incidents, to develop cyber incident response plans and to undergo cybersecurity vulnerability assessments. Finally, it's not just about having a plan on paper. We need to verify that they put that in place.

Mr. Churence Rogers: When I listen to all of the advice you're giving us—and Ms. Lantsman mentioned this as well—it sounds like we have to spend much more money in order to be properly prepared. Is that an accurate assessment?

Dr. John de Boer: BlackBerry, together with the Canadian Chamber of Commerce and its members, has put forward a budget submission. We are calling on the government to double its investment in cybersecurity. That would bring us up to what our peers in the G7 are spending on cybersecurity. So, yes, we need to spend more, and we need to spend it smartly. There are also initiatives that won't cost money that we can do right now, as I mentioned, in terms of cyber incident reporting.

The final thing I'll mention very quickly is that we need leadership at the top. Describing that cybersecurity is a priority. President Biden is out there almost daily talking about cybersecurity. We need to take that type of leadership as well.

The Chair: Thank you very much, Dr. de Boer, and thank you, Mr. Rogers.

Mr. Churence Rogers: Thank you very much.

[*Translation*]

The Chair: The next speaker is Mr. Lemire.

Mr. Lemire, I welcome you to the committee. You have the floor for six minutes.

Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Thank you, Mr. Chair.

I would also like to thank the entire technical team.

Mr. de Boer, in 2021, the Government of Canada chose BlackBerry for its needs in terms of secure productivity and communication as well as critical event management. As this statement leaves a lot of room for interpretation, I would like to know your views on this matter.

What exactly is the nature of the cybersecurity services that BlackBerry provides to the federal government?

[*English*]

Dr. John de Boer: Mr. Chair, BlackBerry provides a range of services from our unified end point protection and unified end point management services, which protect mobile devices. We also provide secure communications to the Government of Canada, which are certified by the Canadian cybersecurity entity CSE as well. It's primarily oriented to secure communications and unified end point management, which, again, is about secure mobile technology.

[*Translation*]

Mr. Sébastien Lemire: Thank you.

According to a report published in 2017 by the Communications Security Establishment, the federal government alone is subject, every year, to more than 2,500 computer intrusion attempts by foreign state actors.

Mr. de Boer, can you tell us approximately how many cyber-attacks the federal government has been targeted with since it began collaborating with BlackBerry in 2021?

[*English*]

Dr. John de Boer: It's hard to say. I don't have the precise numbers on the government. Again, our remit is focused largely on secure communications and on mobile technologies. We don't monitor the overall security posture of the Government of Canada.

[*Translation*]

Mr. Sébastien Lemire: If you can't give us numbers, can you talk about the nature of the attacks? Since the beginning of your mandate with the federal government, have you felt that the seriousness of cyber-attacks targeting Canadian institutions has been increasing?

[*English*]

Dr. John de Boer: I don't have visibility personally on that type of information, on the seriousness of those attacks. I can only comment on what's been in the news and what I've seen on a personal basis. I'm afraid I'm not able to provide you with a precise answer to that question.

● (1715)

[*Translation*]

Mr. Sébastien Lemire: In your speech, you talked, on the one hand, about the security of devices and the risks that anyone could be subject to cyber-attacks. On the other hand, you talked about the legal obligation of companies to report cyber-attacks on critical infrastructure.

As a contributor, would you be able to give us any information on that? If you provide a system, you have access to it. Are you in a position to help the government receive this data so that it is more transparent?

[*English*]

Dr. John de Boer: BlackBerry regularly collaborates with the Government of Canada, the Canadian Centre for Cyber Security and others, whether it be related to vulnerability disclosures or other threat assessments.

One thing I would like to offer, though, is that a lot of the emphasis has been on information sharing. I think there's room to emulate what the United States has done again here, which is collaborative planning. This is a preventative approach to dealing with upcoming potential events. That's what I would emphasize.

It would be much more robust public and private sector collaboration with the government, where there is two-way communication and we are engaged in collaborative planning for potential events that may come our way.

[*Translation*]

Mr. Sébastien Lemire: I think you can see that—

The Chair: Unfortunately, Mr. Lemire, I can see the lights indicating that there is a vote in the House.

[*English*]

Do I have the consent of the committee to continue, or are there those who see fit for us to adjourn?

Mr. Clerk, how long are the bells? Do you know?

The Clerk of the Committee (Mr. Michael MacPherson): They're 30 minute bells.

The Chair: Perhaps if it's okay with the committee, we'll conclude the questioning for Monsieur Lemire, and then we can conclude. Does that work?

Mr. Churence Rogers: I would suggest that, Mr. Chair, yes.

The Chair: Thank you very much, Mr. Rogers.

[*Translation*]

Mr. Lemire, you can continue.

Mr. Sébastien Lemire: Thank you, Mr. Chair. It is much appreciated.

Mr. de Boer, you can see that Russia is cyberbullying and trying to influence public opinion in several areas of interest. We saw this during the United States elections, for example. I have heard that there was an attempt to influence the perception of projects such as the deployment and sale of hydroelectricity in the northeastern part of the United States. Allegedly, there was intimidation from foreign countries.

Is that the kind of information you're able to see on the ground?

[*English*]

Dr. John de Boer: BlackBerry is not necessarily in the business of dealing with this information or influence [*Technical difficulty—Editor*]. Our focus is strictly on the technical side of cybersecurity. I wouldn't be able to comment on that aspect of this threat landscape, unfortunately.

[*Translation*]

Mr. Sébastien Lemire: If Russian planes invaded our airspace, would you be able to know that?

[*English*]

Dr. John de Boer: No, that would not be information we would have access to or that we would engage in.

[*Translation*]

Mr. Sébastien Lemire: Very well. Thank you very much.

The Chair: Thank you very much, Mr. Lemire.

[*English*]

Thank you, Dr. de Boer, for being here and for providing us with your testimony.

That concludes this committee's testimony on Canada's preparedness to respond to Russian threats to Canadian waters, ports and airspace.

Thank you very much, colleagues.

The committee is adjourned until Monday, March 28, at 11 a.m.