



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 104

Monday, April 29, 2024

Chair: Mr. Heath MacDonald



Standing Committee on Public Safety and National Security

Monday, April 29, 2024

• (1545)

[English]

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

Welcome to meeting number 104 of the House of Commons Standing Committee on Public Safety and National Security.

Pursuant to Standing Order 108(2) and the motion adopted by the committee on October 23, 2023, the committee is resuming its study on the growing problem of car thefts in Canada.

Before we begin, I would like to remind all members and other meeting participants in the room of the following important preventive measures. To prevent disruptive and potentially harmful audio feedback incidents that can cause injuries, all in-person participants are reminded to keep their earpieces away from all microphones at all times.

As indicated in the communication from the Speaker to all members on Monday, April 29, the following measures have been taken to help prevent audio feedback incidents. All earpieces have been replaced by a model that greatly reduces the probability of audio feedback. The new earpieces are black, whereas the former earpieces were grey. Please only use an approved black earpiece. By default, all unused earpieces will be unplugged at the start of a meeting. When you are not using your earpiece, please place it face down in the middle of the sticker for this purpose, which you will find on your table as indicated. Please consult the cards on the table for guidelines to prevent audio feedback incidents. The room layout has been adjusted to increase the distance between microphones and reduce the chance of feedback from an earpiece. These measures are in place so that we can conduct our business without interruption and to protect the health and safety of all participants, including the interpreters. Thank you all for your co-operation.

Today's meeting is taking place in a hybrid format. In accordance with the committee's routine motion concerning connection tests for witnesses, I'm informing the committee that all witnesses have completed the required connection tests in advance of the meeting.

I would like to make a few comments for the benefit of members and witnesses. Please wait until I recognize you by name before speaking. I remind you that all comments should be addressed through the chair.

I would now like to welcome our witnesses for our first panel.

From the Canadian Automobile Association, we have, in person, Ian Jack, vice-president, public affairs; and by video conference,

Elliott Silverstein, director of government relations, insurance. From the Insurance Corporation of British Columbia, by video conference as well, we have Shabnem Afzal, director, road safety; and Kelly Aimers, chief actuary.

Up to five minutes will be given for opening remarks, after which we will proceed with rounds of questions. I now invite Ms. Aimers and Ms. Afzal to make the opening statements, please.

Ms. Kelly Aimers (Chief Actuary, Insurance Corporation of British Columbia): Thank you for welcoming ICBC to appear before this committee.

My name is Kelly Aimers, and I am the chief actuary at the Insurance Corporation of British Columbia, or ICBC. With me is my colleague, Shabnem Afzal, who is ICBC's director of road safety.

I would first like to recognize that we are at ICBC's head office in North Vancouver, British Columbia, on the traditional ancestral indigenous territories, both unceded and treated, of the Musqueam, Squamish and Tsleil-Waututh first nations.

ICBC is a provincial Crown corporation mandated by the Insurance Corporation Act, the Insurance Act and the Motor Vehicle Act to provide universal, compulsory auto insurance to drivers in British Columbia. In addition, ICBC provides British Columbians with optional auto insurance products, vehicle registration services, driver's licence services. We work with external stakeholders on road safety projects and auto crime initiatives.

I would like to applaud the work of this committee and all of the participants. We support the ongoing efforts to date and look forward to enhancing initiatives to prevent vehicles from being stolen within Canada.

According to statistics provided by B.C.'s integrated municipal provincial auto crime team, otherwise referred to as IMPACT, in 2023, B.C. had its lowest number of auto theft incidents across the province since 2018. B.C. had 7,538 auto theft incidents reported to police, a 10% decrease from 2022, with declines posted across the province.

Vehicle theft is covered under optional comprehensive insurance from ICBC or other private insurers.

In 2023, of those 7,500 auto theft incidents reported to police, 6,255 of them were reported to ICBC, with an average cost of \$5,700. This average cost also includes the deductible for a stolen vehicle claim reported to ICBC. While there has been a slight decrease in stolen vehicle claims reported to ICBC from 2022, the average cost of these vehicles has increased.

While ICBC has the majority of the optional insurance market, I want to emphasize that these are just claims reported to ICBC. Claims can also be reported to other optional insurance carriers, and some motorists may not even have optional insurance. Further, these preliminary financial figures and incident counts may continue to settle as claims are closed.

With that, I would like to pass it to my colleague, Shabnem Afzal, who is ICBC's director of road safety.

• (1550)

Ms. Shabnem Afzal (Director, Road Safety, Insurance Corporation of British Columbia): Thank you.

ICBC has partnered with the B.C. government on the integrated municipal provincial auto crime team, or IMPACT, as Kelly was just mentioning. The mandate of this team is to fight auto crime. We've partnered to successfully target chronic auto theft offenders and organized auto crime groups since 2004, the inception of IMPACT. IMPACT heads the successful provincial bait car program, too, which also targets chronic auto crime offenders across the province. This year, 2024, marks the 20th anniversary of the creation of the integrated municipal provincial auto crime team, and ICBC has been a funding partner since the inception of IMPACT.

ICBC also has a dedicated special investigation unit, otherwise known as the SIU, and we have an officer from our unit attached to the IMPACT team. They act as a liaison with other law enforcement in B.C. as well as the other ICBC offices that are dedicated to the identification of cloned or "re-vinned" vehicles. Having these dedicated offices obviously helps us protect the integrity and minimize the risk of the vehicle registration process in B.C.

To further combat vehicle crimes, ICBC's SIU detection unit employs a dedicated team of specialists who leverage data and analytics to identify concerning theft claims, and ICBC has an internal fraud analytics model that uses data and natural language processing to identify concerning claims for review.

We partner with local police and stakeholders for auto crime prevention initiatives such as providing steering wheel locks and preventing catalytic converter thefts. ICBC also provides insurance incentives to encourage customers to use these passive electronic immobilizers to protect their vehicle.

With that, I would like to defer to the committee and answer any questions that you may have.

Thank you.

The Chair: Thank you to you both for your remarks.

I now invite Mr. Jack or Mr. Silverstein, please.

Mr. Ian Jack (Vice-President, Public Affairs, Canadian Automobile Association): It'll be me, Mr. Chair. Thank you very much.

[Translation]

Good afternoon.

Mr. Chair and honourable members, thank you for inviting us to share our views on the effort to combat auto theft.

[English]

My name is Ian Jack. I'm the vice-president of public affairs for CAA's national office here in Ottawa. My colleague, Elliott Silverstein, our director of government relations for insurance, joins me virtually today to help answer your questions.

Together, CAA and CAA Insurance represent the interests of 7.1 million motorists who are members of our not-for-profit association, whether that be AMA, BCAA or CAA, and tens of thousands of auto insurance clients whose policies are with CAA Insurance.

As such, we believe that we bring a unique perspective to the issue of auto theft informed by the practical, mental and financial costs of the issue to all Canadians.

Most of you will be familiar with the brand.

[Translation]

Founded in 1913, the Canadian Automobile Association, CAA for short, is a national organization representing eight automobile clubs and providing members with roadside assistance, insurance services, savings and discounts, and travel services.

[English]

The CAA Insurance Company was established in 1974 and, since then, has provided dependable, fair and trustworthy service to protect Canadians and what matters most to them.

CAA was pleased to be the only consumer advocate invited to the federal government's February auto theft summit to represent vehicle owners, who are the first line of defence in preventing auto theft and the most impacted in their daily lives when a theft does occur. The summit was just a first step and now, nearly three months later, we are still waiting on some key elements of the national strategy that was promised. The subject is no less urgent today. We need to get going, and not just with the starter's pistol but with concrete and short but reasonable timelines for results.

As you know, the costs of vehicle theft are rising astronomically. There have been \$1.2 billion in additional payouts in 2022, and these costs are being passed on to consumers in the form of higher premiums and, in some cases, vehicle surcharges of up to \$500 if you happen to be unlucky enough to own one of the top 10 most stolen vehicles. We believe that these costs will be significantly higher for 2023.

To put this in perspective, the impact of auto theft for the insurance industry is the equivalent of a flood or a tornado, except it is occurring year-round and with no end in sight.

● (1555)

CAA is concerned that if the rate of vehicle theft is not brought under control, auto-related costs will continue to rise for drivers already struggling with affordability issues. Insurance premiums, deductibles and overall costs are likely to go up for everyone if auto theft rates remain high.

We would like to underscore that soaring auto theft rates are more than just a cost pressure for consumers, as important as that is.

[*Translation*]

Victims of auto theft lose their means of getting to and from work and, occasionally, important appointments.

[*English*]

It can mean waiting months to get a vehicle replaced, or having to trade down in this inflationary market in order to get a vehicle. It has a mental toll as well. We are pleased with the actions taken to date by law enforcement and provincial and federal governments, but we need commitments, with reasonable but aggressive timelines, to further step up action to stem the flow of auto theft.

Specifically, CAA calls on the government to, first, empower the CBSA to do more enforcement at ports, specifically the Port of Montreal, by upping boots on the ground, installing cargo container scanners and prioritizing random inspections on exports, which today are virtually non-existent.

We call on the government to launch with a tight timeline an update on vehicle anti-theft standards, which are now more than 15 years old. This technology is being exploited by criminals to easily steal vehicles. CAA has pressed for a quick consultation period so that the regulations can be revised with minimal reasonable delay. Owners should not be left to incur the cost of installing expensive aftermarket anti-theft solutions to make up for inaction by the industry.

We call on the government to increase minimum penalties in the Criminal Code for repeat offenders. CAA was pleased to see that the budget acknowledged the need to enhance these penalties, but again, we would like to see action now, not in months or years.

We call on the government to deliver more funding and better coordination and intelligence sharing among law enforcement agencies. We have already seen the fruits of this in recent weeks. We need to see more of it.

In this regard, we need to re-examine the authorities and responsibilities given to rail police in such places as Mississauga, and the resources that the CBSA devotes to these areas.

Let us be clear: We understand that everyone has a part to play in combatting auto theft, including provinces, municipalities, local police, manufacturers and others. More consumer awareness is also needed. That is on us.

[*Translation*]

I can assure you that we are active on several fronts.

[*English*]

Simple tips like locking car doors, parking in the garage if you have one and using a Faraday pouch for your key fob at night can help prevent theft. These are messages that we are passing on.

With that short introduction, Mr. Chair, I will close. We welcome your questions.

[*Translation*]

Once again, thank you for inviting us to meet with the committee today.

[*English*]

The Chair: Thank you, Mr. Jack.

We will go right into our first round of questioning.

Mr. Caputo, I believe you're up first.

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

My intention is to ask questions for a few minutes and then to move my motion, which was provided last week.

Thank you to all of you for being here. As a B.C. MP, I thank and welcome our fine people from ICBC. I also welcome and thank very much the people who are here in person.

I'm relatively new to the committee. I'm still kind of getting a handle on all this.

Mr. Jack, I heard you speak, and the question I'm curious about is this: How did we get here? How did we get so complacent? You described this as "the equivalent of a flood or a tornado". I was quite happy to hear that you have some tangibles, but how did we actually get here, to something that really is at a crisis level?

• (1600)

Mr. Ian Jack: Well, it's interesting; we understand when we look back and when we do research that there was a lot of auto theft in this country 10 or 15 years ago. I think a lot of emphasis was put on it. Since then, that emphasis has gone. That worked, and then the emphasis went away.

I think organized criminal gangs are like a water leak in a house. They go to the path of easiest resistance. I think for a variety of reasons, auto theft has now become fairly easy. We have very lax standards that are not at all modern. We have iPod-era standards for anti-theft devices in vehicles right now. It's easy to get into a vehicle. It appears quite easy to put them into containers at rail yards and trucking containers, where there doesn't appear to be enough oversight from our CBSA officials looking at exports. It appears very easy to get them onto ships and out.

I will note as well a couple of what were, to us, very interesting pieces of testimony. I can't remember if it was IBC or Équité that pointed out that in Canada, the Canadian rules are such that you can change a ship manifest after it sets sail. That makes no sense. Nothing should be changing inside a container after it sets sail. You can claim that it's dishwashers and then change that when you get into waters: Oh, by the way, it's actually cars—bye.

That makes no sense. These are rules that should be changed. There's also a 72-hour rule that we'd like to see, one that the U.S. has, that says you can't change the manifest within 72 hours of shipping. That makes sense to us as well.

I would say that a whole series of things happened to lead us to where we are today.

Mr. Frank Caputo: It seems to me there a lot of tangible issues, and there are some regulatory issues relating to anti-theft devices and coming with the times. Then there are the tangible issues with prevention, compliance and enforcement. I assume that at your level you've probably had some discussions with the CBSA and groups like that. Is that accurate?

Mr. Ian Jack: Yes, we absolutely have.

Mr. Frank Caputo: How have your suggestions been met, when you met with the CBSA?

Mr. Ian Jack: The opening line was that they don't really do export inspections; they worry about imports. That's fair enough, but I think the clear message from us—from this committee, I would hope, and, I believe, from some government officials, at least—has been that this is not good enough and we need to do a lot better.

I do know that some dollars have been put aside for the CBSA for that. However, I think we need a mentality shift, and they do actually need some dollars. CAA has done tours of both the Montreal and Halifax ports in recent months and met with port officials. They have described the CBSA inspection routines, which don't really seem fit for the 21st century, if I may say so, although I'm not an expert. They need more and better facilities, and they need to be told to do more, frankly, on exports.

Mr. Frank Caputo: Thank you.

I believe Mr. Kurek will be replacing me, but with that, I will move the motion for which notice was given last Thursday, I believe.

The Chair: You have two motions, Mr. Caputo. Which one are you referring to?

Mr. Frank Caputo: I'm sorry. It's the notice of motion that starts with "Given that continued instances of repeat offences".

The Chair: Do you want to read the whole motion, Mr. Caputo, just to make sure?

Mr. Frank Caputo: This is dated Friday, April 26, 2024. I move:

That, given continued instances of repeat offences while criminals are out on bail, including the case of a man who was arrested for attempted carjacking, was let out on bail and was arrested for carjacking again the next day,

and that in the news release about this incident, the Victoria Police Department identified Bill C-75, the revolving door bill, as the reason this individual was released to then go on to commit the same offence within a day of the first,

the committee concur with the findings of the Victoria Police Department that the Liberal government's Bill C-75, the revolving door bill, is adding to the challenges police departments are facing when combatting auto theft when offenders are expeditiously released back into the streets.

Thank you.

The Chair: Thank you, Mr. Caputo.

Mr. Genuis, please go ahead.

Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC): Thank you very much, Mr. Chair.

I want to thank my colleague, Mr. Caputo, for putting forward this motion and for his excellent work on this important issue.

I appreciate the opportunity to say a few words about the sad trajectory that rates of crime have taken in this country in the last nine years—in the time that Justin Trudeau has been Prime Minister.

We have seen how this NDP-Liberal-Trudeau experiment of catch-and-release policies in the area of bail has simply failed. We have many instances where, let's say, the same people are committing crimes over and over again. Someone commits a crime in the morning, they're released on bail and they proceed to commit another crime in the afternoon, evening and so on.

This is not a coincidence that all of a sudden Justin Trudeau becomes the Prime Minister and suddenly people's disposition towards criminal activity changes. It's a consequence of policy decisions that were made by the government that allow repeat violent offenders to have easier access to bail and to go out and commit crimes that harm our community.

That is why I think this motion is important. It's a motion that was put on notice—and I hope will have the support of colleagues—that simply supports the findings of the Victoria Police Department and recognizes the failures in the Liberal government's Bill C-75, the revolving door bill, as it relates to bail. The motion responds to and recognizes the determinations of that police department that this revolving door bill is causing significant problems. It's making life more difficult for police officers and for everyday citizens. It's making life easier for repeat violent criminals.

I appreciate the clarity of the motion and the fact that it responds to an evident reality in the government's record on crime. Crime statistics tell this story very clearly. Crime was dropping up until 2015 and then rose dramatically after 2015. We all know what happened in 2015.

It's been nine years of failed NDP-Liberal experiments on crime that haven't worked. It's time for a new approach.

I'll leave my comments there.

• (1605)

The Chair: Mr. Kurek, please.

Mr. Damien Kurek (Battle River—Crowfoot, CPC): Thank you very much, Chair.

I appreciate the motion that my colleague, Mr. Caputo, has moved.

Let me share for a brief moment some reflections that are not my own, which I heard over the course of the constituency week from some law enforcement professionals in my constituency. To make sure that I protect them, I won't get too specific as to where they're from and which police force they're a part of. Suffice it to say, they police a large rural area and part of the region that I have the honour of representing.

The reason it's so relevant is that it relates to the catch-and-release policies that see a very small number of offenders—in many cases dangerous, violent offenders—being arrested time and time again for the same crimes. You have small communities.... In the area that I represent, there are several hundred people who are terrorized by a small group of people. Everybody knows who is perpetrating these crimes. The police know that is in fact the case. It is so frustrating, and in fact demoralizing, to our hard-working men and women who wear police uniforms of various departments.

I know this motion specifically references the Victoria Police Department and that's very valid, but it's an amplification of the message that we hear from so many law enforcement professionals. These are individuals who put their lives on the line every day to keep our communities safe, yet they feel like the forces are pushing back against them being able to do their jobs with the catch-and-release policies like those that we've seen from Bill C-75.

Whether it's in small towns across rural Alberta, in the north, in the Maritimes or in our big cities where we see cars sometimes the same day or within a couple of days being shipped overseas, this is a huge concern. I suggest it requires the continued urgency of this committee, especially as we are hearing from those who are on the front lines.

I cannot emphasize that enough. Those who are on the front lines are facing the direct consequences of this. I could not imagine a more difficult career in today's world than being a law enforcement professional, a police officer, with all of the pressures. They have policies of their government working against their ability to do their jobs and protect the communities where they live and work and that they care so deeply about.

There is much more that I could say on this subject. I would simply say, to my colleagues from other parties, let's treat this with the urgency that Canadians are demanding this committee treat it with. Let's pass this motion. It's a small step to acknowledge some of the urgency in how we can address auto theft, and specifically the issues surrounding those repeat violent offenders. Hundreds of hours of police work go into those arrests, yet the offenders are being turned out within hours. In many cases, they are then back out on the streets committing those same crimes, endangering our communities and traumatizing individuals. Quite frankly, Canadians deserve better than what they're getting.

I hope that this committee seizes this opportunity to take a serious look at this issue with some of the information that is being brought forward by the Victoria Police Department, to amplify that message that we are hearing from so many across our country.

• (1610)

The Chair: Thank you.

Ms. Michaud, please.

[*Translation*]

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

I feel far away from you today, but I understand that it helps keep our interpreters healthy and safe, and without them, we could not do our jobs day in and day out. I'd like to thank the House technicians for implementing this measure.

The motion put forward by my Conservative colleague pertains to a crime in which an individual was arrested for carjacking. The Bloc Québécois is obviously very concerned about any offence or situation related to the rise in auto thefts across the country—which is why I proposed the study in the first place. We are in the middle of the study, and we have witnesses here today to discuss that very issue. They've taken time out of their day to speak with us and share their recommendations. Out of respect for them, I would like us to get back to the study.

If I'm not mistaken, Bill C-75 was debated, and voted on, in the 42nd Parliament. It received royal assent in June 2019, so I don't think we need to vote on conclusions that tie back to a bill from a previous Parliament. If we can vote on the motion, we can get back to the study, and I'll be voting against the motion.

[*English*]

The Chair: Thank you.

Mr. MacGregor, go ahead, please.

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

I don't really have any skin in the game for this one. I'm speaking as someone who did vote against Bill C-75. I was present in the 42nd Parliament during the Liberal majority government.

I just find it curious that this motion is being brought forward when we're actually in the middle of a study on car theft. Questions come to mind.

Why is this motion so necessary when we have plenty of opportunity during the middle of this particular study to ask questions?

Has anyone thought of bringing in the Victoria Police Department or inviting them as a witness so we could ask questions? There's a lot of language in this motion that is asking us to go on the good faith of the Conservatives, which in some cases is in short supply.

I just wanted to make those observations that there were probably other opportunities and more conciliatory ways of bringing this forward during the middle of a study on car thefts.

The Chair: Thank you.

Mr. Genuis, go ahead, please.

Mr. Garnett Genuis: I'd like to propose an amendment based on Mr. MacGregor's excellent suggestion.

I would add at the end of the motion the following: "and invite representatives of the Victoria Police Department to appear before the committee for two hours."

• (1615)

The Chair: Is there anyone else?

(Amendment negated: nays 6; yeas 4)

(Motion negated: nays 6; yeas 4)

The Chair: We're going to continue now with our line of questioning. I believe Ms. O'Connell is up.

Ms. Jennifer O'Connell (Pickering—Uxbridge, Lib.): Thank you, Chair. Thank you to the witnesses for sticking through that.

I want to start with you, Mr. Jack. Thank you.

I think CAA has done a study—correct me if I'm wrong—that found that 33% of Canadians who own vehicles have factory-installed anti-theft systems. I want to know a little bit more.

You spoke in your opening remarks about these anti-theft systems. It's somewhat unfair to put that on the consumer after they've already purchased the car.

Are you finding that there are certain manufacturers whose cars are harder to steal, who are putting in place some of these regulations? I recognize the point you've made in terms of updating the legislation on anti-theft systems and that it is quite dated.

We've heard at committee that some cars are stolen far more often than others and that some in the industry are making headway.

Do you have anything to add to that?

Mr. Ian Jack: I would like to turn to my colleague Elliott in just a moment on this. He's a bit more knowledgeable than I am.

I will make couple of observations.

I think what gets stolen is what's most valuable to potential buyers. I think that our criminal gangs put more effort into figuring out ways to steal some vehicles than others. That's one factor among many.

I think the other point I would make is, again, the importance of a national standard, which is a federal responsibility for new vehicles going forward, so we don't end up with an ongoing game of whack-a-mole where maybe one manufacturer does do a better job, and their vehicles stop getting stolen. But guess what? The theft just moves over to another sort of vehicle.

With those two points, I'll turn it over to Elliott.

Mr. Elliott Silverstein: Thank you.

It's a great question. We certainly know that there are a lot of vehicles that are highly in demand. Part of the challenge we face is that the standards in Canada are grossly out of date. As we look at the industry as a whole, the challenge really becomes that, as some vehicles become tougher to steal, thieves are looking for vehicles that are in demand, and they'll move on to other ones.

We need to update the standards so that all vehicles are safe. It shouldn't matter what make or model we're focusing on. We tell Canadians that they know that their vehicles are safe. We really need to update standards that haven't been looked at since 2007. We really need to look at that as we approach 20 years. There's a lot more that the industry can and should do, because Canadians should not be shouldering the cost of the aftermarket costs to keep their vehicle safe when they are already paying a lot for those vehicles and other types of theft deterrence in their own home.

• (1620)

Ms. Jennifer O'Connell: Thank you.

We've heard at committee—and Mr. Schiefke has raised the point as well—that we're seeing the same trends in the increase in vehicle theft in the U.S. per capita. I was meeting with some of our U.S. counterparts at the border and ATF. Europe is also seeing an increase. While domestic politicians want to play games and try to blame certain legislation, we're seeing an increase around the world. New Zealand, I believe, is seeing the highest number of car thefts that they've experienced as well.

On the manufacturing anti-theft side, it's quite important that we also keep up with international standards or else the value of stolen cars in Canada just goes way up.

Mr. Ian Jack: Absolutely. There are other jurisdictions acting on this as well. To your point, if we don't or if we're slower, we will simply see more car theft in our country than in other jurisdictions. I think, again, that it's a very good argument to be moving as quickly as we can.

My only other observation, with great respect, is that Canadians drive vehicles in Canada and are worried about them being stolen here, not about New Zealand.

Ms. Jennifer O'Connell: It was more about the point that, if we are behind in making these changes and other jurisdictions update their anti-theft legislation, then we will be more vulnerable.

If I have a little time left, I would like to ask the question of Ms. Afzal or Ms. Aimers.

I was just in B.C. this past weekend doing a ride-along with police in Chilliwack. They had a bait car and were talking about it. They did talk about the fact that they are not seeing the increase in auto theft in B.C. This was the RCMP there representing what they're seeing on the ground.

Do you have any idea why B.C. is not experiencing the same levels of auto theft?

Ms. Shabnem Afzal: One reason we're hearing that from our law enforcement partners is that there are a number of variables, obviously. It's never black and white; there are lots of grey areas. We can say definitively that we feel that the organized crime aspect of vehicle theft has not really reached B.C. so much. We have organized crime of all different types, but in terms of auto theft, we're not seeing that same rise in organized crime.

Part of that may be due to the fact that our borders are connected to different countries, obviously. This is speculation and not for me to say, obviously, and enforcement could answer these questions way better. We just don't have the same markets that eastern Canada has to be able to ship to. The western side of Canada does not. Most of our vehicles that are stolen remain in Canada. We have a good rate in that seven out of 10 vehicles are recovered. That was the last I heard from our enforcement partners.

Also, the nature of the vehicles that get stolen here hasn't really changed to the newer models with the anti-theft devices. It's really mostly still the older vehicles. They're usually stolen, from what we're told, in the commission of a crime or those similar types of things.

The Chair: Thank you.

Ms. Michaud, you have six minutes, please.

[*Translation*]

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

My sincere thanks to the witnesses for being with us today.

Throughout our auto theft study, my focus has been on figuring out the causes and identifying solutions with the help of the various witnesses. I want to hear their recommendations on what else the government can do to prevent auto theft.

For the benefit of my constituents, I'd like to take this opportunity to ask, first, the ICBC representatives and then the CAA representatives about how auto theft impacts victims.

We know that insurers paid out more than a billion dollars for auto theft claims in 2022. How do you determine car insurance premiums? Can you tell us more about that? Is auto theft affecting rising insurance premiums across the country? I would think so, but I'd

like to hear from you. If someone's vehicle is stolen, how much would their premium go up? What about people whose vehicles are stolen over and over again? In a case in Montreal, a resident had their vehicle stolen and was able to get it back, but it was stolen again a few months later. What effect does that have from the insurer's standpoint? How do you calculate that and how does it affect the people who insure?

The ICBC representatives can go first.

• (1625)

[*English*]

Ms. Kelly Aimers: Is it possible to repeat that question in English?

[*Translation*]

Ms. Kristina Michaud: I can repeat it in French. You should have the interpretation.

Could you please explain to the witnesses how the interpretation works?

[*English*]

The Chair: Ms. Aimers, are you receiving interpretation? No? Did you choose the channel at the bottom of your screen? I believe there's a globe. Have you got it? Okay.

Do you know what, Ms. Michaud? You start over.

[*Translation*]

Ms. Kristina Michaud: All right. Thank you.

I'll start over. First, though, ladies, could you tell me whether you are hearing the interpretation?

Is it working? Great.

I said that, since the beginning of our study, my focus had been on finding out the causes of the auto theft problem in Canada, as well as identifying stakeholders' solutions and recommendations for police, the Canada Border Services Agency, or CBSA, and even the government, which could introduce new legislation or regulations.

Today, for the benefit of my constituents, I want to take advantage of your expertise, as insurers, to ask how the rise in auto thefts across the country is affecting people. We know that insurers have paid out more than a billion dollars for auto theft claims.

What impact is the rise in auto thefts having on the premiums of people whose cars haven't been stolen and those whose cars have? Is there a difference? Are everyone's premiums going up? How does it work? How do you go about determining someone's premium?

I will have more questions afterwards.

[English]

Ms. Kelly Aimers: I can take the insurance part of it.

If you do have an auto theft claim, it does not impact your insurance costs unless you have multiple claims in the last few years. If you have, I believe, three or more, it will have an impact on your insurance costs. It actually will have an impact on the deductible that you pay, but otherwise, it's not your fault if your car is stolen. If you have an anti-theft device in your vehicle, we do provide a \$100 rebate off your deductible if that device has been tampered with in the event of a claim.

[Translation]

Ms. Kristina Michaud: If I understand correctly, someone who's had multiple claims in the past few years would see their premium go up.

Do the claims have to involve car theft, or does the reason for the claim not matter, say a broken windshield or a fender-bender?

If the person's vehicle is stolen a few months or years later, their premium can go up. Is that right?

• (1630)

[English]

Ms. Kelly Aimers: If you have multiple thefts it will increase the deductible. I think it's a minimum deductible of \$2,500 if you have multiple thefts in the last few years.

[Translation]

Ms. Kristina Michaud: Thank you.

Thank you for being here, Mr. Jack.

In your opening statement, you made some very important points, especially the fact that cars are easier and easier to steal. Do you think technology is having a negative impact in this situation?

It seems as though cars you unlock the old-fashioned way, in other words, with a key, are less likely to be stolen than new cars, whose systems are all technology-based. You can connect your car to your cellphone, for example.

Does new technology create an additional risk for manufacturers?

Mr. Ian Jack: We don't think so.

We can't turn back the clock either. Do social media platforms have a harmful effect on teens? Yes, but that's the world we are living in. The same goes for the technology used in vehicles. Things have to advance. Consider that iPhones use two-factor authentication. Why wouldn't today's cars have that?

I'm going to turn the floor over to our expert, Mr. Silverstein.

[English]

Mr. Elliott Silverstein: Thank you.

I think when it comes down to it, a lot of people like the technology for convenience, but we're trading off the safety right now and that's a big challenge because we are at a breaking point. We have

the challenge of how frequently thefts are happening. We have people who are struggling to find vehicles when they're stolen.

While people love the push-button starts and they love the convenience of what's in their vehicles, we can't trade off the safety aspect. There's the fact that the standards have not been updated in nearly 20 years. There's the fact that when people have to get new vehicles they're facing higher interest rates, they're facing higher prices for the new cars and they're having their family life disrupted because they can't get rental cars. All these pieces come together.

Is the technology a blessing or a curse in some ways? People love it, but it's also been a bit of a driver for the challenges we face. I think we need to make sure that standards are updated because safety should be paramount for everybody.

[Translation]

Ms. Kristina Michaud: Thank you.

Mr. Jack pointed out that cellphones use face recognition technology now, and wondered why vehicles don't do the same. It only makes sense. As I've told other witnesses, when I park my car, I get a notification on my cellphone telling me where it is. Wouldn't it be possible to have a similar mechanism, where you get a notification when someone else starts your car? It can't be that difficult to set something like that up.

The committee met with car manufacturers, and they were rather quick to lay the blame at the door of organized crime, saying that police and the government needed to do more. Do you think car-makers have a role here as well and should be doing more?

[English]

Mr. Elliott Silverstein: I'll speak on this.

I think that automakers play an important role in this. We've talked to our members and we've done public polling. We know that over 80% of those surveyed feel that manufacturers need to do more.

We know that it is a challenge, and certainly organized crime is a component of this. Everybody plays a role in this, whether you're an insurer, government, law enforcement, but manufacturers as well. We all have to play that important part.

At the end of the day, two-factor authentication is important. However, when we hear of proprietary issues and other challenges like that, we have other industries like banks that have been able to keep their proprietary pieces in order and still ensure the safety of their industry. We need to do the same here for Canadians because a vehicle is somebody's second-largest purchase outside of their home and we need to have the standards and the security up to date to make sure that they have the peace of mind that their car is going to be there in the morning.

The Chair: Thank you, Mr. Silverstein.

For our last questioner in this round we have Mr. MacGregor, please.

You have six minutes.

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

I'd like to start with ICBC.

It's great to see some fellow British Columbians join us at committee and provide our west coast perspective on this issue.

I just want to talk a little bit about the bait car program, because that did have remarkable success when it was first introduced. I can remember at the time it seemed like the B.C. government was actively trolling car thieves, daring them to go and steal a car, knowing that a bait car was out there tempting them to be caught.

We know from the Vancouver Police Service press releases at the time that the program had remarkable success in driving down rates of auto theft.

Can you just tell us, have those rates remained fairly consistent? Is the bait car program still owning a little bit of responsibility for keeping those rates low, or is it a broader question with a lot of different things at play here? Could you just add a little bit more to that, please?

• (1635)

Ms. Shabnem Afzal: There is no doubt that the bait car program is still a successful program. There are also many other aspects in terms of IMPACT, the team and how they are integrated, and different police units and police departments that are all involved in the proactive tackling of auto crime. I think the important thing here is to remember that the IMPACT program is an enhanced program in terms of fighting auto theft. We're not just relying on baseline enforcement against auto crime through the various police departments, but it's actually this concerted data-driven program across the province of B.C. Of course, bait car is part of that program, so yes, bait car is very successful. We've seen a lot of auto crime go down due to that, but there are always new tactics being employed by thieves and there's new technology in vehicles as well. It continues to have success, but in the space of the larger program, IMPACT, I think it's important to remember the integrated approach across B.C. has led to much success in this space.

Mr. Alistair MacGregor: I know that ICBC offers discounts on premiums for anti-theft devices on vehicles. Does ICBC have to re-examine that policy, given that thieves seem to be easily able to overcome some of the standard anti-theft devices that are part of cars that are manufactured today? Is that something the insurance industry as a whole is pressing the car manufacturers to do better on? Is that a big part of the conversation here?

Ms. Shabnem Afzal: Well, we've actually not seen the same increase in auto theft in B.C. so—I hate to say this—we still have quite low rates compared to the rest of the country. As I said, there are a number of different variables involved here, so we haven't seen fit to change our incentives in terms of anti-theft devices yet. Hopefully, that remains the case and we continue to see a decline in auto theft...over the last five years. As Kelly was saying earlier, we've seen a recent decline as well, just from last year, so we have

not been thinking about changing any of our insurance premiums as a result.

Mr. Alistair MacGregor: I'm going to turn to CAA for my last two minutes. I certainly appreciate the times BCAA has been there to help me on the side of the road, so we definitely know the value of your organization. Coming off that conversation, when you look at insurance models in the rest of Canada, in provinces where auto theft is a growing concern, what is CAA's position on what role insurance companies can play, in their conversations with auto manufacturers, on offering discounts for anti-theft devices? If you can add a little bit more to that conversation, I think that will be helpful.

Mr. Ian Jack: I'll turn to my colleague in a moment: This is what he does for a living, especially in recent months and years.

It shouldn't be up to your house insurance to take care of faulty door locks because people who build homes can't be bothered to have proper locks on the front doors. We can do our part, and we do our part—and Elliott will speak to that in just a moment—but a lot of people have to do their jobs here, I think, and not just either insurers or individuals buying their own aftermarket anti-theft devices to try to stop having their vehicle stolen.

• (1640)

Mr. Elliott Silverstein: By and large I think insurance companies have tried to do a lot thus far. We've tried to really focus on the most actively stolen vehicles, which doesn't impact the entire population in terms of their policies. I think the idea about working together on that is a noble one, and I think it's one people would love to work on, but we need to get the manufacturers fully to the table. They are at the table, but they need to do more on this to actually be part of that solution. Right now, deferring it by saying it's an organized crime issue—while that is the epicentre of where it's coming from—time and again doesn't get us to the end state. We need to get to that end state as soon as we can because we can't afford, day after day, to pay out the claims we're doing.

Mr. Ian Jack: If I might just add to that, it was striking to me that at the auto summit we participated in, at a table even bigger than this one, everybody around the table said, “*Mea culpa*, we have something to do,” including CAA. As I said in my remarks, we need to do better consumer education. The only people at the table who took no responsibility at that time were the manufacturers.

The Chair: Thank you.

Thank you to all of you for your testimony.

We will now suspend for a couple of minutes to enable you to leave and to get our new witnesses ready.

Thank you so much.

• (1640) _____ (Pause) _____

• (1645)

The Chair: I call this meeting back to order.

I would now like to welcome the witnesses for our second panel.

In person, from the Halifax Port Authority, we have Captain Allan Gray, president and CEO; and by video conference, from SHIELD automotive cybersecurity centre of excellence, we have Mitra Mirhassani, professor.

Up to five minutes will be given for opening remarks, after which we will proceed with rounds of questions.

I now invite Captain Gray to make an opening statement.

Please go ahead.

Captain Allan Gray (President and Chief Executive Officer, Halifax Port Authority): Thank you.

We at the Port of Halifax recognize the importance of this issue and sympathize with the thousands of Canadians who have been impacted by these criminal acts. We join Canadians in our concern over the growing problem of auto theft, which has become a very sophisticated crime. Those involved are highly organized. We are committed to working with the government and other supply chain stakeholders to address this issue and broader concerns surrounding the illicit movement of goods and/or people.

Canadian port authorities are delegated with specific and limited responsibilities for port security. Therefore, ports must work closely with their partners, including local police, federal enforcement authorities and the Canada Border Services Agency to achieve security.

When it comes to illicit activity, which also includes illegal drugs and human trafficking, there is no single solution to this problem. There are many groups, and they each have a role to play in terms of enforcement and prevention. Developing a strategy that will involve all groups working together is necessary.

For many years now, I have worked closely with the International Maritime Organization, or IMO. I can tell you that port security has been on their radar for a long time. At the start of the century, ports used to be open environments, but 9/11 changed all that. The IMO developed measures designed to combat terrorism—not specifically contraband—and continued to focus on security in a

holistic way. The international ship and port facility security code was adopted in 2004. Following that, the IMO continued its work on maritime security. The IMO code of practice on security in ports offers a valuable framework for developing and implementing security strategies and identifying potential risks. There is a call at IMO to broaden the scope of the ISPS code to consider organized crime. I would recommend that the Canadian representatives on IMO engage with and support this initiative.

As it relates to security and containers, I want to talk a little bit about the process of packing and moving containers through a terminal. In general around the world, and also in Canada, there is no X-ray or scanning of export boxes unless the country of destination has a security requirement for a preload scan. This is because most border controls are focused on the import of illicit materials and not the export.

Typically, a shipping container is packed at an off-site location. The paperwork is done. That includes a self-declaration of what's inside. The container is closed and marked with a customs seal. When a container arrives at a terminal by either truck or rail, the container number is matched to the booking number, the customs seal is physically checked to see that it hasn't been broken, the serial number of the seal is noted against the container and then the container is put in the stacking area for export. Neither the terminal operator nor the port authority have the right to hold or open a container unless directed by the shipper, the shipping line or the CBSA.

In terms of documentation, there is a bill of lading, which is a legal contract between the shipper and the carrier that shows ownership, and there is a cargo manifest, which lists the contents of what is claimed to be inside the box. On the manifest document, you will find words like “said to contain”, because the only one who knows for sure what is in the container is the one who packed it.

If we consider the effectiveness of scanning export boxes, if the manifest says the box contains household goods but a scan reveals a car inside, then it's reasonable that enforcement agencies know they should be inspecting the container. But if they scan a box that has a car inside, and the manifest says there is a car inside, there is no way of knowing if that car is stolen without opening the container and looking to see if the VIN matches the ownership documents. Even that check might not catch a VIN that has been tampered with.

The point is that spending a lot of money on scanners may not fix the problem, and scanning every single container may not fix the problem. What we do know is that scanning containers takes time, resources and trained people. It's simply not realistic to scan every single export container or even the majority of them.

The other gap is the port security clearance. In many other jurisdictions, security credentialing is a requirement for anyone who must access a secure area more than once in a calendar year. That's not the case in Canada. Currently, there is no consistency in maritime transport security clearance cards between different ports. Every port creates its own card. The inconsistencies make the system vulnerable to fraud. Other jurisdictions have centralized systems with standardized cards, which make it easier to detect forgery and compare a card against a centralized database.

- (1650)

The federal budget proposes funding for Transport Canada and the RCMP to administer a centralized transportation security clearance program, which is a positive step.

We are respectful of the fact that people are concerned about auto theft and the threat of violence in communities affected by this problem. We need a broad solution that is realistic about the level of control required to effect positive change. Relying on port security as the last line of defence may not be as effective when considering such well-organized criminals. We need to consider a more integrated approach to port security that includes all levels of government, and considers the export of drugs and other illicit goods and people.

Thank you.

The Chair: Thank you.

Dr. Mirhassani. Go ahead, please.

Dr. Mitra Mirhassani (Professor, SHIELD Automotive Cybersecurity Centre of Excellence): Thank you.

I'm the co-director of the SHIELD automotive cybersecurity centre of excellence. This centre was established in 2020, right at the onset of the pandemic. However, we've been researching these challenges associated with automotive security and, in general, Internet of things security since 2012 or so.

We created the centre to address three key areas that we saw were lacking. Especially back in 2012, or even in 2020, when we were talking with different ranges of people, they looked at us in amazement and wondered what we were talking about when we talked about the issues surrounding automotive security. A lot of the time, it's mistaken with safety features in vehicles. They are two different challenges and issues. They're interrelated, but not exactly the same.

SHIELD is working with the automotive industry. We have partners coming to us. We can offer solutions for their immediate needs and challenges, but how many of the offered solutions they employ remains with them.

At the centre, other than offering technological solutions for the problems that are facing the industry, we offer training and education with respect to the issues and challenges auto theft has created

in Canada. One of the more challenging issues in terms of security is a lack of knowledgeable people and the ability to attract young minds into this field. We are actively trying to remove the barriers in the field and allow the younger generation to come into it, as well as trying to upskill the current workforce that is in the workplace in the automotive field to be able to understand the new ecosystem of the vehicle.

As much as possible, we try to talk with policy-makers, we attend and are members of different standards committees, and we transfer our knowledge of issues that we have experienced and learned about, which will hopefully be reflected in the advanced science, standards and policies.

Going back to the issue of the biggest challenge in the automotive industry, which is a lack of talent, we currently have a very serious void in our workforce. A lot of organizations working in the automotive industry do not have people with the necessary skills, which sometimes showcases itself in the products that are coming.

However, there are newer standards being developed, and car-makers are slowly adhering to them. In July 2024, they're going to start enforcing some of the world's harmonization standards. We are hoping that there will be more investment in the training and education of students and professionals.

Unfortunately, the day that automotive cybersecurity becomes an issue will come earlier than we predicted. Our prediction was that with the rise of AI, we would have more devastation and more problems, especially with fleets of vehicles. Because auto theft is a public issue, it has created this attention to the details related to automotive cybersecurity.

We are hoping that by working with different organizations, different institutions and the private and public sectors, we can rise to some of the challenges in this field.

Thank you for having me today.

- (1655)

The Chair: Thank you, Professor Mirhassani.

Now we will move right into questioning, with Mr. Shipley for six minutes, please.

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

Thank you to the witnesses for being here today.

I would like to start first with Mr. Gray.

Mr. Gray, you may have touched on this, but I just want to recap.

In your experience, what percentage of shipping containers would you say the CBSA is scanning at the Port of Halifax?

Capt Allan Gray: In the Port of Halifax, it's probably only somewhere between 3% and 5%. It's not a large volume. That's only import containers, so—

Mr. Doug Shipley: I'm sorry. I meant export, but I didn't say it.

Capt Allan Gray: For export, it would be zero.

Mr. Doug Shipley: There is absolutely zero scanning of export.

Knowing that, do you have any statistics?

Has there ever been a car successfully seized at the port?

Capt Allan Gray: There hasn't been, that I am aware of. I have heard anecdotally that cars may have moved through the port, but I haven't seen a seizure of a vehicle in the port.

Mr. Doug Shipley: How long have you been there, Mr. Gray?

Capt Allan Gray: This is my fifth year at the port.

Mr. Doug Shipley: Do you think that the security clearance program administered by Transport Canada for employees working at your port is adequate for preventing the infiltration to the public sector?

• (1700)

Capt Allan Gray: No, I don't.

Could I expand on that?

To my point, in other jurisdictions—I come from Australia, which is a similar jurisdiction—with the security cards that exist, if you have a requirement to access a security-regulated area more than once in a calendar year, then you're required to have a transport security clearance card. That means transport drivers or workers who come down to do maintenance in the place. It doesn't matter where you're from, if you have to access a security-regulated thing more than once a year, you must have a security clearance.

The other point is that the card for the Port of Montreal and the card for the Port of Halifax, whilst they will have some similarities in the information on them, are different. We can have different coloured backings and that. In other jurisdictions, they have security hologram films that can be purchased only from the government. They're put on the card and every card is identical throughout the country. It is very difficult to forge, from an organized crime point of view, because you can pick that up through the hologram systems.

We don't have that in Canada.

Mr. Doug Shipley: Thank you.

My next question will be for Ms. Mirhassani.

I'd like to first just have a quick discussion.

I brought up an example of a carjacking a while ago, which happened in the Toronto area. It's maybe been misused a couple of times in this committee. I had mentioned some very young people—one as young as 11—and there were three or maybe four of them. I can't recall exactly. It's been brought up a couple of times that they were so young and yet they could get the technology and steal that vehicle. They didn't use any technology. They opened the door, pulled out the driver, beat him, stabbed him and drove away. I just want to make sure that it is clear that there was no technology used by those perpetrators.

For my next question, Mitra, we've heard from several witnesses that the age of car thieves is becoming quite young. While we know that many of these thieves obtain stolen vehicles through violent means such as carjacking and home invasions, I'm wondering how easy it is for a young person to obtain...and learn how to steal a vehicle other than, as I said, pulling a driver out and driving away.

Dr. Mitra Mirhassani: Stealing a car has basically always been a little bit easy, but these days, because of information sharing and the availability of resources online, information is much easier and readily available. Let's admit that our newer generation is more tech-savvy than some of us, so if they are seeking information, they can easily find that information.

There are different resources and there is actually no way to stop those resources from sharing the information about the weaknesses of certain technologies. There is no way for censuring those data sources. Having said that, there are also always stories of young hackers who hack into extremely secure databases and datasets. It's always basically a little bit of interest and intrigue for the younger generation to go for these newer ways to find information and employ it.

Mr. Doug Shipley: Thank you.

I have one minute. I'll make this very quick, then. From your perspective, what recommendations do you have for manufacturers to improve the vehicle's resilience to getting stolen or cyber-attacks?

Dr. Mitra Mirhassani: Unfortunately, there is not just one piece of advice. We have to remember that although we like to have our cars to be smoother, have a lot of safety features, be connected and do a lot of amazing things, the manufacturing of automotive vehicles has turned into a super complex issue, as well as the whole engineering and concept. I'm afraid there is not just one piece of advice that I can give them. You usually ask them to apply a "secure by design" principle, but we are saying that even that design principle and engineering protocol fails to secure such a complex system.

• (1705)

Mr. Doug Shipley: You're saying, basically, that no matter what they can do, they're still going to get stolen.

Dr. Mitra Mirhassani: Unfortunately, there is no way to secure a system or a car 100% and say, "It's done and we are okay."

The Chair: Thank you, Mr. Shipley.

We go to Mr. Schiefke, please, for six minutes.

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

I add my thanks to our witnesses for appearing before us today.

Ms. Mirhassani, I'm going to direct my questions to you today. Thank you for bringing your expertise to our committee on this very important issue.

We've had representatives of the car manufacturers appear before committee, and I asked them questions about how much they were investing in research and development to make their cars harder to steal. They weren't immediately forthcoming with that information. I learned that there were submissions to INDU, the industry committee, where they were asked similar questions about what they were doing to make their vehicles harder to steal. I've read all of those, and basically, none of them were forthcoming on what they were doing, citing that they didn't want to share this information as it would tell the criminals what they were doing to stop them from stealing their vehicles.

There was one, however, that I came across, which was submitted by Ms. Audrey Dépault, who's the senior adviser for public policy and development for Tesla and who, without even being requested to submit information, did so anyway because Tesla's actually quite proud of what they've done to make their vehicles—according to the Highway Lost Data Institute of the United States—between 2020 and 2022, the hardest vehicles to steal. We're not talking about the high-end vehicles. We're talking about the Model 3, which actually comes at a manufacturer's suggested retail price below the average now.

There are a couple of things that they include in the basic vehicles, such as the “sentry mode”, which has a live camera, so whenever there's suspicious activity around the vehicle it sends to the owner's phone a live feed of what's happening around their vehicle. They also include relay attack mitigations. We heard from the Montreal police as well as the Sûreté du Québec that we have 15- to 20-year-olds who are buying \$100 gadgets on Amazon and stealing the messaging that's coming off the vehicle. Well, they have something that mitigates that attack, and they have what's called “PIN to drive”, which allows the driver to secure a four-digit verification code that must be entered before the vehicle can be driven.

What, amongst what Tesla's doing, to be the most successful...? By the way, I don't drive a Tesla. I have no interest in Tesla, but I'm very intrigued by what they've been able to do. What is Tesla doing that the other manufacturers simply cannot get or are not doing?

Dr. Mitra Mirhassani: In terms of identifying the differences among Tesla and the other carmakers, basically, they all make cars but they're making cars very differently from each other. Tesla has its own weaknesses that I'm not going to disclose here.

In terms of auto theft, yes, they have a little more success. They also have bounty hunting and participate in a lot of competitions, basically encouraging people to help them in identification of flaws of their systems. The same sometimes goes for the other carmakers as well.

Some of the technology is easier to be adopted by the other carmakers, but remember that the manufacturing styles among Tesla and the other carmakers are completely different. That renders the ability of some of those carmakers to jump easily into modifying their process, so as a result they are a little slower in adopting solutions that, for example, Tesla—

Mr. Peter Schiefke: Ms. Mirhassani, I'm on limited time here, and I'm really trying to get as much of your expertise into this report as possible.

We're looking at ways we can strengthen our ports. We're looking at ways we can strengthen law enforcement. One of the aspects I really want to get to the heart of is what we can do as far as regulation is concerned, because we've heard that hasn't been updated in almost 20 years.

What do we need to be doing as a government?

What would a regulation look like that we could put in place and would be the most effective in producing vehicles that are harder to steal? What would be included in that regulation, and what would that have to look like for it to be effective now and in the future?

• (1710)

Dr. Mitra Mirhassani: Although the regulations haven't been adjusted in Canada, the SAE standards and ISO standards and the world forum for harmonization of vehicle regulations have recently been adjusted.

In Europe, those will be enforced starting in July 2024. This means that vehicles will have to have the secure-by-design principle and some level of testing for security incorporated before they can start selling new car models.

Mr. Peter Schiefke: Based on your experience, will that be effective in curbing the rise in vehicle thefts we're seeing in Europe, the United States, Canada and all around the world?

Dr. Mitra Mirhassani: I'm a cynic and a researcher, so my answer has that bias in it. I always go by the fact that no vehicle is 100% secure. If we close the door on this side, there will be another way to open it.

Mr. Peter Schiefke: If we were to adopt standards similar to those that have just been passed in Europe, would that be beneficial to Canadians?

Dr. Mitra Mirhassani: Yes, certainly.

Mr. Peter Schiefke: Thank you very much for your testimony today.

The Chair: We're moving on to Ms. Michaud, please, for six minutes.

[Translation]

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

Thank you to the witnesses for joining us.

Ms. Mirhassani, I'll be asking my questions in French, but first, I'd like to make sure that you are getting the interpretation. I see that it's working. Thank you.

I'll continue along the same lines as my fellow members.

Following the auto theft summit, the government announced that it planned to amend the Radiocommunication Act in order to restrict the sale, possession, distribution and importation of devices used to steal cars. The government reiterated that intention in its recent budget. The amendments would give law enforcement agencies the ability to eliminate hacking devices from the Canadian marketplace. It didn't take long for people's reactions to come in.

Someone from software development firm JuniperOne explained that the software defined radio, or SDR, devices that the federal government is proposing to ban are pretty basic, saying that a Flipper Zero can't be used to unlock or start newer vehicles. As we know, thieves tend to target much newer vehicles. We also know that they don't necessarily have to use a technological device. As Mr. Shipley pointed out earlier, a thief can simply use violence to steal a person's car.

Do you think restricting the availability of these devices is really the way to go, or is it just a waste of time since organized criminals will find a way to get their hands on the devices anyway? Obviously, we need to work on a number of fronts at the same time.

[English]

Dr. Mitra Mirhassani: Unfortunately, I believe that banning those technological devices is not going to help. The thieves are certainly not going to abide by the law. They'll get them from other sources.

The only thing it did was create a bit of panic in my students, who wondered what they would use to learn. Banning those devices is not going to impact auto theft. It's probably only going to harm training and education.

On one small note, yes, those devices cannot open some of the cars, but we tested them and, unfortunately, they work on some of the new car models.

[Translation]

Ms. Kristina Michaud: Thank you.

The president of Équité Association appeared before the committee, and she talked about vehicle anti-theft technologies that had been deployed by automakers in the United Kingdom, and security patches that prevent the CAN bus or controller area network from being overcome.

Apparently, these technological solutions are rather simple and would prevent vehicles from being stolen, but the push for automakers to deploy them came after some insurers decided to stop insuring the top most stolen vehicle models.

Do you think Canadian automakers should follow suit and deploy these technologies?

Do you think we're going to end up in the same boat, where insurance companies decide to stop insuring certain vehicle models because they are stolen too often?

• (1715)

[English]

Dr. Mitra Mirhassani: I don't think I can answer on behalf of insurance companies. They have to answer that part.

Yes, there are certainly some technologies we can use to basically make it more difficult. The thing is that although any system is not 100% secure, if we make it difficult or create a process so that it takes longer to attack or get into the vehicle, that could be a deterrent for whoever is trying to steal that car. In a way, if a car takes 15 or 20 minutes to steal because of some of the principal challenges that are placed along the way, that will deter the thieves.

Unfortunately, I can't say what the insurance companies can do. I can only answer on the technology side.

[Translation]

Ms. Kristina Michaud: Thank you.

I have a question for Mr. Gray about the Port of Halifax.

Your situation seems to be quite different from the one at the Port of Montreal, which has really come under fire. Its geographic location makes it a hub for exports and stolen vehicles.

I want to be sure I understood something you said earlier. You think that focusing on port security is the last thing we should be doing to combat the rise in auto thefts.

Is that actually what you said? If so, why?

[English]

Capt Allan Gray: If you were relying on the port as a last resort or as your only defence, it would not be very successful because of the number of issues around documentation. We don't physically open every box because it's sealed prior to arrival. If that was your only line of defence, it would not be a very successful one. We need a broader one.

To me, one of the problems is that we don't have good data transfer from agencies to ports and terminals. We can't access CBSA data because of the way the legislation is written. Once it goes into the CBSA, it can't come out. Therefore, we have issues in data sharing amongst ports, terminal operators and supply chains.

Things like that would help us notice the anomalies. If more data could be shared amongst the agencies, players and stakeholders, that would be there.

The other side is that if you don't have a good security card or clearance system that's deep enough into the system, organized crime will get hold of trusted insiders or threaten people within the chain. That makes it much easier to pass through. Boxes will be missed on that sort of thing.

To me, it's increasing data and also broadening the card for more people.

With the IMO legislation or rules that they're talking about, affiliation with or belonging to organizations that are affiliated with organized crime will discredit you from being able to get a security card. That is a big shift that's coming in many other countries. It's a really important shift.

Even if you don't look at the contraband—I've raised human trafficking and drugs as additional to cars—it's just the fact that terrorism can use organized crime as a means of passing dangerous goods. It's something that has to happen.

The Chair: Thank you, Mr. Gray and Ms. Michaud.

Mr. MacGregor, please.

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

I'd like to start my first questions with SHIELD.

Professor, in your opening statement, you mentioned artificial intelligence and touched on the fact that it's going to lead to a lot more problems in the future. Certainly, at this committee, we've touched on the subject of AI. I have spoken to stakeholders who are experts in the field, and there is a great deal of concern. We are really at the beginning stages of how this technology can be employed, but the use by malicious actors in developing a code to foment cybersecurity attacks is a very real concern.

You mentioned the Internet of things and how so many of our household devices—and, of course, vehicles—are increasingly going to be connected to the Internet. I know from my work on the agriculture committee that this is increasingly the case for a lot of our farm equipment as well, with that real-time data link so that farmers can know exactly how their machines are operating.

I'm just wondering if you could touch on that. Also, I know of AI as an offensive tool, but do you foresee also its applications in defence? Can you expand a bit more on that with this particular problem?

• (1720)

Dr. Mitra Mirhassani: Sure.

Yes, AI is currently used in both cases, on both sides, as a tool to create defence and to basically identify, for example, if you are you, through some of the very simple applications. Face recognition on your phone or some of that might have AI to basically some capacity. It's used also on the other side as an offensive to attack the other systems. It's a tool, so it basically plays both sides.

What we at SHIELD are very much concerned with is that AI is usually used as a very good tool, but as long as it's working. What if someone or a malicious actor attacks that tool and breaks it? That will create a lot more problems, essentially, so we have been advocating a lot about responsible and secure AI. With these devices and as AI is basically now going everywhere, it's left to its own devices. No one is thinking about protecting the AI unit itself to make sure that it's working appropriately or as intended.

The problem is that if you are not securing and not taking care of the AI unit that is going to be used for protecting us, if that AI centre's own activity gets attacked, then basically the consequences could be a bit more damaging than what we are seeing in some cases—

Mr. Alistair MacGregor: Thank you for that.

I want to move on to another question.

You are very knowledgeable about the technology that exists to deter car thefts. I agree with you that no technology is going to be

100% foolproof, but some are better than others and can greatly decrease the chances that a successful theft will happen.

My colleague Mr. Schiefke, in previous committee hearings, in looking at the sticker price of cars, has alluded to the profits that car manufacturers are making. Given your knowledge on the existing technology that's out there and the costs associated with it, in your opinion, what would be a reasonable amount for a car company to invest in a vehicle—a dollar figure per unit—to make sure that it had much less likelihood of getting stolen?

Dr. Mitra Mirhassani: That is a very hard question to answer. I don't have that number about the actual numbers that can go into the vehicle to make it secure, so unfortunately I can't answer that question.

Mr. Alistair MacGregor: Is there anything more broadly speaking? We've heard from a number of witnesses who have said that car manufacturers are not living up to their end of the bargain in this whole issue.

Dr. Mitra Mirhassani: In the big picture, yes, there are certainly things that the car manufacturers can do. Some are taking this more seriously than others.

Since 2016 and before, some of the car companies and OEMs actually started looking into the issues of cybersecurity. However, the technology is advancing much faster than we can find the loopholes in the security and fix it. A lot of times when the car is on the market, the security loopholes are just identified. We are playing a game of cat and mouse a bit with this feature, and that could be one of the reasons why the carmakers are falling behind. The process of adjusting their technology might take them some time to get into the market. That could be one of the reasons.

• (1725)

The Chair: Thank you.

We're now moving on to the second round, and we're going to have a hard stop, so we can get at least four questioners in.

Mr. Kurek, you're up first, please, for five minutes.

Mr. Damien Kurek: Thank you very much, Mr. Chair. I'll be splitting my time with Mr. Viersen here.

Mr. Gray, I have a couple of questions for you.

You mentioned before that when it comes to Transport Canada security clearance, currently connections to organized crime are not a consideration when somebody is granted security clearance to a port.

Capt Allan Gray: Yes. Currently, it's focused on weapons-based crime—so, things that are associated with terrorism—because the transport security card came in from the IMO's ruling, which was based around the prevention of terrorism. Their focus at that time was really around weapons or violence-related crimes.

Only now the IMO is saying that there's too much evidence that says that organized crime is related to terrorism and that this should be extended, but—

Mr. Damien Kurek: I'd say it's certainly past due for that recognition. That is astounding—that that's not the case—and that's certainly something that needs to be addressed.

I'm curious. Could you provide any data as to the number of interactions that your port has with the CBSA, the RCMP, CSIS, CSE and other federal investigative entities in terms of containers that might be going out from your port? We've heard a lot about Montreal. We've heard a lot about Vancouver. However, I'm just curious. Do you have that information? Is that something that you could provide to this committee?

Capt Allan Gray: I could have a look into it, but in my own interactions, we very seldom talk about cargo going out of the port. Most of the focus is on cargo coming into the port. Even then, it's kept very close to the chest. There was a recent announcement about a drug bust in Halifax. As the port authority, we weren't aware of that occurring until after the event.

So, they keep that sort of information very close. That's something that I'm not used to from my previous jurisdiction where we had a trusted information network, and multiple agencies would come together and share information around multiple things, including terrorist information and other organized crime information.

Mr. Damien Kurek: I have just one final question. Just answer yes or no. Is that something that needs to be improved in Canada?

Capt Allan Gray: Yes.

Mr. Damien Kurek: Okay, thank you very much.

Mr. Viersen.

Mr. Arnold Viersen (Peace River—Westlock, CPC): Hello, Mr. Chair.

Thank you to the witnesses for being here today.

Professor, I am old enough to remember... I'm an auto mechanic, and I worked at a Chrysler dealer for a long time. I remember when the SKIM code came in on the Jeep Grand Cherokee in 1998. As that SKIM technology came in, we watched a nosedive in vehicle thefts in general. However, with that, over time, we've also lost the column lock. I don't know if people remember this, but you used to have to put the key in the side just to get the steering wheel to turn. Most modern vehicles don't have that anymore. This is more of a hardware rather than a software situation.

Is there any desire from the industry to bring back the column lock or other hardware? There's been a lot of discussion around software, but is there any discussion around hardware pieces to prevent theft?

Dr. Mitra Mirhassani: Just remember that hardware is also easy to capture, so with those mechanical car keys, you also have the ability to reproduce and remanufacture them. If you're thinking about organized crime, they certainly have access to generating those car keys mechanically and distributing them through their system.

As to whether industry is planning to bring that in, I am not aware of such motivation.

Mr. Arnold Viersen: The column lock is just an example of a hardware theft deterrent. We see the aftermarket steering wheel lock; people put The Club on the wheel. Those are aftermarket. Is there any desire from the industry to bring in something else that we haven't heard of yet?

Dr. Mitra Mirhassani: I'm not aware of anything in that regard.

Mr. Arnold Viersen: The SKIM key that Chrysler came out with in 1998 had been, until about 2015—maybe you can correct me on that... Up until 2015, people hadn't been able to get around it. Today they can just duplicate the key, the electronic side of that key, really quickly, so that has basically made it moot. Is there any light at the end of the tunnel around the reintroduction of something like that?

• (1730)

The Chair: Answer very quickly, Ms. Mirhassani.

Dr. Mitra Mirhassani: I'm not sure if they are going to bring those cases. If there is any intention of that, I'm not aware of it. However, at this stage of information availability, I'd say that even those mechanical car keys can be manufactured rather easily.

The Chair: Thank you.

We're moving on to Mr. McKinnon.

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

Thank you to the witnesses for being here.

I'm going to direct my questions to Mr. Gray.

We are particularly interested in the ports, because we see them as the last line of defence for interdicting the export of stolen vehicles. I understand this doesn't really apply to you. You don't have data in this regard. However, I want to look a little further up the logistics chain.

You mentioned that many of these containers are filled at terminals in the vicinity, presumably. I'm wondering if any of these terminals have some sort of trusted status or bonded relationship, so you can decide whether, based on whoever filled the container, this manifest may be more or less reliable.

Capt Allan Gray: Some packing houses are customs warehousing, so they've gone through a customs system to have customs brokerage. There would be some that are more reliable than others. I would think you would approach it in the same way you risk assess import cargoes: look at where they're coming from, who has packed it and what the shipping line is. You would take a similar approach, such as whether they put good electronic seals on—that sort of thing. If they're a reliable, trusted customs broker, it would be less likely you're going to have a problem there. If it's something packed by an individual or by a warehouse you're unaware of, that would be a higher risk profile.

Again, the port doesn't have that information. The CBSA would have that information going through. We don't get told the origin of that cargo. We aren't given that information.

Mr. Ron McKinnon: Would it be helpful to have it be required to offer you that information, so that, if and when you were able to, or had a need to scan export containers, you might be able to filter them on that basis?

Capt Allan Gray: Yes, that sharing of information would help the risk assessment process. It all helps. The more information we get, the more the terminal can make assessments. If the CBSA were advising us that these are higher risk and they want them scanned, it would be a process that would help.

Mr. Ron McKinnon: Who—if anyone—is responsible for verifying that the manifest matches the contents? Is there someone who can be held accountable if they find out there's a significant material error or discrepancy there?

Capt Allan Gray: The person who packed and declared the goods is the person responsible. However, in most cases, this discovery is only made at the destination port. There's no way to see into a container, other than through scanning.

As I said, if the paperwork has been falsified, as well, you could have a situation. For example, if it says it's a car and the paperwork matches, that's fine. You don't know whether the car was stolen or if the ownership is correct.

Mr. Ron McKinnon: Who puts the customs seals on these containers? Is that the CBSA themselves, or it some agent or some bonded or trusted person?

Capt Allan Gray: It's whoever packs the container or the customs broker associated with it. It's not necessarily a trusted network with customs.

Mr. Ron McKinnon: It seems very important that we be able to identify who placed a seal on it and whether they in fact verified the contents of the container. Are they able to verify the contents of the container, do you think?

Capt Allan Gray: The person who seals it should be verifying the contents, or whoever declares on the paperwork should verify it. Again, in an organized crime situation, there are a lot of trusted insiders, so the person who's declaring could be a trusted insider. Unless you have multiple people in the chain who are testing that pro-

cess, it could still slip through. That's the nature of smuggling for whatever it is that you're smuggling: It's trusted insiders who are the ones, quite often, responsible for falsifying documents.

Unless you're going to open every container.... It's the same as imports. We don't open every container. We don't scan every container that comes in. It's risk assessment-based. You would have to take a similar approach, a risk assessment-based approach.

The more you can do to validate the security credentials of the people involved in handling the cargo along the chain, the more likely you are to reduce the number of trusted insiders you have in the system.

• (1735)

Mr. Ron McKinnon: I guess that's what I'm driving at, that we need a way to filter the vast number of containers we have that we need to be looked at and be able to identify who is responsible.

Would you see this as a recommendation that we should put forward, that the logistic chain and the provenance of these containers be provided to the ports?

Capt Allan Gray: Yes.

The Chair: Thank you Mr. McKinnon.

Thank you, Mr. Gray, for your co-operation.

Go ahead, Ms. Michaud, please.

[*Translation*]

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

I'm going to continue with Mr. McKinnon's line of questioning.

One of the solutions you recommended was better information sharing among partners, the port authorities, obviously, the CBSA and law enforcement. That seems appropriate given that the police officials we heard from said that would be a good practice. They also recommended a review of the security clearance process. Personally, I wasn't aware that Transport Canada was in charge of that, so I asked to have the Minister of Transport meet with the committee to explain how it all works and what can be done to improve the clearance process.

You also mentioned the CBSA's mandate and the fact that border controls are focused more on imports than exports. Even so, the CBSA doesn't inspect every container leaving the country.

Should we change the rules or the mandate of the CBSA? I'm not sure whether we have the ability to do that or whether the agency has the staff it would need. Isn't it a good idea to do just that and pay close attention to exports? Should we do what Mr. McKinnon was talking about and look at who is putting a seal on the containers before they are shipped out of the country? Do we need to tighten the rules around when changes to the manifest are allowed, including the number of hours before shipping, to ensure that changes to the manifest aren't made once the container is shipped? Do you think implementing those measures would be a positive step?

[English]

Capt Allan Gray: Yes, I think it's important that most customs authorities around the world are focused on protecting a country and looking at goods coming in. Whether it's quarantine or bringing pests, bugs and other things or illicit material in, their primary focus is about protecting a country, so their resources are allocated that way. I suspect, from a resource allocation perspective, that it would be challenging to take a complete focus on export.

It's co-operation between countries' enforcement agencies that is important. If you're going to try to stop the movement, that relationship with other international customs agencies to say, "Look, we have a problem here of export, and we're trying to get hold of it, but

we need your assistance in blocking it at the receivable end" would help, so it's not so much our doing all the work; it's a combination of work. More information along the line and better security clearances will reduce the risk and then make it more able to do, as I mentioned, risk-based assessment; therefore, a portion of the export market could be checked based on a risk assessment.

[Translation]

Ms. Kristina Michaud: Thank you.

[English]

The Chair: Thank you.

We want to thank those in attendance today, and we appreciate your testimony.

I have a couple of quick notes.

The subcommittee meeting is on Thursday, and a notice went out.

Finally, the Minister of Public Safety will appear on car thefts on Thursday, May 9, and potentially the Minister of Transport. We're still working on the Minister of Transport's schedule.

With that, we are adjourned.

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <https://www.ourcommons.ca>

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante :
<https://www.noscommunes.ca>