HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

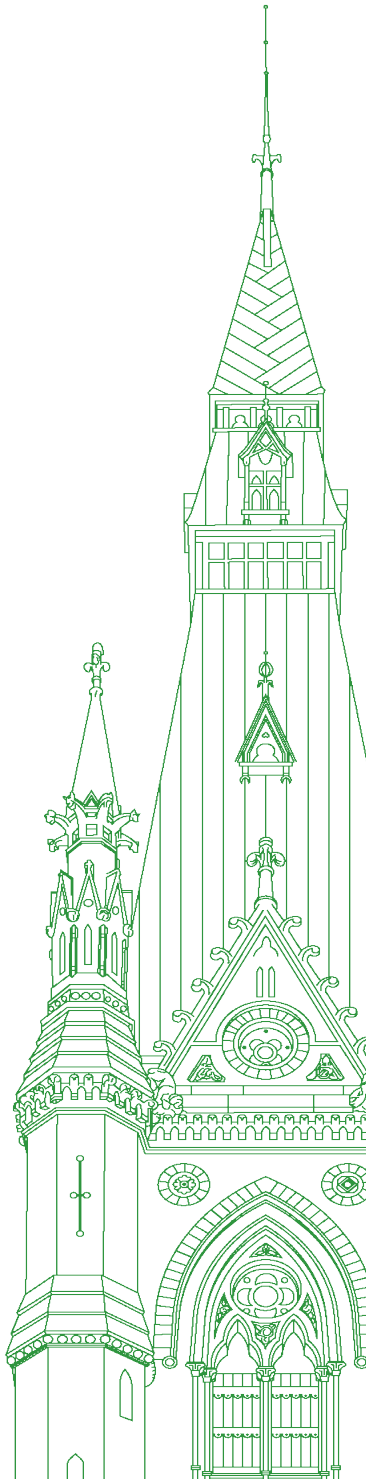
44th PARLIAMENT, 1st SESSION

Standing Committee on National Defence

EVIDENCE

NUMBER 049

Friday, February 10, 2023



Chair: The Honourable John McKay

Standing Committee on National Defence

Friday, February 10, 2023

● (0845)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Colleagues, I call this meeting to order.

I want to deal, first of all, with the balloon motion.

Is this motion still up in the air or are we going to land it?

An hon. member: We're going to land it.

The Chair: Who would like to move it?

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): I move:

> That the Standing Committee on National Defence invite the Minister of National Defence, the Hon. Anita Anand, and the Deputy Commander of NORAD, Lt. General Alain Pelletier, to provide a briefing of no fewer than two hours concerning the foreign airship from the People's Republic of China that recently violated Canadian airspace, and that the briefing be held in public within the next four days.

The Chair: Do we have any excessive debate?

Mrs. Shelby Kramp-Neuman (Hastings—Lennox and Addington, CPC): I'd like to make an amendment so that the motion reads:

> That the Standing Committee on National Defence invite the Minister of National Defence, the Hon. Anita Anand, to appear prior to March 11, 2023, and that the Deputy Commander of NORAD, Lt. General Alain Pelletier, and the Commander of the RCAF, Lt. General Eric Kenny, appear within the next week to provide a briefing of no fewer than two hours concerning the foreign airship from the People's Republic of China that recently violated Canadian airspace, and that the briefing be held in public.

The Chair: Okay. Are there any other...?

Are you speaking to the amendment?

Mr. Bryan May (Cambridge, Lib.): I have an additional amendment, but I can speak to the amendment.

The Chair: Let's do it on the amendment.

Mr. Bryan May: We agree, obviously, with wanting to host these meetings. The only language I would add, to the attendance of officials, is a line that says, “all other appropriate officials”.

The Chair: Or “relevant officials”...?

Mr. Bryan May: Yes, “relevant officials” would be fine.

We are fine with the 11th date. In terms of trying to keep this clean, we'd prefer “as soon as possible”, but that would be up for debate.

The other slight change I would make is changing the name of the object to “high-altitude surveillance balloon”, which is the common language for this.

The Chair: Okay. I guess we're not going to land this balloon any time soon.

Let's go through these things backward and see whether we have consensus back and forth.

The last one you moved was “high-altitude surveillance balloon”.

Do we agree to that?

An hon. member: Yes.

Mrs. Shelby Kramp-Neuman: Chair, we accept the friendly amendments.

The Chair: Do you accept all three?

Mrs. Shelby Kramp-Neuman: Yes.

The Chair: Okay. You accept all three.

(Subamendment agreed to)

The Chair: We've accepted those. Now, has the other side accepted Shelby's amendment to Cheryl's original motion?

Mr. Bryan May: Yes.

(Amendment as amended agreed to)

The Chair: Therefore, we have a clean motion.

Mr. Clerk, do we have a clean motion at this point?

The Clerk of the Committee (Mr. Andrew Wilson): More or less, yes.

The Chair: Okay.

Mr. Blaine Calkins (Red Deer—Lacombe, CPC): Which one is it? Is it more or less?

The Chair: We're going to go with more.

With that, we all know what we're voting on.

(Motion as amended agreed to)

The Chair: Thank you, colleagues. I won't make any more lame jokes about landing this balloon.

With that, we can now turn to the main business of the meeting. We have with us two witnesses: Dr. Thomas Keenan, professor at the University of Calgary; and Alex Rudolph, from Carleton University, who is a Ph.D. candidate.

Since Professor Keenan got up earliest in order to be able to give this testimony, we should defer to him.

Sir, you have five minutes. Welcome to the committee.

Prof. Thomas Keenan (Professor, School of Architecture, Planning and Landscape, University of Calgary, As an Individual): Thank you very much.

Mr. Chair, distinguished committee members, ladies and gentlemen, thank you very much for inviting me today.

I would like to speak to you about a subject that I have been studying for years as a researcher, a University of Calgary professor and a fellow of the Canadian Global Affairs Institute. It's artificial intelligence. I believe it's going to revolutionize everything, including cybersecurity and cyberwarfare, and a lot quicker than most people expected.

AI is all over the news right now, because of things like ChatGPT. I was teaching it 30 years ago, and many of my students who built backpropagation in neural networks then have gone on to do great things. Artificial intelligence now does everything from detecting tiny tumours on MRIs to helping cities optimize traffic signals.

There is a dark side to artificial intelligence, something we call adversarial AI. My fear is, like so many industries, our defence folks will embrace AI without fully understanding how it can be used against us.

You probably heard about those snoopy information kiosks in Cadillac Fairview shopping malls. The company was chastised by the Privacy Commissioner for secretly collecting data on five million people, including their approximate age and gender. How did they know your gender? They made an educated guess using AI and facial recognition.

For 25 years, I ran a program for highly gifted high school students called Shad Valley Calgary. It culminated in a science fair where they showed off their work. One year, they built a neural network to predict your gender from body measurements, like hip to waist ratio. One corporate sponsor stopped at their booth and, yes, he was rather portly. They measured him, and they told him that with 84% probability he was female. That was actually a good thing, because those students realized that AI was just making informed guesses.

If you go to ChatGPT or similar programs, they will give you answers that don't have any percentages or degrees of uncertainty. They read like statements of fact. They can be dead wrong. I asked ChatGPT, “Is Danielle Smith intelligent?” It came back with, “I cannot accurately determine who you are referring to as Danielle Smith.” It does say that Justin Trudeau is widely considered to be intelligent. What's going on here?

I lifted the hood on the current free public version of ChatGPT. It's knowledge base ends at 2021. At that time, Danielle Smith was an unemployed talk radio host. She didn't rise to her current political prominence until 2022. I'm sure that ChatGPT's database will be updated, and its answer will be different in the future.

That's another problem. You can ask an AI bot the same question twice and get wildly different answers. It doesn't tell you why.

Don't get me wrong, I love AI and its potential upside. There are plenty of companies that will tell you all about that, since they have products to push. My mission is to make sure we look at the risks and apply this tool intelligently.

Here are three things to worry about as AI moves into national defence.

First is the source of training data. Most AI is trained on public domain data that might be inadequate. We've seen issues with facial recognition having trouble recognizing people of colour, because it was exposed mainly to white faces. In the defence industry, much of the most important data is not in the public domain.

Second is the lack of ethics in AI. We all remember Tay, the Microsoft chatbot that went off the rails and started spouting Nazi ideas and foul language and referred to feminism as a cult. Tay was just learning from people who interacted with it. Unfortunately, that's what it talked about.

Third, malicious actors can try to poison the database. A woman has been trying to rewrite the Wikipedia entry on Nazis to paint them in a favourable light. Way back in 2003, Democratic supporters linked the terms “miserable failure” on Google to George W. Bush's official White House biography. When you did a Google search for “miserable failure”, up came the president's picture.

● (0850)

If you don't want your political profile to be linked to miserable failure or worse, you should heed what ChatGPT has to say about this very committee:

> The Standing Committee on National Defence,
> Within the House of Commons, its power immense.
> A place where decisions are made with care,
> For the safety and security of all to share.
> With members from every party, they convene,
> To review and assess, and to make things clean.

Wait a minute. To make things clean...? What does that even mean? Only ChatGPT knows for sure, and it's not telling.

Thank you very much.

● (0855)

The Chair: Thank you, Professor Keenan. We don't generally get poetry about our own committee

Mr. Blaine Calkins: We do, but it's not that nice.

The Chair: It's not nearly as good as that. I don't think we should be putting to votes the intelligence of either of the political persons mentioned, including the present company.

I noticed that you have a very interesting map behind you: submarine cables of the world.

Prof. Thomas Keenan: Yes, sir.

The Chair: That in and of itself is a pretty interesting discussion. However, we're on to our next witness.

Mr. Rudolph, you have five minutes, please.

Mr. Alexander Rudolph (Ph.D. Candidate, Department of Political Science, Carleton University, As an Individual): Mr. Chair and members, thank you for inviting me to speak here today.

I am Alexander Rudolph, a doctoral candidate at Carleton University and a Canadian Global Affairs Institute fellow. I am researching how and why countries develop the institutional means to conduct cyber-operations. As part of this research, I look extensively at Canada.

I'll divide my comments between two themes today: the cyber-threat domain and current trends in cyber-conflict; and Canadian cyber-defence.

The cyber-threat domain can best be described as existing in a perpetual state of conflict and tension. This is a result of its long-standing architecture, which, although improved over the years, is still very much present and can produce vulnerabilities and exploits. These vulnerabilities and exploits ultimately form the basis of malware in cyber-operations that we view as cyber-conflicts or cyberwarfare.

Right now, there are a few major trends to keep in mind.

The first is that no norms or international laws currently exist to address cyber-conflict and cyberwarfare. To be clear, this is not the stance of Canada and many NATO allies. Presently, there's no international regime or consensus on how to address international law in cyber-conflict.

The second is that ransomware has completely revolutionized how adversarial states and non-state actors view cyberspace. As an example, North Korea has been very prolific in using cyber-operations, particularly ransomware, to find ways to evade international sanctions, but this also overlooks how Russia and many other actors use ransomware in cyber-operations as well.

There's also the commodification of “zero days”. Zero days are unknown vulnerabilities in a system, computer or piece of software. The commodification of zero days and exploits has significantly contributed to the proliferation of cyber-capabilities and the ability to conduct cyber-operations. In particular, China mandates that all new vulnerabilities or zero days be reported to the government within two days. This is the first type of law of its kind, tending to go against existing norms in an industry that has generally favoured maximum protection of users.

I would be remiss if I did not mention Russia's unprovoked invasion of Ukraine and utilization of cyber-operations with near-simultaneous joint kinetic military operations. I want to echo the comments made at the previous meeting, but I also want to highlight the type of operations that have been most numerous. While the Viasat attack is quite noteworthy, there have also been at least 16 wiper malwares deployed into Ukraine to specifically target Ukraine to date. These are viruses that destroy data completely to prevent recovery. This is novel because it's not what most criminals do. The way they gain money is by holding data for ransom and extorting individuals. Wiper malware has the sole intention of destroying data in systems. It's noteworthy that 16 have been deployed, which is more than there have been in the past 20 years.

I'll now move on to Canadian cyber-defence and what all these trends mean for Canada.

In particular, Canada needs both a whole-of-government cybersecurity response and a very targeted cyber-defence response. Cyber-defence, in particular, includes the CSE and Canadian Armed Forces. Today, I'm going to focus on the Canadian Armed Forces.

The CAF is, in no way, prepared to face cyberwarfare in the event of a conflict. I further question to what degree they are able to even co-operate and work interchangeably with allies, including the United States.

● (0900)

The reasons for such are numerous, but I'll go over a few today.

At best, Canadian cyber-defence policy can be described as incomplete, ad hoc and inconsistent in strategy and definition with Canada's allies, particularly the United States. I will use CSE's definition of a defensive cyber-operation as an example. The way that CSE in Canada uses it, it generally refers to a purpose—to attack back or to respond to an active threat to Canada. This isn't traditionally how defensive cyber-operations are discussed or explained. They're generally not about an active response back.

While this is maybe just legal language, it creates difficulty in speaking with allies on the exact same topic when you're talking about defensive cyber-operations, which are traditionally just on one's own networks, similar to cybersecurity in many ways. If you're talking about offensive actions, it is a big disconnect between thinkers in Canada and allies on how cyber-operations are conducted and understood.

The Chair: Mr. Rudolph, I think I'm going to have to ask you to get the balance of your presentation in during the questions. You're past the five-minute mark. I apologize for that, but it is what it is.

With that, Madam Gallant, you have six minutes, please.

Mrs. Cheryl Gallant: Thank you.

My first question would be for Dr. Keenan.

Should there be an open discussion and agreement in Parliament outlining the limits of use of AI for the military?

Prof. Thomas Keenan: Yes. I believe there should be. There is a policy on the responsible use of AI on the Canada.ca website. I read it and it's fine, except that it's dated 2021.

The first point I want to make is that you have to do this continuously. It's not one and done. There definitely should be a policy. I've consulted with my friends in industry, particularly Microsoft, because they've put many millions of dollars into ChatGPT. There are moves to ethical AI.

My suggestion would be that, yes, that should be done. It should be done in consultation with industry and academia.

Mrs. Cheryl Gallant: How should Parliament balance the safeguards from the dark side while encouraging the positive discoveries? How do you seek that balance?

Prof. Thomas Keenan: That's a million-dollar question. We'd all have the Nobel Prize if we knew that.

The answer is to keep track. I'll give you one little example.

Google has a search engine. We all know about it. By using Google, someone was able to find out the name of a young offender whose name was protected by a publication ban in an Ontario case. The way it worked was that so many people said, "Johnny Smith is a bad boy," that when you Googled "Johnny Smith" and the heinous crime that happened, Google formed the association. When they were asked about that, Google said, "Oh, we didn't do it. None of us did this. We didn't break the publication ban"—but their algorithm did.

The point of that story is that you have to keep watching. You have to keep looking for examples like that. That was several years ago. I don't know that Google has actually done anything to cover themselves—you might ask them—when they potentially break a publication ban that's ordered by a judge.

It's continued vigilance.

● (0905)

Mrs. Cheryl Gallant: Mr. Rudolph, how does Russia use malware or ransomware during kinetic operations versus just for blackmail and money?

Mr. Alexander Rudolph: I'll use one example from a recent invasion. They deployed what looked to be ransomware that was encrypting the system and saying, "Your system is now locked down and your data's encrypted. You now need to pay us *x* dollars." Behind it, they were actually deploying wiper malware to destroy all the data.

It's always on a case-by-case basis. Russia in particular uses it to target specific systems and organizations during their invasions, while traditionally it's been used with the intelligence services in various ways to extort money.

Mrs. Cheryl Gallant: At what point should a company, the private sector, get in touch with somebody from government? When should the military be alerted that they have to harden their cybersecurity even more because there is an attack under way, and then link it to the possibility that it's just the beginning of an escalation for a kinetic interaction?

Mr. Alexander Rudolph: It's always quite difficult to determine if it will lead to a kinetic response, as cyber-operations can be escalatory. It's oftentimes how it is combined with other efforts. A cyber-operation itself is not necessarily going to cause kinetic damage, but how states respond or use that operation in unison with kinetic operations is the great concern, which is what Russia has attempted to do in Ukraine.

Mrs. Cheryl Gallant: We have a new cybersecurity bill that has been proposed, but it's geared more towards civilians. Should there be another cybersecurity bill specifically to address your concerns for the military? Should it dovetail with the civilian cybersecurity? At what point does a civilian attack interface with military infrastructure? How can that happen? Has it happened?

Mr. Alexander Rudolph: I can't comment if it has happened in Canada or not. You would need to ask the military if there have been any attacks on military infrastructure. It's often difficult to determine. With critical infrastructure, much of it is dual use. If it targets explicitly military infrastructure, I would consider that an attack on the military, but I would say that there needs to be another bill to address cyber-defence in the armed forces and CSE. There particularly needs to be a formal force and command structure that organizes CSE and the military, as it currently doesn't exist. It's very ad hoc.

Mrs. Cheryl Gallant: Thank you, Mr. Rudolph.

The Chair: Thank you, Ms. Gallant.

Mr. Fisher, you have six minutes, please.

Mr. Darren Fisher (Dartmouth—Cole Harbour, Lib.): Thank you, Mr. Chair.

Thank you, gentlemen, for being here.

When the Rogers system went down, I was on the way to Cape Breton, Nova Scotia, for work meetings. It basically shut down all our critical infrastructure. You couldn't get gas. You couldn't go to an ATM machine. Nothing was working. Then I think about Atlantic Canada when Fiona hit. Gone are the days of having a newspaper on your doorstep. You couldn't get news. You couldn't pay a bill. You couldn't do anything when our critical infrastructure went down because of Fiona.

I highlight those two examples essentially to show the reliance on our critical infrastructure and how important it is to everybody in every neighbourhood across the country and around the world.

I guess I'll go to you, Mr. Rudolph, first.

How can the federal government along with provinces and territories better protect and defend this critical infrastructure that is so absolutely necessary in the lives of Canadians?

Mr. Alexander Rudolph: It's quite a big question. I will first state that there needs to be a lot more funding to the Canadian centre for cybersecurity and ways for the centre to interface with the rest of government and for the government to look to what the provinces need and what the federal government needs, as there are very different, diverse needs for both to provide services, as you mentioned, but also protect the government from threats.

The holistic cybersecurity response that I mentioned before would cover aspects of critical infrastructure that are needed, but the Canadian Armed Forces are still very much reliant upon many public systems, in part because their internal systems are very insufficient. There is flatly a need for greater funding and a need to address how to respond to bigger incidents like that and what role the Canadian centre for cybersecurity has in these, similar to how the Cybersecurity and Infrastructure Security Agency in the United States does.

● (0910)

Mr. Darren Fisher: When we think about emerging technologies, things that Canadians adopt on a mass scale, like cellphones and things like that, which trends represent the greatest cybersecurity risks? What initiatives could the federal government undertake to mitigate these risks when you think about smart phones and things like that?

Mr. Alexander Rudolph: The use of ransomware, I'd say, affects phones just as much as our regular computers—and particularly with the proliferation of surveillance software, which many of you have probably heard of, such as Pegasus or NSO Group. The greater proliferation of these zero days and malware has made any piece of technology a target for potential profits or for targeting by adversarial states.

This is part of the constant tension that I referred to, and part of the responsibility of the government is to face these threats and to address criminals by working with allies to arrest and target some of the ransomware actors who were named yesterday, I believe it was, or the day before.

Canada, I would say, is currently a low-level player in this. They are helping.... CSE is well regarded around the world, but.... The Canadian Armed Forces could do more but simply can't. There are many other initiatives across the government that could look to what they are really contributing to their own department's cybersecurity and the constituents they're helping.

Mr. Darren Fisher: Dr. Keenan, do you want to jump in on this?

Prof. Thomas Keenan: Were you inviting me?

Mr. Darren Fisher: Yes, sir.

Prof. Thomas Keenan: Wonderful. Yes, first of all, I wanted to discuss something that I call the “ransomware from hell”. It's a scenario that I made and that I think needs to be aired here.

Let's say you're a hospital administrator. You get an email and it says, “One of your employees just clicked on that phishing email from a Saudi prince and now we're inside your system, but we are not going to hold your data for ransom or erase it.” They say they have a much better idea: that they've traversed your network and they know that you have 75 Picker X-ray units, four Siemens MRIs and 2,000 BD infusion pumps. They're all there and they all have vulnerabilities.

There are zero-day vulnerabilities in many technologies that the manufacturers don't know about.

They say they're for sale on the dark web. They say they bought them on the dark web and they need to get their money back, so you have to pay them $10 million in Bitcoin by tomorrow, and, if you don't, they're not going to encrypt your data—that's so old school—they're just going to kill a patient every day.

I did look up an article from Israel on “Seven Ways to Kill a Patient with a Picker X-Ray Unit”: from hitting them physically with it to giving them too much radiation.

The reality is that I took this to a bunch of hospital administrators in the U.S., and they said that either they would pay the ransom—and I said, “Okay, great, then they'll be back for $20 million tomorrow”—or they'd ignore it. I said, “Well, then, you'll be on the front page of the New York Times under 'Hospital Kills Grandma by Refusing to Pay Ransom'.”

They also said they'd try to air gap it. This is where we get technical. They'd say that they will separate all the different hospital systems so that they can't do this. My medical colleagues says that's nonsense because that Picker X-ray unit has to talk to the doctor, the lab computer and the intraoperative MRI. My point is that it's a tightly connected network.

The answer is—and I've taken this to everybody I know who's smart—that there is no answer.

● (0915)

The Chair: Thank you, Mr. Fisher.

There is no answer.

[*Translation*]

Mr. Garon, welcome to the committee. You have six minutes of speaking time.

Mr. Jean-Denis Garon (Mirabel, BQ): Thank you, Mr. Chair.

Thank you for being with us, Mr. Rudolph.

I have a question for you.

It has recently come to light that the federal government is doing substantial business with private firms. McKinsey has been mentioned a lot, and there are others. Departments with extremely sensitive activities do business with these firms, including the Department of National Defence and the Department of Immigration and Citizenship. We have learned that some of these firms, including McKinsey, had dealt extensively with companies controlled by the Chinese regime.

Do you think we should pay particular attention to this issue and that we should be very careful about the firms we do business with in Canada? Is it completely normal for the Department of National Defence to enter into very large contracts with firms that deal with the Chinese government?

[*English*]

Mr. Alexander Rudolph: I would agree that it is a major risk, particularly with.... I don't recall the name of the communications company that was recently suspended because of ties to Chinese firms.

I'd say that is a constant, ongoing problem, as we have seen evidence that China will actively taint supply chains to try to implant surveillance capabilities. The most recent one, I believe, was almost a full fleet of cars in the U.K. that were found to be bugged through this manner.

At the same time, with certain other firms.... I want to parse the different risks between, let's say, large consulting firms and those at the end of the supply chain as two completely different risks. In cyber-defence and cybersecurity, McKinsey and these large consulting firms are, really, the big names in the business that will be doing much of this business. There really is no getting around them.

When you are taking into account the massive inflation and the massive competition to get these skilled individuals, you can't necessarily compete with them.

[*Translation*]

Mr. Jean-Denis Garon: If you will allow me, Mr. Rudolph, I will continue.

There is the Group of Five, among others. Since you say that some of these firms are unavoidable, don't you think it would be better for Canada or the federal government to have a much more effective selection and transparency regime? That way, when Quebeckers and Canadians see the federal government doing business with these organizations, they will at least have an idea of the information that has been disseminated or the information to which these organizations have had access. We know that China has extensive means for espionage, cyberwarfare, and so on, and that these firms are also doing business with China.

Do you think we have to take a step towards transparency so that Quebeckers and Canadians are less worried, whether these fears are rational or not?

[*English*]

Mr. Alexander Rudolph: I will completely agree that there is a need for more transparency, I'd say, across the board on Canadian cyber-defence policy. Most of my research is from looking at audits and looking at departmental results, and then I'm surprised that people are surprised by what I know about the Canadian Armed Forces.

As much as I know broad themes, there are still a lot of gaps in my knowledge. That's simply because the Canadian Armed Forces doesn't want to tell you and because they are prevented from doing so. It's very much a policy problem.

I really want to stress that there is a difference between the transparency and putting more demands on the Big Five or these firms, because there are already quite a few demands.

[*Translation*]

Mr. Jean-Denis Garon: You said something interesting. You mentioned that the lack of transparency, particularly within the Department of National Defence, is so endemic that it can prevent Canadian researchers from doing research on the subject.

Is that what you said to me?

[*English*]

Mr. Alexander Rudolph: I would agree. It's endemic to the system.

Recently the National Security and Intelligence Review Agency found out that there were 180 independent databases in the Canadian Armed Forces, meaning that you need personnel management, not information management, in order to access much of this data.

● (0920)

[*Translation*]

Mr. Jean-Denis Garon: In closing, I have a question for Professor Keenan.

We know that social media plays a very big role in surveillance and artificial intelligence. A lot of Canadians and Quebeckers give their information, which feeds the algorithms. They give their information without knowing what they are dealing with. There is obviously a surveillance capitalism, and we know that these images, these photos that feed the algorithms are part of the problem.

Is the Government of Canada doing enough to support Canadians in protecting their information? What tools are available to the Government of Canada to improve the protection of our digital identity? We know that once you lose it, it's very hard to get it back.

[*English*]

The Chair: Unfortunately, Mr. Garon has left you 20 seconds to answer that good question, so be very brief, please.

Prof. Thomas Keenan: Thank you so much for mentioning Shoshana Zuboff's idea on surveillance capitalism. My son is actually a cybersecurity researcher and worked with her on that book.

There is no question that we give up too much information on social media. There is a wonderful video on The Onion, a satire site, in which Mark Zuckerberg is honoured as CIA agent of the year because he got people to give up so much information about themselves—where they're going to go, what events they will attend. If you want to arrest them, you just have to look at their schedule.

Absolutely, we need a greater awareness. There's a reality there that people love sharing information. It's not necessarily a good thing. At the very least, everyone needs to look at who gets access to their information. Is it you, your friends, the friends of your friends or the whole world?

The Chair: Thank you, Mr. Garon.

Mr. Boulerice, welcome to the committee. You have six minutes, please.

[*Translation*]

Mr. Alexandre Boulerice (Rosemont—La Petite-Patrie, NDP): Thank you very much, Mr. Chair.

It is a pleasure to be with you this morning.

Mr. Keenan, I really liked your reminder that artificial intelligence systems can be fed by preconceptions and biases that designers can install in the learning system. You also talked about the ability to poison the database by changing the conversation.

Am I wrong in saying that you could use artificial intelligence to create fake accounts on social media that will change the conversation and then contaminate other artificial intelligence systems, which were using that database in their learning? So it would be a war of artificial intelligence that would come and spoil other artificial intelligence systems. This is starting to get a bit complicated.

[*English*]

Prof. Thomas Keenan: I want to mention that I have a wonderful graduate student, Anika Kale, who has been studying intelligence curricula around the world, particularly from the point of view of gender. She finds that there is almost no awareness of gender in there.

You are absolutely right. One source can pollute another source, and there's really no control on that. The best thing to know about this is that AI generally doesn't explain itself. It gives you an answer. My big objection to ChatCPT is that it makes that answer look very authoritative when it's making it up out of nowhere. I got it to write a poem once, and it put a disclaimer at the bottom that I thought was very interesting. It said that this was a creative work and it didn't really have any facts in it.

You are absolutely right. One data source can poison another data source. I have no doubt that intelligence agencies around the world are busy trying to poison our wells of open-source data right now.

[*Translation*]

Mr. Alexandre Boulerice: Does the malicious use of artificial intelligence, especially on social media, represent a potential danger to the quality of our democratic life and encourage the rise of extremism and populism?

[*English*]

Prof. Thomas Keenan: There's no question that we've seen this in U.S. presidential campaigns and other campaigns. Bots are created for the explicit purpose of getting people riled up. Sometimes they'll do both sides; they'll do the left and the right. The reason is that they want to sow discord in the United States. You can probably think of what countries are doing this.

I want to mention technology—because it was mentioned before—and where the risks are. The American military tried an e-voting project where soldiers who were posted overseas could actually e-vote. I was asked to comment on the security of the system. It was great. You had to do a video selfie of yourself, and you really proved who you were. However, some of those soldiers had cellphones that were made by Huawei, Xiaomi, Meizu. Here you had the end point, the cellphone, that could be vulnerable. It's the weakest link theory. That could be the way in which the e-voting system might have been corrupted.

● (0925)

[*Translation*]

Mr. Alexandre Boulerice: This is very interesting. Thank you very much, Mr. Keenan.

Mr. Rudolph, my question is about cyberattacks on infrastructure.

In the 1970s I was very small, but I remember that tourists could not take pictures of power plants or dams, because it was considered critical infrastructure and we did not want the information to spread.

Of course, in 2023, we are no longer there. Today, when we talk about a cyberattack on Canada's critical infrastructure, what exactly are we talking about?

[*English*]

Mr. Alexander Rudolph: I want to first take your example of being unable to take pictures as a security issue. We're now dealing with the greater proliferation of open-source intelligence. We're able to use just Google Maps to conduct that same exact intelligence and analysis that 20 years ago was illegal. Using this kind of open-source intelligence can also feed into operations on critical infrastructure. It is often the individuals, the people, who are the draw or the vulnerability in a system.

Any organization will have professionals to watch this and work on cybersecurity. You look for any weak link in a system. It can be any small thing. If they can gain entry, they will attempt to lock it down and use it for whatever means they have. If it is a state, they'll just lie in wait for a conflict to happen to then initiate it. If it is a criminal, usually it will involve locking down the system, preventing its use, such as the Colonial pipeline attack, and demanding money. If they don't get that ransom, they'll publish that data online, no matter how secret or sensitive that data is.

The Chair: Thank you, Mr. Boulerice.

Colleagues, we have a little more than 15 minutes, and we have 25 minutes' worth of questions in the second round. The math doesn't work, so I'm going to have to take a minute off of everybody's line of questioning, starting with Ms. Kramp-Neuman.

Mrs. Shelby Kramp-Neuman: Thank you.

Dr. Keenan and Alex Rudolph, thank you for your testimony today.

Mr. Rudolph, your comments with regard to being in no way prepared to face cyberwarfare are extremely concerning.

I'm going to start by referencing an article from 2021 from the Canadian Global Affairs Institute where you highlighted the importance and necessity for the CAF to create and operate an effective cybersecurity force. You indicated that, if the CAF cannot fulfill its cybersecurity needs, it may need to rely on the CSE.

In April of that same year, the CAF released the report titled “Evaluation of the Cyber Forces”, in which they highlighted several concerns with regard to the CAF and retention and recruitment.

What sorts of problems would this cause, particularly having civilians taking on roles that would otherwise be filled by armed forces members?

Mr. Alexander Rudolph: As the CSE official confirmed on Tuesday, CSE is able to support and help the CAF on cybersecurity and cyber-defence issues. When doing so, they take on Canadian Armed Forces mandates. That would mean if the CSE were required to be called upon in a conflict, particularly a war, CSE civilians who are assisting the Canadian Armed Forces would be considered combatants in a war.

You have to contend with and understand to what degree this extends to the rest of the organization at that point.

● (0930)

Mrs. Shelby Kramp-Neuman: Mr. Rudolph, how is the CAF's current reconstitution order affecting the development of its cyber-forces?

Mr. Alexander Rudolph: I can't comment too much on that, as the information I have is limited.

I will say that a big reason for the difficulty in retaining those with the skills in the CAF is that they simply don't have the infrastructure and means to actually do the work. There are a lot of bureaucratic walls and slow procurement. They are joining the forces to do this work, but they don't necessarily don't want to be sent out to just set up radios.

Mrs. Shelby Kramp-Neuman: Thank you.

Going back to the original article that I spoke of, you commented that recent information "indicates that the CSE and the DND/CAF are in the [same] planning stages towards a similar type of organization, but public information remains limited on a timeline for its creation."

Could you speak to the lack of information on the initiative and also how it raises serious implications for the CSE's civilian employees? Could you elaborate a little bit on that?

Mr. Alexander Rudolph: I can elaborate as far as I'm aware that it is a plan. That's really the most knowledge I have on that.

From the information that I've heard from officials, it seems the existing relationship is very much ad hoc. They potentially have CSE individuals embedded with the CAF or vice versa. I don't know too much on that, because it just doesn't really exist in open sources.

Mrs. Shelby Kramp-Neuman: With regard to the urgency of solving the aging and failing digital services, why do you think the government has been slow to address the failing system?

Mr. Alexander Rudolph: It's been a long problem that....

Are you referring to just the CAF or broadly in the government?

Mrs. Shelby Kramp-Neuman: I mean more specifically in the CAF.

Mr. Alexander Rudolph: Part of that is the ad hoc process that I referred to. The creation of Shared Services Canada basically gutted the armed forces of their cybersecurity and cyber-talent. The idea of just centralizing it in SSC was a good idea, but it overlooks the central importance of national defence and the digital capabilities for that.

They had—

The Chair: Unfortunately, we're going to have to leave that answer there. I apologize again—insincerely, but I still do it.

Ms. Lambropoulos, you have four minutes, please.

Ms. Emmanuella Lambropoulos (Saint-Laurent, Lib.): Thank you.

I would like to start by thanking Mr. Rudolph and Mr. Keenan for being here with us to answer some of our questions and for giving us their interesting testimony.

I'm going to start with Mr. Rudolph.

You spoke about the fact that currently there is no specific way to address cyber-conflict. Given that the National Security Act could undergo a statutory review in 2023, do you believe there are any changes that should be considered in the course of this review?

How can we strengthen legislation or create legislation? What should we include in that, so that we can prepare Canada for potential cyber-threats or cyberwarfare?

Mr. Alexander Rudolph: Thank you for the question.

I would say the number one thing that Canada needs to do is to state its position on persistent engagement. This is the U.S. strategy of constantly engaging adversarial elements in cyberspace. When you hear about U.S. Cyber Command or NSA conducting offensive attacks in order to arrest or target ransomware operators, this is the type of action that is under persistent engagement.

Canada has voiced certain ways of supporting this, but it's very unclear. The supports to such actions have been very inconsistent.

Ms. Emmanuella Lambropoulos: Okay, it's to be very clear and more consistent in the way that we deal with those threats.

Mr. Keenan, what I'm hearing you say is that we are very vulnerable due to our reliance on technology. There isn't too much we can do about that. I'm wondering if there are any suggestions you would make to that same review—the National Security Act. Are there any changes?

Prof. Thomas Keenan: There's explicitly addressing what we call "hack back" or active measures.

I did question the Canadian Armed Forces. They directed me to the document "Strong, Secure, Engaged". Alex probably knows more about this too. There's a spot in there where it does say that with the right level of authorization we can hack back. The reality is that we're going to have to hack back. It's not really negotiable anymore.

Of course, it becomes a definitional question. I was told at one point that the United States government was looking at physical facilities in Russia that might possibly be victims of an attack. We do know the U.S. government put a virus in printers that went into Iraq and so on. It's going on out there.

I don't think we have a clear policy on it. I think we need to know. I've realized for security reasons that they may not want to be forthcoming about when they actually do it. It seems to me, from what I've been able to find as a civilian, that they are not clear on when they can use active measures.

● (0935)

Ms. Emmanuella Lambropoulos: All right. Thank you.

Mr. Rudolph, my next question is for you again.

I'm wondering if you can give us a bit more of an explanation about the difference between cybersecurity and cyberwarfare. At what point does it become cyberwarfare? What are the overlaps between the two?

The Chair: You have about 10 seconds to answer that question.

Mr. Alexander Rudolph: I'll try to be quick then, which is difficult for an academic.

Cybersecurity is very much holistic, whereas cyber-defence and cyberwarfare are very targeted on the threats, and for the most part include states and not non-state actors. In cybersecurity you're dealing with low-level criminals as well as states, while cyber-defence is targeted, just like national defence.

[*Translation*]

The Chair: Mr. Garon, you have one minute.

Mr. Jean-Denis Garon: Professor Keenan, we've been talking about critical infrastructure. I have in mind electrical grids and hospitals, for example, which are obviously a provincial responsibility.

I wonder if, in Canada, the provinces and Quebec are sufficiently included in the discussions and protocols that would eventually aim to protect our critical infrastructure.

If not, what specifically should be done?

[*English*]

Prof. Thomas Keenan: We need to consult the provinces and the private sector as well. So many of those things are in the hands of private companies. I know there are meetings. I know there is collaboration.

I don't want to bring up the balloon again, but the reality is that people have asked, “What if there was an electromagnetic pulse weapon in that thing?” It certainly is possible that somebody will do a high-level attack on our critical infrastructure. That would require all hands on deck.

I agree that there should be wider consultation. There should be contingency plans. We wouldn't last very long without our power grid, and that's a fact.

[*Translation*]

The Chair: Mr. Boulerice, you have one minute.

Mr. Alexandre Boulerice: Oh, I have one minute!

My question is for Mr. Rudolph.

Your comments about our inability to cope with cyberattacks are quite worrying. We are very dependent on private sector consulting firms, large telecom companies and web giants, who have a lot of control over our lives and personal information.

Are you not somewhat worried by our dependence on all these private companies and our lack of ability to cope at the public level?

[*English*]

Mr. Alexander Rudolph: I'm not at all. I think cybersecurity professionals are just as important as members of the military and of a police force. Sure, they can be viewed as a risk in certain senses, but cybersecurity professionals are integral to the functioning of our society. It would be undue to say that it's entirely at risk, but it's a risk that we have to take into account, as with any organization for that matter.

The Chair: Thank you, Mr. Boulerice.

Mr. Kelly, you have four minutes.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Just taking you back, Mr. Rudolph, to your opening statement in which you said that CAF is in no way prepared for cyberwarfare, you were limited by time to explain the different ways. I think that information is important for the committee and the report we're going to make, so you could take whatever time I have to itemize the recommendations that you would have for CAF to become prepared.

Go ahead.

Mr. Alexander Rudolph: Thank you for that opportunity.

Fortunately, on many of the questions, I've been allowed to expand on many of the points.

The one I don't think I've touched on too much yet is a general lack of cyber-infrastructure in the forces. One part is the slow procurement process, as many of you will be well aware, but it's also not incorporating and understanding the unique challenges and differences that cyber has from a traditional defence sector.

I will preface that I'm still very much a novice in defence procurement, but I'm very much aware that current ITP policies, in many cases, fail to capture investments by large, potentially prime contractors in cybersecurity and cyber-defence. In addition, the slow process is even more damaging to SMEs working in cyber, because they don't have time to waste, 12 or 16 months for an ITQ, when they have funding for maybe a year at the most, if they're lucky, especially when you're dealing with AI and a lot of these advanced offensive capabilities. These SMEs need all the support they can get, and when your only customer is potentially the government, and it is going as slow as can be, Canada isn't necessarily going to be a customer.

● (0940)

Mr. Pat Kelly: Is it fair to say then that PSPC or the Government of Canada's procurement processes are prohibitive for a small or medium-sized enterprise? You can't even deal with the bureaucracy, and you can't deal with the process. Is that correct?

Mr. Alexander Rudolph: I won't say across the board, but specifically with cyber-oriented SMEs, I would say yes.

Mr. Pat Kelly: Let's give you a minute to talk about CSE, because you said that neither CAF nor CSE.... You didn't have as much time to elaborate on CSE, so go ahead with what steps CSE needs to take to get prepared.

Mr. Alexander Rudolph: I would say that CSE is the most prepared, in part as a lot of their planning has been good and a lot of their open reporting on what they've been doing has been fantastic. It's largely that the connections between CSE and the CAF are almost non-existent. It's very informal, from what I've been able to learn.

There needs to be an actual formal command structure in place to mediate what happens in the event of a conflict. Right now what is likely to occur is that it's going to be given to CSE to respond in an active cyber-threat. I believe that there are more formal connections in relations between CSE and Global Affairs than there are between the CAF and CSE.

The Chair: Thank you, Mr. Kelly.

Ms. O'Connell you have four minutes, please.

Ms. Jennifer O'Connell (Pickering—Uxbridge, Lib.): Thank you, Mr. Chair.

Through you, I want to continue on this line of questioning and on some answers from Mr. Rudolph earlier.

I just want clarification. You spoke about transparency, and I wasn't quite sure if you were referring to transparency in policy or the details of these relationships. You talked about databases and that they're all separate databases. Are you talking about the policy around these mechanisms or the details themselves?

Mr. Alexander Rudolph: I would say both. That ad hoc policy that I referred to was very much new policy every year, or finding that our policy last year did not work, so let's do something new. There really isn't much coherency and logic through the years.

Ms. Jennifer O'Connell: I can see that from an academic's perspective, but you would also have to, I would think, appreciate that when it comes to national security and certainly around cyber there is a policy around a need-to-know basis as well. With transparency of policy, I can totally understand that needs to be out there in open source, but in details or databases, I could also see why you would have multiple databases, because not everybody who has security clearance is on a need-to-know basis for every database.

Then if you use the example of Dr. Keenan about cyber-attacks, malware attacks, could you not see the benefit—maybe not from a researcher's perspective—of silos? I can't believe I'm saying this because I've spent many years on finance trying to break down silos between governments or between government departments.

When it comes to actual cyber-information and having a need-to-know basis and not having that balance of having it in the public open-source network. Open source also means our adversaries can also access that information.

I can understand from a research perspective, but don't you think that there is a very real necessary reason to limit some access to the details of how CSE works with CAF and how CAF works with other departments? Do you see the nature of the security risk if that was all open source?

● (0945)

Mr. Alexander Rudolph: I would agree in principle, but I would caution against painting it as black and white in that sense as there are varying levels to this, just as there are varying levels to security clearance. The problem is that these silos exist without much thought to whether this needs to be silos in the first place and to what degree these silos are being detrimental to the actual productive work of the armed forces.

Ms. Jennifer O'Connell: Do you have any examples so that we can delve into that a little bit deeper?

Mr. Alexander Rudolph: The specifics on the databases in question is definitely separate from the policy. The ad hoc nature is very much overall, but the policy that I would really put my finger on that needs to be clarified is CAF's position and strategy related to persistent engagement.

Ms. Jennifer O'Connell: Persistent engagement of what?

Mr. Alexander Rudolph: Persistent engagement is the U.S. strategy of how to respond to adversarial states in cyberspace.

The Chair: Unfortunately, I have to draw this meeting to a close. As you can see from the last three or four questions, we're starting to get to the meat of the issues, particularly CSE's relationship to CAF and the relationship it has with Global Affairs and Public Safety, etc. It's silos. We hope it's not entirely silos because security is security is security.

Also, the persistent engagement issue calls into question CSE's ability to conduct in Canada those kinds of operations. I would invite you, on behalf of the committee, to submit any other thoughts, any written thoughts that you have, because we are going to have to try to arrive at some sort of policy recommendations.

I appreciate both of you making yourselves available today to engage the committee in this very challenging conversation.

With that, colleagues, we will suspend and re-empanel.

Again, I thank Mr. Rudolph and Dr. Keenan, and particularly Dr. Keenan for getting up a couple of hours early. Thanks very much. I appreciate it.

● (0945)

(Pause)

● (0950)

The Chair: Colleagues, we're back on.

Before I ask Kristen Csenkey and Alexis Rapin to make their five-minute presentations, we should take note that our friend and colleague James Bezan is not with us today. The reason why is that his grandson had open-heart surgery yesterday. I'm given to understand that the baby is doing well, but for those of you who know James well, a note would be in order. Given the Laval incident, our guts all turn when it comes to our kids and grandkids—particularly mine, because I have a few grandkids. As I said, those of you who can should send James a note.

With that, I'm going to first call on Ms. Csenkey for five minutes, and then Mr. Rapin for five minutes.

Ms. Kristen Csenkey (Ph.D. Candidate, Balsillie School of International Affairs, Wilfrid Laurier University, As an Individual): Good morning, Mr. Chair, Vice-Chairs, members of the committee and the other witnesses on this panel. I'm honoured to be invited and thank you for the opportunity to speak to you all today.

I would like to acknowledge that I'm speaking to you from the traditional territory of the Anishinabe Algonquin nation, whose presence reaches back to time immemorial and continues today. This land acknowledgement is meaningful to me as a commitment towards reconciliation practices and recognition of our relationship to place and identity.

My name is Kristen Csenkey and I'm speaking to you as a Ph.D. candidate or “all but dissertation” at the Balsillie school of international affairs through Wilfrid Laurier University. My research focuses on cyber-governance and the management of emerging technologies in Canada.

I have the honour of being called by the committee to speak on the study topics of cybersecurity and cyberwarfare. My approach to these topics comes from my personal capacity as a researcher and academic focusing on the governance side of cybersecurity. I have written on issues of relevance to the study topics, including threats associated with cybersecurity, the roles and responsibilities of involved actors, and the intersections with conflict. It is through my research and previous publications that I approach these topics.

In my opening statement, I will focus my remarks on two main points that may benefit the committee in its study. These two main points are, first, that the threats associated with cybersecurity are dynamic and, second, that preparing to address these threats requires coordination and co-operation among diverse actors.

Let me elaborate on each of these points for the committee.

When I say “dynamic”, I mean that cybersecurity is complex, constantly changing and involves multiple actors, contexts and ideas. This is because cybersecurity is an interconnected social, political and technical endeavour, wherein humans and technologies are intertwined. We live in a cyber-physical world, where many aspects of our lives occur in digital spaces with physical linkages. Therefore, threats associated with cybersecurity should include a nuanced understanding of their technological capacity and capability, as well as the role of human actors, especially in interpreting threats and the responses to said threats.

This leads me to my second point. Preparing to address threats associated with cybersecurity requires coordination and co-operation. If we are to speak about the evolving nature of threats associated with cybersecurity, including the technological capabilities and capacities of various actors, we also must speak about how to address them. This point may seem straightforward, but it is not always this way in practice.

I will provide an example for the committee. In a recent journal article, my co-author and I looked at how different co-operating states understand the quantum threat. A quantum threat is a specific cybersecurity threat associated with the capabilities of quantum computers. Among the Five Eyes partners, we found differences in how this threat and its intentions, associated technology, users and potential threat actors were understood in policies. Discrepancies in understanding the threats associated with cybersecurity will have an impact on the roles and responsibilities of actors involved in addressing these threats.

Coordination among diverse actors involved in interconnected political, social and technical aspects of cybersecurity must occur. This could take shape by leveraging existing pathways and expertise beyond a single contextual understanding of the threat. This requires co-operation.

Co-operation is a key part of addressing cybersecurity threats and keeping Canada safe. Canada can leverage existing trusted partnerships to coordinate responses to threats that appreciate the dynamicism of cybersecurity. This could mean fostering informal or formal engagement with other like-minded, high-tech allies to holistically define threats and understand the associated technological capability and capacity, as well as the complex human and technical dimensions of cybersecurity. Prioritizing innovative partnerships may help ensure security, as well as protect and promote Canadian interests abroad.

It is through co-operation and coordination that Canada can work to ensure we remain safe and secure in an already complex cyber-physical world.

I look forward to discussing any ideas and issues raised in the course of my statement during the question period. This concludes my statement.

Thank you for your kind attention.

● (0955)

The Chair: Thank you, Ms. Csenkey.

Mr. Rapin, you have five minutes, please.

Mr. Alexis Rapin (Research Fellow, Raoul-Dandurand Chair in Strategic and Diplomatic Studies, Université du Québec à Montréal, As an Individual): Mr. Chair and members of the committee, good morning. Thank you for the opportunity to be here today.

I am a research fellow at the Raoul-Dandurand Chair in Strategic and Diplomatic Studies at the Université du Québec à Montréal. My research focuses on issues related to cyber-strategy, cyber-defence and more generally on the impacts of information technology on international security.

In 2020 the research team that I'm part of launched a database dedicated to publicly recording geopolitical cyber-incidents targeting Canada, whether it be its government entities, its companies, its research institutions or its civil society. Our feeling at the time was that geopolitical cyber-incidents in Canada were quick to make headlines but were even quicker to be forgotten. We felt that the Canadian public was not fully equipped to grasp the full, cumulative and pervasive character of foreign cyber-operations targeting Canada. Thus, we set up an online and freely accessible directory of geopolitical cyber-incidents aimed at documenting publicly recorded incidents—their nature, their targets and, when possible, their initiators. The aim of the database was also to keep score of foreign cyber-activities targeting Canada so as to provide the public with a barometer of this phenomenon.

Three years later, as of today, our database has recorded 93 geopolitical cyber-incidents in Canada since 2010. Among those, 14 incidents took place in 2022 alone. In fact, we've observed that the frequency of such incidents is clearly increasing. As I mentioned, our work is based on only publicly recorded incidents, which means that many more incidents remain unreported to this day.

[*Translation*]

These 93 incidents include various types of malicious activity: economic espionage against Canadian businesses and universities; covert electronic surveillance of Canadian-based activists and non-governmental organizations; and intelligence gathering targeting Canadian government organizations, among others.

Our data further indicates that the overwhelming majority of these incidents originate from just four countries: China, Russia, Iran and North Korea. While it is not always clear that the governments of these countries are responsible for each of these attacks, there is little doubt that these four states pose major cybersecurity challenges for Canada.

In 2021 and 2022, our team also published annual reports summarizing our key observations of the most recent cyberincidents. These reports were also intended to highlight certain current trends that we felt were critical to Canada's national security.

● (1000)

[*English*]

Our last assessment, published in 2022, focused on the following trends: the growing threat of ransomware cyber-attacks against Canadian entities, sometimes state-sponsored, which may disrupt critical infrastructure or serve as cover for clandestine intelligence collection; the increasingly aggressive targeting of Canadian-based activists, exiles and dissenters by foreign powers for purposes of espionage, intimidation and harassment; and the rise of the cyber-mercenaries industry, which is starting to target Canadian entities, most probably at the request of foreign powers.

Needless to say, these three trends do not represent the whole picture of cyber-threats that Canada is currently facing. The conflict in Ukraine or the constant economic espionage against Canadian research and development, for instance, should also get our close attention.

What I have tried to demonstrate with these facts, however, is that cybersecurity issues are not a futuristic, hypothetical, distant threat for Canada. Cyber-threats are already here with us. While they may appear discreet or intangible, they directly impact the lives of many people in Canada every day.

Hence, I think it is urgent to address these issues more vigorously and also to discuss them more publicly and more frankly. Today's hearing is an excellent opportunity to do so.

I look forward to answering your questions.

The Chair: Thank you, Mr. Rapin.

Mr. Calkins, you have six minutes.

Mr. Blaine Calkins: Thank you, Mr. Chair.

Today has been very enlightening.

I guess the first question I have for either witness is this: If there's an all-out, coordinated cyber-attack on Canada by all the rogue actors in the world, can Canada protect itself? Will our critical systems fail?

Ms. Kristen Csenkey: I can answer that.

Right now, the Government of Canada, through the various departments that are tasked with protecting Canadians and Canadian critical infrastructure, is doing the best job it can. There's always room for improvement, especially when it comes to reporting cyber-attacks. Right now it's not mandatory to report major cyber-attacks. Especially for SMEs, or companies in that category, to have a mandatory reporting for cyber-attacks would help us understand the breadth of the situation. It would also provide us with more information so that we can come up with a better threat assessment, risk assessment and framework to better protect certain industries and private sector companies.

The government is doing the best it can, but we can always do more. Part of doing more is mandatory reporting of major cyber-attacks.

[*Translation*]

Mr. Alexis Rapin: I will answer in French, if I may.

As far as critical infrastructure is concerned, I think there is a risk. Critical infrastructures are indeed extremely important. They are aptly named because they are critical. Cyberattacks on critical infrastructure are a high-risk but unlikely threat.

The fact that cyberattacks on critical infrastructure are a high-risk threat means that, of course, you have to think about them, prepare for them and have plans in place in case they happen. However, they remain fairly unlikely.

In my view, there is perhaps a risk to us in paying too much attention to threats to critical infrastructure insofar as, as I say, these are things that are relatively unlikely.

Very few, if any, have actually materialized in Canada. On the other hand, many other threats that are much more subtle, less serious, but still have consequences because they are repeated and occur on a daily basis, get less attention and less thought from us.

I think that's a problem, because the critical infrastructure issue is something that is very visible; it's not necessarily very difficult to draw red lines, to be clear about what would be tolerated or not and what would elicit a vigorous response or not.

In the face of this set of smaller threats that individually are not deemed serious enough to elicit a response, but cumulatively produce damage that I think is problematic, I'm not sure we have a good strategy and ways of trying to discourage and prevent them.

● (1005)

[*English*]

Mr. Blaine Calkins: The mere fact that we're not an important enough target as a nation and that our critical infrastructure is not an important enough target.... However, we are involved in organizations like NATO. I believe that the increase we're seeing is the direct result of our involvement in supplying Ukraine with defensive assets.

Would you agree that, because of our involvement with Ukraine, we are exposing ourselves to risk? I'm not saying that we shouldn't involve ourselves with Ukraine, but are other actors right now using this as cover to probe our defences?

[*Translation*]

Mr. Alexis Rapin: In my opinion, in comparative terms, Canada is not, at this time, a priority target for Russia or for cyberactors who would put themselves at its service.

From what we observe and the information I have, the geographical factor still seems to play an important role. It is the countries that are rather close to Ukraine or Russia and the NATO members that are most targeted. I'm thinking of Poland, Slovakia, and the Baltic States in particular, which, from what I've seen publicly, have suffered far more attacks than Canada.

If Russia's goal had been to punish Canada by encouraging its criminal networks to deploy ransomware or by encouraging activists to conduct hacking and information disclosure operations against Canada, for example, we would have seen them by now, and we would have seen a very marked increase by now. But from what I can see, that's not the case.

That being...

[*English*]

The Chair: We're going to have to leave it there.

Thank you, Mr. Calkins.

Mr. May, you have six minutes, please.

Mr. Bryan May: Thank you, Mr. Chair.

I was delighted to hear, Ms. Csenkey, that you're from the Balsillie school. I know it very well. Being from the Waterloo region myself, I know that ecosystem and some of the amazing work that's coming out of there. In fact, just a few weeks ago, I had the pleasure of joining Minister Champagne at the Perimeter Institute, which is just around the corner, and launching Canada's quantum strategy. Much of what was discussed there, I have to admit, went completely over my head, but I recognize the amazing work that's being done there.

On that note, how are advancements in artificial intelligence and quantum technology changing the cyber-threat environment for Canada?

Ms. Kristen Csenkey: Thank you so much for that question from Mr. May.

I would say that there are certain technologies that can have huge impacts related to cybersecurity issues. We can call them disruptive. We can call them emerging technologies. Sometimes we think of them as being a threat themselves or as being very disruptive. However, how I see this problem or this concept is that technologies also interact with humans. Humans create the technologies. We work with them. We can use them for a variety of purposes.

When we think about quantum computers, for example, quantum computers have the potential to benefit many fields. It's not just from a defence perspective that we can look at this. We also can look at the benefits in, for example, accelerating artificial intelligence and for improving simulations and a variety of other purposes, including weather predictions, etc.

When it comes to talking about investing in and developing certain technologies with the intention of developing capabilities for Canada, I think we have an expert base in this country in a variety of regional hubs that are doing excellent work, but I think what needs to happen is that there needs to be more co-operation to address the threats we associate with the use of these particular technologies, while also keeping in mind that it is not just the technology that's the threat. It's the potential for certain malicious actors to use these certain technologies in a way that could cause harm.

One of the ways in which we can help to co-operate to address those threats is through leveraging these existing partnerships. It's by leveraging existing partnerships at home, in Canada, between government, industry and academia through the various research centres that we have dedicated to these particular types of technologies, but also by leveraging existing pathways for partnership amongst our allies.

● (1010)

Mr. Bryan May: Thank you.

Monsieur Rapin, do you have anything you would like to add? You've covered it well, I suppose.

In terms of maybe the concept of mass adoption of emerging technologies among Canadians, which trends, in your opinion, present the greatest cybersecurity risks?

We'll start with you, sir.

[*Translation*]

Mr. Alexis Rapin: Are you referring to technology, especially new technologies, innovation?

[*English*]

Mr. Bryan May: Yes. I'm thinking in terms of things like smart vehicles, wearable tech and that sort of thing. Are there certain things we should be concerned about that might be vulnerable to cyber-attack?

[*Translation*]

Mr. Alexis Rapin: I wouldn't be able to prioritize the issues according to their importance, but something is attracting my attention a lot, and that is the Internet of Things. There is an exponential proliferation of connected objects. For Canada, very simply, it means that the attack surface is increasing. There are more devices through which to conduct cyberattacks and cyber operations.

Actually, in many cases, connected objects are the weak link in the chain. They are small objects that have been designed to be low cost and very easy to use, among other things. Often what manufacturers will sacrifice in their design is cybersecurity.

There may be thoughts to be had about cybersecurity standards to be imposed on connected objects. We should ensure, for example, that they do not become, in the near future, a kind of privileged gateway for larger system breaches or compromises.

[*English*]

The Chair: Thank you, Mr. May.

[*Translation*]

Mr. Garon, you have the floor for six minutes.

Mr. Jean-Denis Garon: Thank you very much.

I thank both witnesses for being here today.

Mr. Rapin, I would like to know whether, in terms of cybersecurity information sharing, Canada is a credible player among its allies. I am thinking in particular of the Group of Five. How are these exchanges carried out? Is it give and take?

Is Canada able to be effective enough in collecting and producing information to be a credible ally with the Group of Five, in particular?

● (1015)

Mr. Alexis Rapin: In the case of the Group of Five, it's a bit of a potluck. Everyone is supposed to bring something to eat and then we share what's there.

Mr. Jean-Denis Garon: That's it. Now, what we need to know is whether Canada cooks a lot.

Mr. Alexis Rapin: I am not in a position to answer that. Unfortunately, I don't sit on the Group of Five committees and I don't have any inside information on that.

However, the secondary view I can give is that, for many researchers and many people who work on this, Canada is not seen as a player that brings much to the table. I'm not saying that's necessarily the strong opinion that all members have, but it's often the opinion that comes through.

Mr. Jean-Denis Garon: We understand the nuance, and it is only appropriate to mention it.

That said, I note that Canada has been very slow to make strategic and important decisions in many cases lately. The Huawei one comes to mind, but there are others. I wonder if this has damaged our credibility with our allies and negatively changed their perception of us.

Mr. Alexis Rapin: It is true Canada did not shine particularly brightly in this regard. It may have looked like we were following the trend rather than making a firm and determined decision.

In my view, there are a lot of factors involved. What I often hear, from foreign colleagues in particular, is that Canada has an image of a country that is very “nice”, or perhaps has what you might call a national security culture...

Mr. Jean-Denis Garon: Are we seen as naive?

Mr. Alexis Rapin: No. At least, that's not the views I hear at all. However, perhaps it's a matter of maturity in terms of national security issues; we're not always quick to seize the problem and want to tackle it head on.

Mr. Jean-Denis Garon: Let me change the subject a bit and address a current issue that I find extremely important.

You know that the McKinsey firm has done a lot of business with Canada. We are talking about hundreds of millions of dollars in contracts awarded, notably by the Department of National Defence. We know that McKinsey, a firm that is not known for its high ethical standards, does a lot of business with China. This has been part of the development of its new core market over the last 15 or 20 years.

Are Canadians and Quebeckers right to be concerned about potential information leaks? If so, do you think we need to have transparency mechanisms for these more elaborate types of contracts?

Mr. Alexis Rapin: I am not at all able to answer this question, quite honestly.

Mr. Jean-Denis Garon: I understand.

Ms. Csenkey, we talked about the threat of quantum computers, among other things. My impression is that in a lot of circumstances where you have vulnerabilities, like cyberattacks, the human factor is a big part of it. In many cases, social engineering makes us vulnerable, regardless of the investments we make in our infrastructure.

In your opinion, is Canada doing enough to ensure that risk related to human factors is as minimal as possible?

[*English*]

Ms. Kristen Csenkey: Mr. Chair, I'd like to thank Mr. Garon for the question.

I'd like to pick up on a question that you posed earlier about Canada's role in the Five Eyes, and then I'll get to your other question.

The Five Eyes, as we know, is an important and trusted intelligence-sharing partnership, and this partnership could extend to information relating to cybersecurity.

As I mentioned in my opening statement, in a recent paper that I co-authored, we found that the specific cybersecurity threats are understood differently between these co-operating allies, especially in the Five Eyes. When it comes to working on solving these particular cybersecurity-related issues, I think one opportunity for Canada to lead on this issue area within the Five Eyes would be in addressing and understanding certain cybersecurity issues, such as the quantum threat. Perhaps this could be through a Five Eyes quantum consortium.

This is understanding that the Five Eyes is an intelligence- and information-sharing partnership. That's its primary purpose. However, we've seen in other partnerships between allies, such as AUKUS, that there can be secondary purposes that might allow us to align and co-operate on particular issues. We know that—

● (1020)

The Chair: Unfortunately, we're going to have to leave the answer there. I'm sure you'll have an opportunity to elaborate further.

[*Translation*]

Mr. Boulerice, you have six minutes.

Mr. Alexandre Boulerice: Thank you very much, Mr. Chair.

I thank our witnesses for being here for this important study.

Ms. Csenkey, in July 2021, you published an article entitled “Selling Simulations: The Seduction of Cold War Techno-Fetishism in a Postmodern Cyber World”.

Firstly, would it be possible for you to send this scientific article to the committee so that it can form part of our report?

Secondly, can you tell us how this analysis applies right now to the tensions or conflicts that we see with Russia and China?

[*English*]

Ms. Kristen Csenkey: Mr. Chair, I would be happy to provide that for the committee.

Incorporating some of the arguments I made in that paper referenced by the committee member, when we're thinking about technology and cyber-threats, it's often caught up in a narrative that excludes human actors, human intentions, ideas about certain technologies and certain capabilities from the lived experience and reality of what cybersecurity is, which is that complex sociotechnical system. If we see cybersecurity threats and that interconnection with humans and technologies, we can also add in services, people, private sector businesses and other connected technologies that flow between different sectors.

What I would like to emphasize is that, when we're talking about connected technologies and we're associating it, for example, with critical infrastructure, it's a more dynamic understanding of cybersecurity issues as related to critical infrastructure. It's that combination of people, services, private operators and those technologies that flow between....

Also, picking up on something that was mentioned in the earlier session, we can't really think of cybersecurity issues as a siloed issue. This goes between different prerogatives of defence, yes, but also of national security. There's also that economic component as well.

I think when we're talking about cybersecurity issues and we're linking them to technologies and people and services, etc., we need to understand that there are cybersecurity considerations for each particular sector. There are different services that are provided within each sector and different technologies, again, appreciating the linkages between them.

We can also appreciate that there are different threats, vulnerabilities and risks for each sector, but there are differences and commonalities in between. When we're talking about what cybersecurity problems are, I think we also need to think about cybersecurity solutions. It's not an across-the-board answer for all.

[*Translation*]

Mr. Alexandre Boulerice: Thank you very much, Ms. Csenkey.

Mr. Rapin, you talked about the concrete effects of cyberattacks on people's lives.

We saw it last summer with the Rogers outage; it was not caused by a cyberattack, but by a maintenance problem. People were left extremely helpless. They were walking the streets and looking for addresses on maps.

There were no consequences, no punishment, for Rogers. Isn't being so dependent on a handful of unaccountable private telecom companies evidence of our vulnerability?

● (1025)

Mr. Alexis Rapin: I don't think I'm in a position to comment on the issue or on the link that there may be between industry concentration and infrastructure vulnerability.

I feel that what is going to be more important than market dispersion is redundancy of infrastructure, as well as having backup systems and having thought about resilience upfront, no matter how many players are involved. Someone has to think at some point about what would happen if such and such an attack happened against such and such an infrastructure and so on.

I have a feeling that maybe that's where we should start.

Mr. Alexandre Boulerice: Do you think the federal government should have the responsibility of requiring system redundancy standards, so that there is better system resilience in any situation?

Mr. Alexis Rapin: I think we will need to think about that, yes.

People are thinking about these things in the US, particularly since the ransomware cyberattack against Colonial Pipeline. On the surface, on paper, this incident could have been like any other ransomware attack, but it ended up having huge consequences. Once pressure was applied to a specific link in the chain, the consequences became disproportionate.

I do think we need to think about this.

[*English*]

The Chair: Thank you, Mr. Boulerice.

Colleagues, again, we're in the same situation. This time we have to have a hard stop at quarter to eleven, so we'll do three minutes, three minutes, one minute, one minute, three minutes and three minutes.

We'll go to Mrs. Gallant.

Mrs. Cheryl Gallant: On July 8 we had the Rogers outage that was mentioned, and the 911 system went down in the Maritimes last week. Two weeks ago there was the Transport Canada civil aviation NOTAM failure on the heels of the FAA outage.

Should the government be compelled to alert the public when a cyber-attack is under way on a major system? The government didn't tell us about the balloon when it was overhead, so you know, why would we believe that it would even tell us there was a cyber-attack under way?

Ms. Kristen Csenkey: What I would pose here is that, when you talk about cybersecurity issues that become major cybersecurity threats, we have to back it up a bit and understand that cyber illiteracy is also a major issue for a lot of businesses and people. When we have cyber-incident reporting, that's good, but we need to sort of back it up and go from the start.

We need to ensure there are cybersecurity considerations for particular projects, for particular—

Mrs. Cheryl Gallant: Mr. Chair, she's not answering the question, so let's go to Mr. Rapin.

Should the public be made aware, when there's a cyber-attack under way on our major systems in Canada?

[*Translation*]

Mr. Alexis Rapin: I'll answer in French, if I may.

My opinion is that yes, there should be more transparency. Of course, as researchers, we are biased because we want more information to do our work, but I think it is obviously in the public interest to have more transparency. What we see is that people do not necessarily feel like it is about them, when it is. It's what we see with the incidents you gave as examples. People are suddenly shocked by what is happening and they do not understand what is going on, because there is very little public debate on cyber issues in Canada, since there is little information to go on.

It would be good for everyone if we could get more transparency on these issues.

● (1030)

[*English*]

Mrs. Cheryl Gallant: Generally, how long does it take for entities to realize that their system is under attack versus dealing with a software glitch?

[*Translation*]

Mr. Alexis Rapin: I wouldn't be able to give you any specific data on that.

[*English*]

Mrs. Cheryl Gallant: Canada has not yet experienced a totally debilitating cyber-attack. Can you tell the committee what a full-on attack would look like?

[*Translation*]

Mr. Alexis Rapin: The example we often hear about is a cyber-attack on the electrical grid. That could cause a lot of damage. We saw examples of that in Ukraine, in 2015 and 2016, if I remember correctly. Hundreds of thousands of people were without electricity for hours. I don't know how vulnerable Canada's electrical grid is.

[*English*]

The Chair: Mr. Rapin, I appreciate the difficulty in responding to that question, but it's still a good question. Maybe there's a possibility you could, if you have the opportunity, write a response. It may be a way to handle that.

We'll go to Mr. Sousa for three minutes.

Mr. Charles Sousa (Mississauga—Lakeshore, Lib.): Thank you, Mr. Chair.

The previous testimonies talk about what seems to be a worldwide threat. This is not just Canada. We talk about the Five Eyes and the partnerships we try to engage with other states to protect ourselves and to protect the world, in essence. It affects our supply chains and ways of businesses, not just politics and elections, and not just defence. There are real economic consequences to some of these issues.

We also heard about silos and how there seem to be silos within Canada. There is greater co-operation being developed, but there are also silos around the world, even within the Five Eyes. You, yourself, mentioned that you don't know all the issues, so how do we then provide co-operation with other states and, at the same time, protect our own national security. We don't want to divulge too much information.

I am also concerned about cognitive warfare and fake news, these other incidents that take place to disrupt our way of life and our democracy. I've heard a lot of solutions and no solutions. That seems to be the answer. There's very little that we can do, because we're still trying to learn and keep up.

We heard an answer that “they don't tell us”—this Big Brother, this matrix that exists. Who are “they”?

[*Translation*]

Mr. Alexis Rapin: When I mentioned transparency… It can be for various types of entities.

The federal government could be more transparent. Nearly a year ago, Global Affairs Canada was hit by a major cyber incident. My sources give me very good reason to think that Russia was behind the incident and that it didn’t take long to figure out that it was the culprit.

For the time being, the government is very reluctant to disclose that information, even though it would be in the public interest and it’s important for Canadians to know.

[*English*]

Mr. Charles Sousa: I'm going to pose the same question to you, Ms. Csenkey, because what I'm hearing is what we're always hearing—that there are a number of groups that are responsible, and they are trying to co-operate to find a solution while at the same time protecting our national security.

How do we provide the solutions you're talking about in regard to silos, where we are aware that there are discussions but there's the notion of transparency without divulging national security issues, even with other states, even beyond the Five Eyes?

The Chair: Very briefly, please.

Ms. Kristen Csenkey: There's a lot of content there so I'm going to try to be as quick as possible.

I would say, number one, attributions are difficult at the best of times when identifying cybersecurity attacks, motivations, the individuals or groups or states responsible for these attacks. That does make it difficult. For example, it could be a cybercriminal group that is attacking a certain target for the purpose of profit. It could be a group that is working on behalf of a—

● (1035)

The Chair: I apologize again, Ms. Csenkey, but I'm going to have to cut off Mr. Sousa.

You have a minute, Mr. Garon.

[*Translation*]

Mr. Jean-Denis Garon: Ms. Csenkey, if you could submit a written response to the committee for the previous question, I would appreciate it.

Mr. Rapin, is diplomacy still a solution with China in trying to prevent cyberattacks, or should we be looking at a more preventive approach?

Mr. Alexis Rapin: I’m not sure I can answer your question.

I can tell you that in the US, where I think they realized much sooner that economic espionage by China, for example, is a massive problem, the Obama administration tried a diplomatic approach.

At the time, President Obama went to meet his counterpart in China and an agreement was negotiated to try to put an end to economic espionage. From what we were able to find out, it worked for about a year. In any case, there was a major decrease in Chinese economic espionage activities. At the next crisis, or for various reasons, economic espionage started up again.

I am not saying that to discredit the diplomatic approach. Diplomacy plays a role in certain aspects.

Mr. Jean-Denis Garon: Diplomacy is therefore not enough.

Mr. Alexis Rapin: I would say that it has its limits, depending on the circumstances.

[*English*]

The Chair: We're going to have to again leave it there.

[*Translation*]

You have one minute, Mr. Boulerice.

Mr. Alexandre Boulerice: Thank you, Mr. Chair.

Mr. Rapin, it worries me to hear you say there have been 93 known cyber incidents in Canada since 2010, and that they are happening more often. It’s not surprising that they are coming from China, Russia, Iran and North Korea. There are espionage, surveillance and intelligence operations.

Are these cyber incidents or cyberattacks aimed at public infrastructure such as agencies and departments, or at private companies such as banks, with information being sought about members of the public?

Mr. Alexis Rapin: It’s not easy to say. Based on the public, open-source information we use, the type and number of Canadian entities that have been targeted are often unclear. For example, we use reports from cybersecurity firms indicating that Canadian entities were hit. We don’t know whether there were many entities or just one or two; we also don’t know whether it’s companies, government bodies or other entities.

[*English*]

The Chair: Thank you, Mr. Boulerice.

Mr. Kelly, you have three minutes.

Mr. Pat Kelly: Thank you.

I want to continue talking about the 93 specific incidents that you've recorded since 2010. You said that China, Russia, Iran and North Korea are the primary...or perhaps all 93 of them can be attributed to those four countries. You talked about economic espionage, but you also talked about the surveillance of activists. Do I take it from that you're talking about dissidents in Canada, diaspora communities? You talked about the number of people who are affected.

Can you tell me how many Canadians would be victims of these kinds of attacks or the targets of these attacks? Give us more information on how these geopolitical cyber-incidents affect individual Canadians and what sort of harm is caused by these incidents.

[*Translation*]

Mr. Alexis Rapin: It's difficult to give a number because these incidents can take different forms and be more or less aggressive, depending on the person being targeted. In the case of the Uyghur community, it can be extremely aggressive. In other cases, it can take other forms. Last December, for example, Amnesty International Canada was targeted by a cyberattack that likely came from China. The degree of involvement of the targeted actor varies, and the aggressiveness of the attack therefore does as well.

I think we've listed three countries that have so far targeted activists, NGOs or dissidents in Canada. Chronologically, the first was Saudi Arabia, which targeted a dissident living in Canada. That was brought to light by Citizen Lab at the time. Next was China, which targeted Uyghurs in particular and conducted operations against members of Falun Gong. More recently, we've started to see Iran doing similar things. It is currently suspected of conducting electronic espionage in relation to demonstrations.

● (1040)

[*English*]

Mr. Pat Kelly: May I just ask you, on that point with respect to China and the use of cyber-incidents against the Chinese diaspora in Canada—against their citizens and Canadian citizens—are Beijing's diplomatic offices in Canada involved in these attacks? Is this coming strictly from outside or is this with the co-operation of their diplomatic missions in Canada?

[*Translation*]

Mr. Alexis Rapin: Unfortunately, I don't have all the information I need to answer that question.

[*English*]

The Chair: Thank you, Mr. Kelly.

Ms. O'Connell, you have three minutes.

Ms. Jennifer O'Connell: Thank you, Mr. Chair.

Thanks to both of you for appearing today.

Mr. Rapin, I wanted to talk about the differences in your database that I find very interesting, the differences between an attack, for example. It's my understanding that it's pretty cheap on the dark web to purchase some sort of malware or program. That sort of blackmail-type of attack on a business might not even be linked to a foreign adversary, for example. There's that distinction. Then there's a distinction between an attack on a government agency, for example, or a department, and then there's a distinction between private entities.

In the course of this study, we would be looking for recommendations to improve our systems. One of the areas at issue is that there is no ability for CSE, CSIS or our cybercommunity to actually intervene with private entities, even if they have been attacked by a foreign actor. That also goes, in some cases, for critical infrastructure. A lot of times, municipalities would be the ones owning that infrastructure. In fact, the CSIS Act directly prevents CSIS from communicating or sharing information with municipalities, provinces, etc.

Could you maybe speak to the differences and maybe some recommendations on how we can make sure we're distinguishing between attacks from, let's say, a bad actor versus a bad foreign actor, and the various levels?

[*Translation*]

Mr. Alexis Rapin: We have to look at different approaches. CSIS, the RCMP and even federal agencies won't be able to fix everything. As you said, a lot of the infrastructure that could be considered critical and that is the most vulnerable is at a relatively low level, where there can be fewer resources and less expertise for cybersecurity.

There are different cases, particularly in the US, where foreign state-sponsored hackers targeted municipal or state infrastructure, expecting them to be less protected at that level. There are therefore various approaches and levels to consider.

I believe Ms. Csenkey talked earlier about making it mandatory for organizations that manage critical infrastructure to report cyber incidents. I believe the US just did this, or is about to. It's a best practice, and I think we should be doing that as well.

[*English*]

The Chair: Thank you, Ms. O'Connell.

I want to thank both witnesses on behalf of the committee.

As you can see this is a hot topic and a very complex topic. I take note that, in this morning's news, the Elon Musk group is cutting off Ukrainian access to the information provided through that satellite. This strikes me as an immense security risk, a clear and present danger to the prosecution of that war.

In the event that you have any thoughts along those lines, I particularly would be interested.

Regardless, I do, unfortunately, have to bring this meeting to a close.

With that, colleagues, the meeting is adjourned.