HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

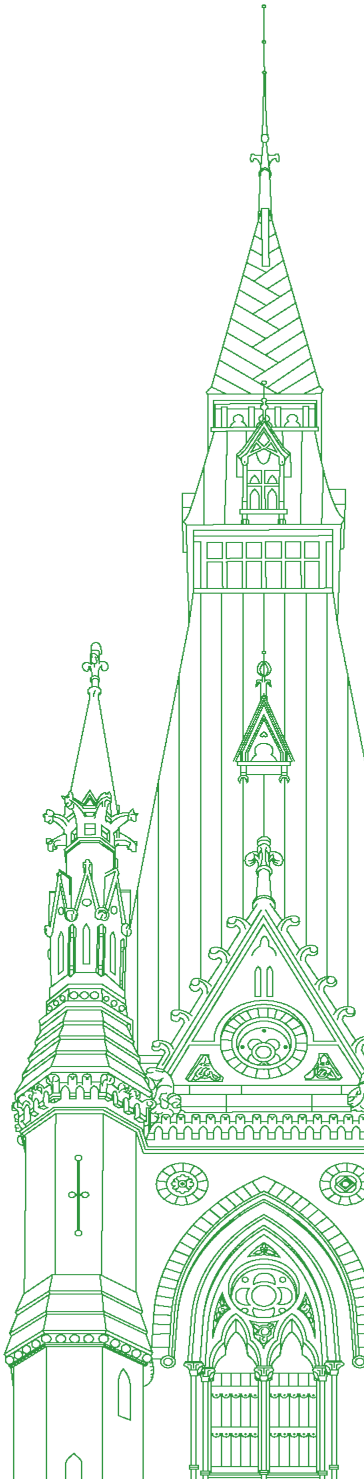
43rd PARLIAMENT, 2nd SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 012

Wednesday, December 9, 2020



Chair: The Honourable John McKay

Standing Committee on Public Safety and National Security

Wednesday, December 9, 2020

● (1530)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): I see quorum. This meeting is now in order. This is the 12th meeting of the House of Commons Standing Committee on Public Safety and National Security.

We have before us Mr. Scott Jones, who is head of the Canadian Centre for Cyber Security, and who has appeared before this committee quite a number of times, I would say.

Before I ask you for your opening remarks, I just want to compliment you on your report. If the standard of a report is its accessibility, I think the report you produced is actually quite accessible, particularly for people such as us who are not particularly expert in the field. I want to thank you for that.

I also want to take note that it is an echo of the NSICOP report submitted by Mr. McGuinty, and there was a letter, which I hope was circulated to members after the last meeting.

With that, I welcome Mr. Jones for his seven minutes, and thank him again for being available to us.

Mr. Scott Jones (Head, Canadian Centre for Cyber Security, Communications Security Establishment): Thank you very much for that, Mr. Chair.

Good afternoon, committee members.

Thank you for the invitation to appear today to discuss cybersecurity and specifically the “National Cyber Threat Assessment 2020” report released on November 18.

As the head of the Canadian Centre for Cyber Security at the Communications Security Establishment, I am very pleased to be here. CSE is Canada's foreign intelligence agency and lead technical and operational agency for cybersecurity. As was mentioned, I have appeared here a few times before.

Created in 2018, the cyber centre is a unified source of expert advice, guidance and support on cybersecurity operational matters. We work closely with other government agencies, industry partners and the public to improve cybersecurity for Canadians and to make Canada more resilient against cyber-threats.

Our goal with the national cyber-threat assessment is not to frighten Canadians or to be downers, but rather to inform all of us about the threats we will be facing in the coming years. I hope it spurs many of us to take simple actions to protect ourselves. We have seen that easy, simple actions can greatly increase our individual security.

Canada is one of the most connected countries in the world, which the NCTA highlights, and the COVID-19 pandemic has accelerated our reliance on the Internet to meet basic needs. We are increasingly leading our lives online, and at the same time threat actors continue to pursue new ways to use the Internet for malicious purposes. While this assessment does not provide specific mitigation advice, more guidance and best practices can be found on the cyber centre's website and through our “Get Cyber Safe” public awareness campaign. As I've said before, by taking even a single action, all Canadians can help shape and sustain our nation's cyber-resilience.

For those Canadians who would like to learn more, we have also published an updated “An Introduction to the Cyber Threat Environment”, which I will confess I may slip and call the “cyber primer”, in which we explain many of the terms and techniques used in cybersecurity.

The assessment analyzes cyber-trends since 2018 and draws upon the cyber centre's unique view of the cyber-threat environment to forecast those trends to around 2022. The assessment also highlights the most relevant cyber-threats to Canadian individuals and organizations.

Before I discuss those threats further, though, I would note that the assessment's findings are based on reporting from multiple classified and unclassified sources, including those related to CSE's foreign intelligence mandate. While the cyber centre must protect classified sources and methods, we have tried to provide readers with as much information as possible, including footnotes.

I'll now provide a brief breakdown of the cyber centre's key findings regarding the cyber-threat landscape. Broadly, these can be grouped into three key observations for our discussion today.

The NCTA 2020 highlights several key observations.

First, cybercrime is the threat most likely to impact Canadians now and in the years ahead, and cybercriminals often succeed because they exploit human and social behaviours.

Second, ransomware directed against Canada will almost certainly continue to target large enterprises and critical infrastructure providers.

Finally, while cybercrime is the main threat, state-sponsored cyber-programs of China, Russia, North Korea and Iran pose a strategic threat to Canada.

First, we assessed that cybercrime remains the threat most likely to impact Canadians. Now and in the years ahead Canadian individuals and organizations will continue to face online fraud and attempts to steal personal, financial and corporate information. Cybercriminals often succeed because they exploit deeply rooted human behaviours and social patterns as well as technological vulnerabilities. Unfortunately, as a result of this reality, Canadians are more at risk for cybercrime than ever. This has only increased during the COVID-19 pandemic.

Malicious cyber-actors are able to take advantage of people's heightened levels of fear to lure and encourage victims to visit fake websites, open email attachments and click on links that contain malware. These website emails and links frequently impersonate health organizations or the Government of Canada. Defending Canadians against these threats requires addressing both the technical and social elements of cyber-threat activity.

Second, the ongoing safety of Canadians depends on critical infrastructure as well as consumer and medical goods, many of which are increasingly being connected to the Internet by their manufacturers. However, once connected, these infrastructures and goods are susceptible to cyber-threats, and maintaining their security requires investments over time from manufacturers and owners that can be difficult to sustain.

We have assessed that ransomware directed at Canada will continue to target those large enterprises and critical infrastructure providers. As these entities cannot tolerate sustained disruptions, they are often willing to pay up to millions of dollars to quickly restore their operations. Many Canadian victims will likely continue to give in to ransom demands due to the severe costs of losing business and rebuilding their networks and the potential consequences of refusing payment. The protection of these organizations and networks is crucial to the productivity and competitiveness of Canadian companies, and vital for Canada's national defence.

Finally, state-sponsored actors are very likely attempting to develop cyber-capabilities to disrupt Canadian critical infrastructure to further their goals. However, we judge that it is very unlikely that cyber-threat actors will intentionally seek to disrupt critical infrastructure and cause major damage or loss of life in the absence of international hostilities. Nevertheless, cyber-threat actors may target Canadian critical organizations to collect information, preposition for future activities, or as a form of intimidation.

● (1535)

While cybercrime is the most likely threat to impact the average Canadian, state-sponsored cyber-programs of China, Russia, North Korea and Iran pose the greatest strategic threat to Canada. We have assessed that state-sponsored actors will almost certainly continue to attempt to steal Canadian intellectual property, proprietary information and, in today's context, information specifically related to COVID-19.

We have also assessed that online foreign influence campaigns are no longer limited to key political events such as election periods. They are now the new normal. Adversaries now look to sustain their influence campaigns across all levels of discourse deemed to be of strategic value. While Canadians are often lower-priority targets for online foreign influence activity, our media ecosystem is closely intertwined with that of the United States and other allies, which means that when their populations are targeted, Canadians become exposed to online influence as well.

I want to reassure you that CSE and the cyber centre are working hard to mitigate many of these threats and protect Canadians and their interests through targeted advice and guidance. CSE continues to leverage all aspects of its mandate to help ensure that Canada is protected against threats. Not only is the “National Cyber Threat Assessment” meant to inform Canadians, but it is also setting the priorities for action by the cyber centre on what actions we can take, often with partners in the private sector who are willing to stand up and assist in directly addressing these threats facing each of us.

A key example of this type of partnership is the Canadian Shield initiative from the Canadian Internet Registration Authority, CIRA. CIRA Canadian Shield is a free, protected DNS service that prevents you from connecting to malicious websites that might affect your device or steal your personal information. The service is provided by the Canadian Internet Registration Authority, a not-for-profit agency that manages the “.ca” Internet domain. The service uses threat intelligence from the Canadian Centre for Cyber Security. In simple terms, if someone who is using Canadian Shield clicks on a link that is known to be malicious, they will be stopped from going to that bad site.

CIRA has seen a number of Canadians pick up the use of this tool, although we would certainly like to see it accelerated more. We are just past the six-month mark. We do recommend that all Canadians take advantage of this free service built by Canadians for Canadians and designed to protect Canadians' privacy.

Through targeted advice and guidance, the cyber centre is helping to protect Canadians' cybersecurity interests. We are dedicated to advancing cybersecurity and increasing the confidence of Canadians in the systems they rely on. We hope this report will help raise the bar in terms of awareness of today's cyber-threats. I encourage Canadians who are looking for easy-to-follow tips on cybersecurity, such as our holiday gift guide, to visit our website, GetCyberSafe.gc.ca.

For businesses and large organizations, or if you would like to read more of the publications of the cyber centre, we can be found at cyber.gc.ca.

Thank you again for the opportunity to appear before you virtually today. I'll be pleased to answer any questions you may have.

● (1540)

The Chair: Thank you, Mr. Jones.

For the first six-minute round I have Madam Stubbs, Mr. Lightbound, Madame Michaud and Mr. Harris, in that order.

Madam Stubbs, please. You have six minutes.

Mrs. Shannon Stubbs (Lakeland, CPC): Thank you, Chair.

Thank you to the witness for being here and for your time, your report and all of your work. It's eye-opening and deeply alarming, so I think we're all glad that you're there.

In your comments and in your report you touched on the cost of foreign hacking to western companies and governments, even to the tune of individual Canadians losing over $43 million to cybercrime fraud in 2019, according to the statistics from the Canadian Anti-Fraud Centre.

Could you explain to us what costs the criminals and the foreign state-sponsored actors who engage in foreign interference in our democracy and society face? I wonder if you have any comments on whether or not they seem to act with relative impunity, without any serious risk of costs to their actions.

Mr. Scott Jones: Thank you for the question, Mr. Chair, and your comments on the report.

I think there are a few things. If we look at cybercriminals, they very much reply upon an extremely developed ecosystem that relies on things like anonymous financial transactions—Bitcoin and the like. Having online digital currencies really does facilitate that.

In terms of the risk, it's certainly a question that I wish one of my colleagues from the RCMP were here to talk about in terms of prosecutions, but it remains a challenging environment in which you can achieve fraud against a Canadian from remote jurisdictions. As the report points out, there are many jurisdictions in which you will not suffer consequences from local authorities because as long as you don't target their citizens, they're not going to go after you. A bit of a quid pro quo seems to exist, and it certainly has been highlighted in some of the research.

In terms of some of the costs, we do try to impose costs. The government has done a number of attributions to call out state activity that we feel is crossing thresholds and crossing lines. Earlier this year we called out Russia for its activity against vaccine research companies. We have certainly joined our allies a number of times to do that. That was one instance in which we joined in with the United Kingdom and the United States to do that, specifically because it was targeting our areas, but we have, at some points, along with our allies, called out behaviour of each of the four nations I mentioned.

Mrs. Shannon Stubbs: Could you expand on the importance of attribution and exposing their intent? Also, do you have any other comments on possible other options to fight back, such as sanctions or other tools?

Mr. Scott Jones: The value of attribution is pretty variable. The primary value of being a cyber defender and somebody who is worried about cybersecurity is that it spurs action. When we do an attribution, it tends to get organizations to take seriously the alerts we put out. When we say, “You need to apply this patch; it's important,” people will respond. When we say, “Apply this patch because country X is targeting this sector, ” they pay attention and they do it. It does have an effect domestically in getting the potential victims to take it seriously and to take action.

In terms of the international side, we certainly have not seen a significant change in the actors' behaviour because of it, but it does form norms. That is something that is probably more appropriate for my Global Affairs colleagues to talk about, and they're probably better positioned to talk about some of the things like sanctions and other aspects of foreign policy. I tend to try to stick to the technical and the cybersecurity elements.

Mrs. Shannon Stubbs: Okay. Thank you.

On page 23 of your report and in the comments you made—and you've already gave the example of a Canadian Shield—you noted that ransomware frequently targets health organizations and that it has ramped up during COVID-19. On page 25, you talked about supply chain vulnerability. I just wonder if you can comment on the Canadian government now mounting a massive COVID-19 vaccine distribution campaign and what measures are being or could be or will be taken to ensure that the distribution supply chain is protected from malicious cyber-actors. In addition to that, are you confident that suppliers, logistics operators, and health clinics also have robust enough cybersecurity measures in place?

● (1545)

Mr. Scott Jones: Thank you for that question. There's a lot in there.

We have been working since the beginning to build up the resiliency of the health care community. One of the things we have been working on, which we've done in partnership with the provinces and territories—which clearly have such an important role to play in health care, in providing advice and guidance—is targeted briefings, targeted information, specifically to that health care sector to build resiliency over time. We knew we were going to arrive at a vaccine at some point, so we have been building up resiliency and making sure that the information flows are in place, and also ensuring that they have the information they need to proactively take steps to protect themselves. We've done that through things such as publishing other threat assessments that are specifically for the health sector. We take those, and then on regular weekly calls, we go over any threat we're seeing and how it could apply to the health sector and what could be done about that. We're trying to very much build up resiliency before something happens.

In terms of the current rollout of the vaccine, we are working with, obviously, our colleagues at the Public Health Agency and the overall task force to make sure that the information is in the hands of any organization that would be part of this to make sure we're taking actions earlier. Then, of course, we do leverage our foreign intelligence mandate, so if we do see things that are happening in foreign space or in our group of allies around the world and not necessarily just the Five Eyes.... We have a lot of allies in cybersecurity, and we all look at and share information very quickly to make sure we're getting that information out. Our goal is not to observe the problem but to give somebody, anybody who's a potential victim, something they can use to protect themselves. That's really been our goal.

We continue to look for new ways that we can build up our cyber resiliency in this [*Inaudible—Editor*].

The Chair: Thank you, Madam Stubbs.

Mr. Lightbound, please. You have six minutes.

[*Translation*]

Mr. Joël Lightbound (Louis-Hébert, Lib.): Thank you very much, Mr. Chair.

Thank you, Mr. Jones, for joining the committee today. Thank you also for this report, which is quite disturbing, but relatively straightforward for someone who is not necessarily as well versed in the field as you are.

My first question concerns the critical infrastructure you report on. I'd like to hear your assessment of the situation in Canada with respect to the awareness critical infrastructure managers across the country have about the cybersecurity risks.

What is the centre doing to ensure that the level of sensitivity to these matters increases?

[*English*]

Mr. Scott Jones: Mr. Chair, that's a really great question. I'm glad to get the opportunity to address this.

We've been working with Canada's critical infrastructure providers for quite a while. Now, we do have to concentrate on the ones that are most at risk, so when we talk about the electricity sector in this report, that's a sector where we have been working both to build the relationships that we need across the country and with energy providers such as the Canadian Electricity Association to make sure we're addressing cyber-threats proactively.

Over a year ago, one of the things I did was that I participated in the tabletop exercise to simulate what would happen in an event where there was a cybersecurity incident, just to make sure that we're prepared, that we had gone through it and there were no gaps in the process. We continuously are looking to improve here.

This is an area where the technology changes are something that the sector is very aware of. They're very much resiliency based. They understand. They're used to dealing with things like major weather events, etc. Cybersecurity can be looked at as just a different source of the same type of impact. They're organizations that understand risk resiliency, and it's a very easy conversation. We're working closely with them. We are looking to address the threats. We're looking to see how we can expand not only into proactive cybersecurity, but into the discovery of threats before they manifest on the network, and we're looking for some joint projects.

At the cyber centre, one of the areas that we really like to concentrate on is innovation. We do that collaboratively, though. We do that collaboratively by bringing in partners from the energy sector and their suppliers, and we ask them if we can we tackle these problems together. If it is the convergence of operational technology, we ask how we can work with them and other leaders in industry, and we ask how we can detect when there's a threat or when there's somebody targeting and then proactively deal with it.

One of our goals is to make sure that is shared sector-wide from coast to coast to coast with every provider and to get that information out quickly. While one might fall victim, we don't want it to be two. Information sharing is also an important piece here when something is hitting, so that others can be inoculated against the threat as well.

● (1550)

[*Translation*]

Mr. Joël Lightbound: Thank you, that's a good answer. I think that, although it's recent, the centre is quite useful in this regard, precisely to build this relationship with critical infrastructure providers.

You mentioned the Canadian Shield in your presentation—I like the name. Could you comment on the use of the Shield by the general public? Do you have any figures on that?

[*English*]

Mr. Scott Jones: I can. It's really the Canadian Internet Registration Authority's project, and I'm hoping that I'm not scooping them, but they did advise us that earlier this week we now have 100,000 Canadians using the service. That's a good number—although not as much as I would like, honestly, because it does offer a significant boost to the privacy of information.

I do understand that one of the things we really thought about when we designed this and worked with them on the service was for the government to be at arm's length. We didn't want it to look like there was the potential that we were collecting information on Canadians. That's not our mandate. That's certainly not within our law that governs us, but there's also a privacy assessment that went along with it.

I'm hoping that as Canadians do look into this, they will see what's out there. We did have commentary from privacy experts in industry who talked about this program and how it's designed. I'm hoping that more Canadians, as they become aware, will grab onto this, because it is a way for every Canadian to do something to protect themselves, and it's something that is silent and in the background.

For me, here's the way I describe it. We're all worried that we're going to make that one mistake and click on that one link on an email and it's going to have devastating consequences. The goal with Canadian Shield and what we've tried to do is to make sure that if you click, it's not going to have devastating consequence, because it will be blocked. That's kind of what it does.

[*Translation*]

Mr. Joël Lightbound: In your report, you specifically name four countries as risks, including North Korea and China.

What factors are taken into account when naming these countries rather than others?

[*English*]

Mr. Scott Jones: That's actually a great question that I was really hoping someone would ask me.

It wasn't an easy decision to name countries because it immediately draws the attention from all the other aspects of the report to the four countries named. However, in reality, we, the Government Canada, had called out.... At some point, we had attributed malicious cyber activity to one of these four, or we joined our allies in doing so. So they were the logical four. They are also the four that demonstrated the capabilities that we mentioned in terms of the risk to Canada. We thought that, well, on one hand, it draws the attention away from some of the things we would like to talk about, such as how is it very easy for a fifth country and a sixth country to appear on that list. However, on the other hand, we need to acknowledge the fact that these four countries are out there and represent significant strategic risk to Canada with their capabilities and what they are able to do.

That was some of the discussion, but one of the things I've said is that the decision to name is more from a cybersecurity perspective. We certainly support this, but it is really in alignment with foreign affairs and foreign policy.

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

[*Translation*]

Ms. Michaud, you have six minutes.

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

Mr. Jones, thank you for being here and for publishing your report. It is indeed very interesting and disturbing at the same time. I think that the general public is not fully aware of the danger around cybersecurity or of the cyber threats that you mention in your report.

You told us about the theft of personal data, for example, and the physical danger to Canadians and Quebeckers. I would like you to tell us how the general public should protect themselves in this regard.

Do the various levels of government have some duty to educate?

This field is evolving quite rapidly, as you mentioned. We are more and more connected and dependent on all this technology, especially since the COVID-19 pandemic and the advent of telework.

How should people be made more aware and how can they better protect themselves?

● (1555)

[*English*]

Mr. Scott Jones: I think there are a few things I'm.... I'm a little concerned. The report is meant to inform; we're hoping not to scare. We believe that fear doesn't really motivate Canadians, in most cases, to take action. However, what we are hoping is that we can give Canadians simple things that they can do to help themselves be secure online. Get Cyber Safe is a great source for that, whether it's the Twitter account or the online account. There are some really easy things that we would like to ask Canadians to do.

One of those is passwords. We've seen that the number one password in Canada remains “password”; the number two password is “123456”. That's from a report, and that's pretty common worldwide. That just leaves it open and makes it easy for the cyber-threat actors. I know that passwords are a nightmare for all of us, but something basic like that can actually really strengthen cybersecurity.

The second easy thing that people can do is just turn on auto updates. Instead of having to install the updates manually on your phone or your computer, just set it to auto update. That also raises the bar for cybersecurity. We find that, in the last year or number of years, it is still the basic, out-of-date systems that are causing most of the cybersecurity breaches, so those two things are simple.

With regard to your point, for small and medium-sized enterprises what we have tried to do is also prepare a guide of simple, straightforward things that small and medium-sized organizations can do because they don't need to be—they shouldn't be—cybersecurity experts. That's our guidance for small and medium-sized enterprises. We designed that specifically so that 20% of the effort would result in 80% of the benefits of what we would do from, say, an enterprise-grade cybersecurity program that exists.

We are trying to do things that are practical and pragmatic, and then we do things that are fun—like the holiday gift guide, etc., at this time of year—to hopefully try to help Canadians make some good online security choices.

[*Translation*]

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

I will definitely be sharing this holiday gift guide. It seems very good, especially to inform our fellow citizens.

I'll now turn to small businesses, large companies and all those that could be threatened by cyber-attacks. We have seen small businesses that have been victims of ransom demands hesitate to consult lawyers, and pay to recover their property or personal data. Several articles in the media have indicated that small businesses have been victims of this.

Perhaps insurance companies could play a greater role and lawyers could be more knowledgeable in this regard. Turning to the federal government, what role can it play in this case?

We can indeed provide information, but are there government programs or legislative changes that could be put in place?

All of this is evolving very quickly, so what role could the federal government play in it?

[*English*]

Mr. Scott Jones: I think there are a few things.

Certainly, embarrassment and shame and fear about a potential loss of business are preventing organizations from reporting. In cybersecurity, unfortunately, we tend to punish the victim and not the perpetrator in our actions as citizens. We tend to shift away, and so there's an incentive for an organization to not admit when they're victims of a cybersecurity incident.

Then there's the second piece where there is embarrassment because the situation usually involves a mistake. Sometimes it's not because a patch has not been applied, but a lot of times it involves their having clicked on something they shouldn't have, and we have to begin to destigmatize that, and make people aware. You can get fooled. Some of the cybercriminal aspects...I believe it's only a matter of time before I'm going to click on something because some of them are so well done.

So if I know that is the case in my job, then nobody else should be feeling shame for it. I will probably be embarrassed when I click, but I'll get over it.

Lastly, I think some of the things we have seen include indications that insurance companies are telling organizations not to report, not to go to police, which makes this a very challenging thing to respond to, and also to get accurate statistics about, so we that know where to apply our resources on the specific threats. If we wanted to start to work on a particular version of cybercrime, without knowing what's hitting Canadians, where do we start?

Cybercrime is a global enterprise, unfortunately, but we should be focusing on what's targeting Canadians, and that's a challenge both for ourselves and the RCMP, because Canadian organizations just simply are not reporting for whatever reasons—ranging from embarrassment all the way to being advised not to report and pay the ransom to get back online.

● (1600)

The Chair: Thank you, Mr. Jones.

Mr. Harris, you have six minutes, please.

Mr. Jack Harris (St. John's East, NDP): Thank you, Chair.

Thank you, Mr. Jones, for coming before us today.

This is a very sobering report. There's some encouragement knowing that we can do some things ourselves and I'd like to ask you first about the CIRA Canadian Shield, which you call a "free protected DNS service that prevents you from connecting to malicious websites".

First of all, for the uninitiated like me, I first heard of this today by the way, so thank you very much for that.

What is a DNS service, for one, and for two, do you have all your personal devices connected using this CIRA Canadian Shield yourself?

Mr. Scott Jones: Yes, absolutely. I'm happy to answer that.

First of all with regard to DNS, the Internet works on a series of numbers and we go to www.website.com, but the Internet doesn't understand what that is. DNS translates back into the actual address on the Internet, which is called an IP address. So it tells the Internet how to route itself and how to get to the location.

Cybercrime actors take advantage of that, so when you click on a link, if you were going to impersonate the cyber centre, for example, you might create a domain or a website that would say "cyber.gcca". You might miss the dot and so fool Canadians; they wouldn't see it—that's called "typo-squatting"—and then they would go to something that looks like the cyber centre website, except you're downloading malware when you're there.

So a DNS firewall says, hey, that's accidentally been blocked as an illegitimate site, so when you click, you don't go there. So it stops you from having the consequence of either the mistyped address or the deliberate....

In terms of my using these, I absolutely do. I put them on my personal devices because, frankly, it gives me a level of protection. I admit it's only a matter of time before something happens and I click. I want to make sure that I'm as protected at every level as I can be.

Mr. Jack Harris: Thank you. If it's good enough for you, it's good enough for me, and I think it should be good enough for a lot of people to take advantage of it. Thanks for that. I'm one step further to being more secure.

Let me ask you a question about the whole issue of ransomware. You say that it's going to be a continuing threat. Leaving aside the ransom part of it, the capability of shutting down someone's access to the Internet itself seems to me to be a threat. As for any individual, criminal or state that has access to that capability and has that as part of its list of weapons, shall we say, that it can use in hostilities, surely it must be considered a threat that must be defended against by government or by any country that wishes to defend itself, just as we would defend ourselves with anti-aircraft capabilities, etc.

Is Canada protected from that kind of threat not just to critical infrastructure like electrical systems, but to banks, hospitals or access to medical information that might be needed to treat patients, things that could shut down not just the economy but activity in general?

Mr. Scott Jones: I think there are a few things we talk about in the security realm. We talk about confidentiality—protecting the information itself—then the availability and then integrity of what's being transmitted so that you can't change it en route.

You're really talking about availability, and I think that's such an important question. There are a few techniques that would be used.

If you're looking to, for example, take me off-line right now as I'm talking, you could do something like a distributed denial of service attack and just overwhelm my Internet connection so that it doesn't know what's good traffic and what's bad. That's something where there are very robust mitigations in place. Canada's telcos have for years been able to defend against this. There are DDoS attacks that happen on the Internet constantly that we just don't know about because they are so well defended against.

Also, then, you have things that will target specific elements of infrastructure. That's usually taking advantage of a vulnerability. That could be flooding, overwhelming it—

Mr. Jack Harris: Could we just focus on this ransomware capability?

Mr. Scott Jones: Yes.

Mr. Jack Harris: You shut down somebody's access. You shut it down, so that's a particular capability, never mind a ransom. Are there countries or operations that can do that en masse and are we vulnerable to that as a nation throughout? If we are, do we have any defence against that?

● (1605)

Mr. Scott Jones: Ransomware typically doesn't work in that way. It's typically used to target, and then it's holding something for hostage, whether it's holding your data for hostage by taking it out of your system and then using that to say that if you don't pay them they're going to release the information, or by encrypting your data and making it unavailable to you. It tends to be done on an organization-by-organization basis.

In terms of a mass ransomware type of thing, we have seen where ransomware will propagate. We saw some examples where it impacted a company, such as Maersk shipping, for example, which was impacted by ransomware, and the National Health Service in the U.K., where ransomware started to propagate and get out of control.

The defence against this is really that you start to block the infected systems and start to do a containment model. At the same time, you start to share the information and innoculate. There are responses in place, and there are things that can be done to protect against it. The worldwide community is pretty adept at dealing with it, but that doesn't mean that there aren't victims of consequence during that process.

Mr. Jack Harris: You still think that someone could use that in an organized and coordinated or massive way to attack a country or a country's enterprises, whether it be a hospital or—

The Chair: We're going to have to leave it there. Mr. Harris is over his time.

Mr. Motz, please. You have five minutes.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you, Chair.

Thank you, Mr. Jones, for being here again. I always appreciate the level of expertise you bring to the field. Thank you again for the great service that CSE provides Canadians.

Scott, you've previously appeared before this committee in talking about our approach to protect our mobile and telecommunications systems and networks, namely, through a system similar to the U.K. model, where they inspected everything before it was even installed. As you know, the U.K. has moved away from that model, going so far as to reverse their decision to allow Huawei in light of security issues raised by the security teams in their government.

Huawei, which we all know falls under the Chinese state-controlled company, because of their security laws cannot be safely used in Canada according to various—basically all I've ever seen—independent experts.

Is your team still working on a recommendation on Huawei for the minister, or have you already briefed the minister and provided advice on the best way forward with respect to this company?

Mr. Scott Jones: I think that one of the things that's really important is that my role here is to advise and implement on policy, and policy decisions go before the government and the elected officials. I have to be careful not to take away our.... It's not my goal to.... I'm not elected, so I really respect—

Mr. Glen Motz: I appreciate that, Mr. Jones. I guess, based on that answer, I would say that you have already provided that briefing, and if you have, thank you for doing that. I'm sure that's something that will go a long way to making the decision.

Your report highlights in many parts the use of indirect attacks to gain access to desired systems—going after suppliers, business partners, clients and governments, all with the intent of gaining access to a particular target. We also know that China is one of those countries that have been identified by various security agencies across our country and other countries. It would seem counterproductive to have the system that transfers all of our information, namely the Internet, controlled by a company that falls under the thumb of a country focused on theft, misinformation, espionage and disruption.

Can you help me and Canadians understand why we still don't have an answer on Huawei?

The Chair: Mr. Motz, you've asked twice that an official of the government comment upon a decision of the cabinet. I think Mr. Jones declined to answer that question the first time. He should probably decline to answer that question a second time.

Mr. Glen Motz: I appreciate your intervention, Mr. Chair. Please take that time off of my five minutes. That would be great.

Mr. Jones, previously—

The Chair: You know I'm always generous with your time, Mr. Motz.

● (1610)

Mr. Glen Motz: Not as generous as you are with Mr. Harris, but hopefully today will be one of those days.

The Chair: He does very well, I have to say.

Mr. Glen Motz: Mr. Jones, you've testified before that you were looking at how to manage security products—this is really key—in a global supply chain and rolling software updates. That was something that you focused on at one of the last times you were with us. That was in September 2018. It's been two years. Have you come to any resolution on securing hardware and software that brings rise to this concern?

Mr. Scott Jones: That's a fairly in-depth question, but I'm happy to try to answer it.

I think there are a few elements. Certainly, the broader Internet and the broader aspect that we face in terms of technology is that it is a global supply chain, and there are a number of vulnerabilities that are in the software. There are a few things that we're pursuing.

The first one is really about building up the layers of security and the work that we're doing with various industries. In the context of the electrical infrastructure in Canada, one of the things we are looking for is to build in security, but not just in the products themselves. We're looking at it from a very similar approach to what would have been done in the safety world for the equipment as well, and now also how we can watch and monitor with them that equipment to make sure it's operating as expected? It's about building it to be as secure as possible, knowing that there's likely to be vulnerability. Then, how do you watch to make sure that it's operating as expected so that you can respond quickly? It's also about building in a response capability as well. In the industry, we call that “managed detection and response”, but it's really about knowing and understanding that nothing is invulnerable anymore. The systems are flawed no matter where they're built, and—

Mr. Glen Motz: So it would be a fair point to note that we can't say that we are secure. Saying that it's a permanent battle would be a fair assessment, and we have to be vigilant moving forward. I guess it would then make sense that we would want to only use supplies from trusted countries. That would make sense.

I have a question. You've appeared before NSICOP as well, and as you know, we tabled a report recently detailing serious concerns around foreign interference and influence in Canada and how China has played a role in those concerns.

As a country, we've been deemed to be an attractive and permissive target, according to that report. From your perspective—

The Chair: Mr. Motz, I'm stopping the clock.

Mr. Glen Motz: This is a question specifically about what we need to do to change that.

The Chair: Okay, I just want to be cautious about whatever questions, answers and deliberations about NSICOP. That is, in fact, a committee of parliamentarians who are sworn to a high level of secrecy, like you.

Mr. Glen Motz: Yes.

The Chair: I just want to make sure that you're going to stay within those guardrails. We know that guardrails are important to stay within these days.

Mr. Glen Motz: Yes, I know that guardrails are very important. I don't want to go to jail for my guardrails. It was tabled in their NSICOP report and thus has already been made public.

The Chair: Okay.

Mr. Glen Motz: Scott, you've read that report. What do we need to do as a country to stop or change being such an easy target? We're an attractive and permissive target. What do we need to do differently to fix that?

Mr. Scott Jones: I think there's a challenge. My goal is cybersecurity, so in raising the cybersecurity bar in this space, one of the things we're encouraging all Canadians to do, frankly, is to take some steps to raise that bar across the country with some basic security elements. Some easy steps can be taken that would increase our security bar. I mentioned them earlier: Basic hygiene, meaning patching our systems, would have a huge effect on our industry and on cybersecurity. That immediately makes us less vulnerable to outside activities and outside exploitation.

The second piece is that when we're looking at some of the applications and technologies out there, we're going in not just based on the cost. The lowest-cost product isn't always the best one. Sometimes looking and saying what's important in security and looking at how to measure that is a challenge that we all face. I know that we all want a good deal, particularly as we're heading into the holiday season and looking for gifts, but a lot of times cheap technology will be out of date and it will not be updated and patched.

● (1615)

The Chair: We'll have to leave it there, unfortunately. Mr. Motz, you are well over time.

Madam Khera, you have five minutes, please.

Ms. Kamal Khera (Brampton West, Lib.): Thank you, Mr. Chair.

Thank you, Mr. Jones, for being here and for your report and all of the incredible work you do.

I'll pick up where my colleague Kristina left off. Your report noted that the vast majority of cyber incidents in Canada occurred because simple or basic elements of cybersecurity weren't followed. In other words, this was completely preventable. What steps can the cyber centre take to further increase awareness and compliance to ensure that Canadians are taking the appropriate steps to protect themselves? What can my constituents do? What is the responsibility of businesses, individuals and the government?

Mr. Scott Jones: That's an excellent question.

I don't want it to sound as if we're blaming Canadians for this, because it isn't easy, nor do I want to blame businesses. The problem with the technology world is that we've made it too hard for business to keep up to date, and a small business owner should not also have to be a firewall expert and a networking expert and a computer expert. There's a certain amount on business to take this on and make it easy for them to do.

But there are some simple things. Our small and medium-sized business guidance does give some simple steps that we've written to be accessible. I really did appreciate the comments about making the report accessible. We really are trying to write this for advice and guidance for all Canadians.

For individual Canadians, though, we do publish tips. We try to put them out such that it's one simple action to take to make yourself more secure. It can be, today I'm going to make a unique password for my bank. That immediately means if it's not being reused—you never use that password—you're raising the bar for your bank. Multi-factor authentication is harder. When you log in to your bank, for example, and you turn it on, it means somebody else can't log in as you. Even if they get your password, there's another step to verify. That, again, makes it hard, so the cybercriminal is going to move on. Essentially what we're talking about is putting hurdles in place. Why would a cybercriminal want to jump over them when they can move on to the next target, who doesn't have the same hurdle in place? That only works for individuals.

When we look at companies, especially large organizations, sometimes they're worth the effort, so they'll pay to invest to develop unique capabilities after them, and that's what we call “big game hunting”, which cybercriminals will target. That's where a large organization has the benefit of a larger budget and a larger cybersecurity organization so they can bring in a really qualified provider to help them.

Ms. Kamal Khera: Thank you for that.

We've also heard about the impacts COVID-19 has had on foreign interference and cyber-attacks during the pandemic, especially now that we're living in this virtual setting. I can see that happening when we have vaccines rolling out and other things in place. What additional steps has the cyber centre taken as a result of this pandemic, especially with the RCMP's Canadian Anti-Fraud Centre?

Mr. Scott Jones: One of the things we've done, which we started early in the pandemic, was to simply work with providers—partners around the world and commercial providers—to take down anybody that was impersonating the Government of Canada. I think we've all gotten the calls from someone pretending to be from a government agency. The same thing happens on the Internet, where you get emails, etc. We've taken down over 4,000 of these since March. It's something we did to try to decrease the amount of fraud that's happening.

The second thing that we've also tried to do is to raise awareness. We did some joint public awareness campaigns with the RCMP and the Canadian Anti-Fraud centre to get information out to Canadians to say, “Hey, look for this, because here's something we're seeing.” We've really tightened up the path of communications there in terms of making sure that information is being shared quickly and is getting out to Canadians so they can know what to be aware of and what is the latest scam.

The third piece, though, is that we have been working with telecommunications companies as Canadians report spam. For anything that's related to the Government of Canada, we've been able to proactively put things in place. For example, on the programs that the government has put in place in terms of the CERB or some of the other response benefits, we're ensuring that we know what those look like ahead of time so that we can pre-position fraud detection. If somebody tries to pretend to be the CERB site to try to get information, we have commercial providers that are looking for that proactively to take it down before any Canadian is victimized.

We're really trying to get ahead of the curve. It's something where we've really relied on those government departments that are responsible for delivery to get that out there.

Finally, we're also telling everybody to go to the root of the truth. If you're looking for the facts, go to the place to get the real facts. In a pandemic situation, Ottawa Public Health, Public Health Ontario and the Public Health Agency of Canada are those roots of truth for me. They'll obviously be different wherever you're—

● (1620)

The Chair: Thank you, Madam Khera.

Ms. Kamal Khera: Thank you.

The Chair: For two and a half minutes, we have Madame Michaud.

[*Translation*]

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

I would have liked to know more, like my colleague Mr. Motz, about everything related to 5G and the government's management. I don't want to go into that, but still, since we want to inform citizens, once again, I'm sure my colleagues have received as many emails as I have from the public about 5G, which is worrisome. I think it is also divisive. There is a lot of misunderstanding. I would like you to speak to us about it.

You said earlier that the population should not be afraid or worried, but there is still a duty to inform.

[*English*]

Mr. Scott Jones: I'm not sure I understood the question. I'm sorry.

[*Translation*]

Ms. Kristina Michaud: I can rephrase it.

How do 5G threats translate for Canadians and Quebeckers?

We receive a lot of emails from our fellow citizens, who are worried about what this may mean for their physical or mental well-being. In order to reassure them, perhaps, I would like to hear from you about what this represents at the moment.

[*English*]

Mr. Scott Jones: Thank you. I'm sorry for the trouble in understanding that.

There are a few things that I would want to highlight. I think that when we're looking at any new technology or new development that's out there.... There is some misinformation around 5G, but I will set that aside to really focus in on the security aspects of this. What we're looking for is that this is a network that can have many more devices that support much faster communications. It has much higher bandwidth. It's much faster, with many more devices connected to it, and it's pretty much real time, which means that you can do things like sending commands to self-driving cars over these types of networks. It's designed for that type of environment.

In general, the threats we look for are around the confidentiality, integrity and availability of things like the network. For the network itself, can I communicate? That's availability. You really look for things like the robustness of the equipment. Do you have multiple providers so that if one provider becomes unreliable you can replace their equipment at some point with something else? That's around the availability side.

Then we look at the integrity. If I send a message over that network, will it get there in the form in which I deliver it? That's where encryption is the key piece for integrity. If I want a message to be clearly delivered, I will send it in a way such that it can't be modified. That's what encryption gives us for integrity. You might have things like digital signatures, etc. What that does is say “this message cannot be modified now”, and we do that through cryptography.

The last—

The Chair: Unfortunately, I have to leave it there.

Mr. Harris, you have two and half minutes, please.

Mr. Jack Harris: Thank you, Mr. Chair.

I do detect a little bit of victim-blaming in some of the commentary and suggestions that are coming from some of your work. Obviously, people are not sophisticated in the use of this equipment.

Are there any of these patchings of our systems that you're urging people to do? Can any of that be mandated by the government via the system providers, the Internet providers or groups of manufacturers to take away some of those even simple steps and make people more secure?

Mr. Scott Jones: We certainly don't want to blame the victims for this. It is hard, I understand, just keeping on top of all of this.

The first thing that we say to businesses, as well as individual citizens, is to just turn on auto updates—on our phones, just slide it to auto updates. However, the industry does need to make this easier. In many cases it is: Our home laptops, our home computers, etc., tend to do this now by default. You have to manually set them to not auto update so that the updates are manual.

That's good progress, but it needs to be made better.

The real challenge is for businesses where the equipment doesn't do that. The equipment requires a system administrator to download a patch or an update, to go onto the device, to install it, to test it, and it may or may not work because the device, really, is finicky. That's where the industry really does need to start stepping up on cybersecurity to make it easier for these small and medium-sized organizations to stay up to date.

However, there is some hope. The cloud does offer some benefits to these organizations where updates are automatic. With regard to the cyber centre, one of the things we did when we stood it up was to move our operations into the cloud because we wanted to work like every business in Canada either was working that day or was going to be working. We wanted to live our own advice. What we do is.... I get updates. In fact, I just saw—my computer just told me—that I just got an update for my Microsoft Teams environment that we use to say that, yes, we have the updates. You get them right away when they're issued by the vendor.

That makes it easier. That takes the pressure off those small and medium-sized organizations to do things. When you do that, that means that you don't have to do it yourself. You don't have to go in and download the patches and install them because it comes with it.

That's really where we're saying that it has to be easier for the users and not place the blame on them.

● (1625)

The Chair: Okay.

Thank you, Mr. Harris.

Mr. Van Popta, you have five minutes, please.

Mr. Tako Van Popta (Langley—Aldergrove, CPC): Good.

Thank you, Mr. Jones, for being here with us today and for your insightful evidence.

I have a question about universities and cyber-threats relating to theft of intellectual property. Perhaps you can comment on that—in the context, of course, that some research universities actually partner with foreign companies to help fund the universities' research.

Mr. Scott Jones: I think one of the areas where we have been doing significant outreach, and that we've been doing with our colleagues at the Canadian Security Intelligence Service, is really to help to inform universities of the threats they are facing, as well as give them some practical advice. They are open research organizations, and they face a unique challenge in that in terms of cybersecurity.

One of the other areas where we have worked is with what's called CANARIE, the Canadian network for research and innovation. It's a non-profit organization. We've been working with it on improving its cybersecurity, and we've been trying to help it bolster that for all Canadian universities as well. We're trying to take some practical steps to make it easier to protect intellectual property.

At the end of the day, one of the things that organizations need to balance and one of the things that I would rely on my colleagues at the service for is really that, in many cases, people just like to talk about the research that's going on and share it widely because they're really excited about their work. That's one of those areas that I would look to the Canadian Security Intelligence Service to provide the expertise on.

The insider threat from our perspective, though.... We are trying to bolster cybersecurity. We're doing it with partnership. CANARIE is the example in this case for the research access. We're also reaching out to the universities in Canada to provide them with advice and guidance, as well as realistic threat feeds that they should be expecting from cybersecurity to try to bolster it.

Mr. Tako Van Popta: How significant of a threat is it in a economic measurement? How much value in intellectual property is being stolen from universities? How widespread is it?

Mr. Scott Jones: I wish I had an answer to that question. I don't know.

The way our mandate is structured, one of the things we don't do is collect information within Canada. We rely on statistics, like from Statistics Canada or anything that is published by other organizations. I haven't seen a figure that monetizes the loss to Canadian institutions, both short and long term.

Sorry.

Mr. Tako Van Popta: That's fair enough.

Would the simple solution be for universities to quit partnering with foreign actors?

Mr. Scott Jones: I'm not an expert. That question's probably best for some of the areas where they're used to these university partnerships.

When we've been meeting with some of the organizations, one thing that has been emphasized to me is that research is done globally and partnerships are really important. All foreign partners...I'm not sure the universities would say they could sustain that.

One of the things we always say for any organization is to go in with your eyes wide open to the threat you're facing and to what their goals are. Is it a mutually beneficial relationship or is it about getting information out there? That's really where the outreach we've been doing with the service is. Hopefully, it's improving that for Canadian universities.

Mr. Tako Van Popta: Of course, these comments about universities would also apply to companies. Just as you were talking, I had to think of the CanSino issue just recently where it looks like some intellectual property around the COVID-19 vaccine may have walked out the back door to the benefit of another country.

I have a quick question. The question is quick; I don't know about the answer.

The best and most efficient allocation of risk when it comes to cybercrime.... I'm thinking, for example, of my relationship with my bank. It's very simple for me to change my password, so maybe if some money is stolen out of my account, that risk should be completely mine and not the bank's. Maybe the risk should be allocated to the software company that provides that interface.

Do you have any commentary about that allocation of risk?

● (1630)

Mr. Scott Jones: That's a very profound question.

In terms of the allocation of risk, I think the banking example is an excellent one. Not only do they have cybersecurity elements, but they also do have a substantial amount of anti-fraud, so if they see something that's out of character, it tends to trigger their fraud controls. I've always been quite impressed with that

I think we've all fallen victim to something like debit card skimming and things like that at some point. Hopefully nobody has, but I had my debit card skimmed once. I think there are some elements there.

Risk is one of those areas where it's really about how to minimize the risk. I'm not sure about risk transference. It's a challenging question. I think, in that case, the question would really be whether you are doing something that's absolutely negligent or not.

Again, that's probably a question best left to a lawyer, not to a cybersecurity engineer. It is something where—

The Chair: Thank you, Mr. Van Popta.

Mr. Van Popta has actually anticipated the question I would like to ask. Maybe we can get to it towards the end because I think it is a live issue.

With that, we have Mr. Iacono, for five minutes, please.

[*Translation*]

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

Thank you, Mr. Jones, for being with us and keeping us up to date with what's happening in the world of technology.

My fellow citizens in Alfred—Pellan, as well as Canadians in general, are concerned by partial data collection. The concern is related to cyber-attacks and the use of data by commercial businesses for targeted advertising. This, of course, is unacceptable to many people.

Can you tell us how we can teach citizens how to properly protect their personal data?

[*English*]

Mr. Scott Jones: Thank you for that question, which I think really does go to the root of some of the things we talked about in the national cyber-threat assessment.

The amount of personal data that's out there on us now is quite extensive. One thing that's been noted is that in any cyber-attack, not only do they have things like your usernames and passwords that they've stolen from other places; in many cases, they also have the answers to your security questions—your mother's maiden name, your first pet, what school you went to and things like that. Those things that we always relied on as kind of a second barrier to security are now just the same as the password type of thing. It's critical.

To protect information, I always ask, “Why does somebody to know this? Are they asking something that's legitimate?" If I'm going on and buying an online purchase and they ask for my social insurance number, they don't need that for the purchase. I'll walk away. They need to start collecting the minimum amount of information viable. The second thing I think about is the risk I am taking on. Of course I do online shopping, not just because of the pandemic but also because it's convenient for me. Where is it going? Who's behind this service? Is it using a third party payment system? That can protect you financially. In reality, though, things like credit cards do have good protection.

It really boils down to, “Do they really need to know?” Over-collecting of information is something we certainly look at. Even when we designed the cyber centre, we made it so that there's a phone number people can call for help. We looked at the minimum information we absolutely needed to be able to respond and help the person, and then we did a privacy assessment on that to protect it. That's something I think every business should be looking at: . “Do I really need to know all of this? Do I really need to keep the history of every purchase they made?" Maybe they do. There could be a real reason for that. That's something I think the privacy commissioners have advice on.

From a cybersecurity perspective, the more information we put out there and the more information we put on our social media accounts, the more vulnerable we're making ourselves. Frankly, we're giving them the information they need to target us.

● (1635)

[*Translation*]

Mr. Angelo Iacono: Thank you.

For several years, we have been aware of the illegal activities and transactions that take place on the deep Web. For example, there is drug trafficking, prostitution, arms trafficking and even contract killings.

Can you tell us if we have been able to put in place means to reduce these worrisome activities and track the criminals in question?

[*English*]

Mr. Scott Jones: I think that investigators at the RCMP, or perhaps at the Sûreté du Quebec, for example, might be in a better position to answer about the investigation phase.

One of the risks we see is that the dark web is certainly facilitating cybercriminals and cybercrime tools. There is an entire ecosystem out there where you can go on and say, “I want a tool that's going to allow me to do this.” Let's say you want to target this type of organization, or even a specific organization. They'll bid and tell you what it will cost. You can pay for 24-7 support or you can pay for a custom tool to be developed for you to achieve your goals.

Then there's the organized crime that goes behind all of that. It is a large enterprise out there. It's facilitated by the dark web and anonymous payment systems like Bitcoin and online currencies. One of the key challenges is that the entire system is designed to be anonymous and to not have attribution.

[*Translation*]

Mr. Angelo Iacono: I see.

As far as cyber-attack tools are concerned specifically, since they are technologically advanced materials, it is reasonable to assume that their manufacture is not easily within reach.

Are you able to tell us, today, who these manufacturers are? Are we able to stop them from selling the equipment on Canadian soil? More importantly, are we able to seize anything in the marketplace that can be used to hurt us?

[*English*]

The Chair: Unfortunately, Mr. Iacono has gone over his five minutes. It is an important question. Perhaps you can circle back to it in another answer.

Mr. Kurek, you have five minutes, please.

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

Thank you, Mr. Jones. This is very enlightening. It's certainly an important subject, especially in the circumstances we find ourselves in regarding COVID. I hope to get through a few questions.

Are there any areas in which Canada is at a higher risk, or is more susceptible, due to evolution in the use of the Internet since the start of the COVID-19 pandemic and the explosion of online capacity required to deal with the pandemic?

Mr. Scott Jones: Let say there are a few areas where we would say that we have to be very careful about the increased risks. One thing is that with so many of us working from home, the fact is that it has changed our technology environment. We're mostly working outside of our organization's perimeter, so in terms of a lot of the defences we relied upon, many Canadians are now working from home and connecting directly to the Internet.

There are ways to try to minimize and mitigate those risks. Those are some of the things we published, but this is probably one of the biggest risks; it's the fact that we're now outside of the defensive perimeter that was set up. In some cases, we're not. For example, I never leave our defensive perimeter because of the way we have set up our remote access. We designed this to work remotely so that I could work from home and stay behind our full suite of cyber defences. In the majority of the government, it's like that.

For a lot of organizations, though, one of the things we have encouraged them to do is to make sure they are either doing something similar to the design we have for government or supplementing with other defences that are there.

That would be one of the major risks, but also, then, we're holding more data at home, and we're having conversations like this, although this is a public forum. There are things like that where we just need to be conscious of what we're doing as well.

Mr. Damien Kurek: Thank you very much for that.

Obviously, health infrastructure is at the front of everybody's mind with the advent of COVID over the last 10 months or so. Have we seen an increase in the threats faced by our health care systems?

How is your organization able to assist in ensuring that the briefings don't get to just the federal government, but that the information is getting onto the ground to ensure that for local hospitals, local clinics and doctors who are working from home—and, in many cases, Canadians who are video-conferencing with their doctors—the whole system is protected?

● (1640)

Mr. Scott Jones: That question really goes to some of the heart of what we've been doing. The goal is to not have this information sitting inside of the federal government, but to get it out to into other hands. I mentioned this earlier when I talked about the weekly call we do with the health sector. That includes our provincial and territorial colleagues, but also any organizations that come to the table. That grows every week as more people sign up for it, and we're happy to walk through what we're seeing on cybersecurity, including advice and guidance.

In general, though, when we also see.... This is where we do leverage in terms of what our foreign intelligence mandate can tell us in terms of where targeting is happening. We have gone out to specific organizations where we see things and have given them tailored advice because they're a system of importance to the government. Really, it's about getting that information into the hands of somebody...our goal is to get it before they are a victim so that they can proactively take steps to protect themselves. That's what we do every week, and we do it consistently.

Then, of course, we publish a number of alerts and advisories that go to sectors. We published the threat assessment for the health sector, and we made that public. We sent it to the health sector ahead of time as well to say what it was that we were going to be saying about things they needed to be aware of. We're really trying to raise the knowledge of the sector, but also to work with them on what solutions will work as well. Our goal is to encourage them to share within the sector best practices—

Mr. Damien Kurek: I apologize. I have about a minute left, and I'm hoping to get in one last question. I don't mean to cut you off.

We are in what is being considered an “infodemic”. There's a ton of information, a ton of misinformation and then a whole bunch that's somewhere in the middle, and I think that's what makes conspiracies believable, because there's always that little bit of truth.

Specifically, regarding the integrity of Canada's democracy, I would ask for your comments on threats to Canadian democracy, elections or any infrastructure associated with that.

Mr. Scott Jones: That's big.

We're really talking about some of the things we've highlighted in our first and second “Cyber Threats to Canada's Democratic Process” reports that we've issued to really try to highlight some of those. It remains a challenge.

Now, I think the response isn't necessarily a cybersecurity response. You'll see Elections Canada stepping in about disinformation. You face this as members of Parliament and as candidates at some point, etc., and how to combat that.... It is one of those areas where, from a cybersecurity perspective, we're very limited in what we can do, because it is just bad information being posted somewhere, frankly, and we're not in a position to be the arbiters of truth.

But it is something where we always are looking to say, number one, how do we bolster our cybersecurity? The goal of the report itself was to debunk some of the threats and some of the misinformation that could be out there and to say, no, this is how democracies work. You can't go online and just change Canada's vote tallies, as there are procedures in place, etc.

The Chair: We're going to have to leave it there, notwithstanding many efforts south of the border to change the vote tallies.

Madam Damoff, you have five minutes, please.

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

It's wonderful to have you here, Mr. Jones.

Thank you for your work and for your report. It's really helpful. You are presenting it in a way that Canadians can understand. A lot of this is far beyond our knowledge. It's important to simplify it so we know what we're talking about.

Back in 2018 you said you were “confident sufficient safeguards exist to deal with the risks of telecommunications hacking or spying by China”, but you acknowledge that risk could increase with the introduction of 5G.

This week's Citizen Lab came out with a report. I don't know if you've seen it, but it said that Canada's 5G strategy shouldn't "be designed to solve a Huawei problem", but it should address a 5G problem "to ensure the resiliency, security".

I'm wondering if you could speak a little about that and about what kind of strategy we should be looking at as we move and companies move to 5G.

Mr. Scott Jones: I'll have to be careful because the policy decision is still pending.

In general, what we're looking at when we're looking at anything approaching a 5G network is that the system needs to be secured in layers, everything from how it's maintained to who's accessing it, to the variety of equipment itself, to whether the software used is open source, publicly scrutinizable or closed, meaning it comes from a particular vendor, and then it's also how we leverage it. That's one of the things where modern telecommunications offer a significant advantage now.

We used to rely on the network itself for security and how you transmitted because encryption couldn't be used. It was too expensive. Our devices weren't fast enough to do it. It is a challenge, when you talk about the law enforcement context.

Encryption offers protection for private information that you're transmitting. It's hard to observe. Encryption is now enabled more and more on our devices by default. All of the Government of Canada websites mandate that they're encrypted. So encryption itself is protecting confidentiality and the ability to know what I'm saying or what's happening.

The second piece is the integrity, knowing that when I send a message, nobody is modifying it. That's one of the areas where we need to think about end to end. For example, if the city is facilitating an ambulance to get to the hospital and is changing the lights, you want to make sure that it's not sending green, green, where traffic will cross—things like that. That's the integrity of the message, meaning that the message you want to send is getting there exactly as determined. You use encryption for that. You don't really care if somebody sees the message; you just care that they can't change it.

Then there is availability: we need the networks to be there. That's where we really look at a robust strategy talking about vendors building better equipment and better software. How is it tested? It's international in scope to make sure that it meets minimum standards, but you also have multiple vendors in place. We want a multi-vendor strategy. We want diversity in the market. We want these things in every section regardless of the type of network or the type of equipment. We're always better off than when it's a monopoly.

We really want to leverage all of those things. That's what I think the Citizen Lab report was getting at. It said it's multi-faceted. There's not one solution to the challenge we face; you need to apply multiple different aspects of security. That's certainly what we try to layer into any security program we do. It's not unique to the next generation mobile network versus a fixed network or anything that's.... For example, we use the same security modelling for the incredibly high-speed network I have at home right now.

● (1645)

Ms. Pam Damoff: I'll be quick because I only have a minute left.

Canadians had expressed concerns about the COVID app and giving away their private information, which we know is not the case. Yet the same people will upload a photo of themselves to an app that will automatically age their face, without even thinking that all of that was going to a Russian company. How do we get past that? You see it on social media all the time, where people are providing access to photos and private information. Let's share personal information that ends up being used for security questions, and you answer them openly on Facebook. How do we educate Canadians about that?

Mr. Scott Jones: It's certainly a challenge, and I wish I had an answer to that question. It's certainly one of the challenges we face.

The COVID alert app was a frustrating experience because of that exact concern. From my perspective, the application was built in the open. We tested it with commercial providers to make sure that we had done everything we could to test for vulnerabilities or just coding errors. It was open sourced. Privacy commissioners reviewed it, but it still persists. It just comes with, "Well, it's the government".

I saw a cartoon. It was the 1950s. It read, "I can't talk. The government might be listening on the phone". And now, you say, "Hey, listening device", which is one of those home speakers we have, "tell me what I'm doing?" It's recording everything we're saying. It's this dichotomy out there, where people are....

I wish I had a great answer.

The Chair: Who knew Siri was out there in 1950?

Madame Michaud, you have two and a half minutes, please.

[*Translation*]

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

I would like to thank my colleague Ms. Damoff for her interesting question. And the answer, in fact, was just as interesting.

I am particularly interested in the task force that was created, and in which the centre participated to protect the 2019 federal election from foreign interference, especially given the fact that an election could come sooner than expected. This is worrisome.

I can't help but think of all the things we've seen on TV, for example *The Great Hack* and *The Social Dilemma*. I don't know if my colleagues have seen them, but there's definitely something worrying there.

What specific measures have emerged from this task force to counter misinformation campaigns or foreign interference in federal or provincial elections?

Are there any specific actions or recommendations that have been made by this working group?

● (1650)

[*English*]

Mr. Scott Jones: I'm going to assume that you're talking about the work of the security and intelligence threats to the elections task force that CSE chaired on behalf of the community.

We're doing a few things. We did work with Elections Canada to support them overall on cybersecurity. I could go into a lot of detail on that, but so could the Chief Electoral Officer and his team.

One of the aspects for us was also making sure that every registered political party that wanted to was getting regular cyber briefings. My team did that on an ongoing basis throughout the campaign to make sure that we shared any cyber-threats that we were seeing. We also contextualized it to say what was really important and what they could be expecting to see. That tended to be with the officials inside of the party.

We also had the hotline set up where political parties could call if they needed assistance with something, such as fake social media accounts, etc. Most of the social media providers were fairly responsive to those types of things. We would try to ensure that connections were made there.

It does remain a challenge. That's one of the areas where we are always looking for ways to connect.

On the other hand, one of the things that has been repeatedly reinforced to me is that if, for example, you are impersonated on social media, I cannot make a complaint on your behalf. You have to do that. The social media companies are quite adamant about that. It's one of the areas where, if something like that does happen, we try to facilitate and hopefully accelerate getting a resolution. We did see some incidents like that where parties asked for some support.

Then, of course, in the report itself—the first and second ones—were the threats to Canada's democratic processes, where we really try to lay the groundwork for what cyber-threats we expect to see to Canada's democratic institutions.

[*Translation*]

The Chair: Thank you, Ms. Michaud.

[*English*]

Mr. Harris, you have two and a half minutes.

Mr. Jack Harris: Thank you, Mr. Chair.

Mr. Jones, could you tell us what's the difference between cyber defence and cybersecurity?

We know your agency reports to the Minister of Defence. As my recollection of defence critic, I don't think you're part of the department. The military, of course, has to protect it's own infrastructure, equipment, communications and all of that.

Is your agency involved in defence planning in any way? You talked about table-top exercises with the electrical power grid people. Do you engage in these kinds of exercises with the military in terms of defence planning or scenarios planning for military activity?

Mr. Scott Jones: We are part of the Department of Defence and we report to that minister. We report to the minister, but we are a separate agency under Defence. I almost slipped back seven years there for a second.

With "cyber defence" we're really talking about when we're actively doing something to prevent a cybersecurity incident. We're taking a block. We are the cyber defenders of the Government of Canada. We take over two billion actions a day, over and above those that are available commercially to protect the Government of Canada. We have a cyber defence part of our program.

"Cybersecurity" is the broader term that we use. That's also about the proactive measures. Rather than just taking action at the point of compromise, it's building those defences and building it to be secure from the start. It's security by design. That's really, in my mind, where we differentiate cybersecurity from cyber defence. Cyber defence really is about that action you take to protect.

In terms of our work with the Department of Defence, obviously they are responsible for the defence of their systems. They're the experts on military equipment, but we do provide a number of services. One would be cartography and the encryption systems that they use to protect all Canadian forces operations. That's a 70-year partnership where we've worked with them on those types of things. We certainly work with defence on any exercise planning.

We would also do that with any other organization to say how we respond to any cybersecurity incidents. We really look for opportunities to raise that bar proactively. We would do that as part of our mandate.

The Chair: Thank you, Mr. Harris.

Sorry, I cut you off a little early, Mr. Jones. Do you want to complete that sentence?

Mr. Scott Jones: Yes, I just want to say finally that part of the CSE Act is about defensive cyber-operations and foreign cyber-operations and being able to take action when Canada is threatened and with the authorization or the acknowledgement of the Minister of Foreign Affairs and the Minister of Defence to say that we need to take action in foreign space to protect Canada as well. That's part of the CSE Act that Parliament passed.

● (1655)

The Chair: Thank you, Mr. Harris.

Earlier in your answer, I thought, you said there were something like two billion attacks a day.

Mr. Scott Jones: We take two billion actions per day to prevent some malicious activities. Some of those are scanning the government, looking for vulnerabilities. Others are malware that is attempting to have itself downloaded.

The Chair: Really? That seems like a lot of attacks.

Mr. Scott Jones: Well, some of it is bulk scanning. It's like somebody is going to every government computer and rattling the doors and checking the windows to see if you left anything unlocked. So we stop that. If you can't see our vulnerabilities, you can't exploit them.

The Chair: Okay. Thank you.

Mr. Kurek, go ahead for six minutes.

Mr. Damien Kurek: Thank you very much, Mr. Chair.

This has been a topic of some debate in Canadian politics as of late, brought on by a fairly explosive New York Times editorial regarding MindGeek and the abusive videos on the site Pornhub and other things. I'm just wondering if you have any comments on what can be done for victims of some of these terrible crimes, such as child pornography or rape. I would love to hear the practical solutions, the recommendations you would have to ensure that these terrible practices could be stopped.

Mr. Scott Jones: Well, it's a disturbing question just because of the material, but it's a deep question as well. I think the broader answer, the best position, would come from my colleagues at Public Safety Canada who really are looking at the online harms aspect to see how to reduce that.

Some of the cybersecurity elements—techniques and tools—that we emphasize are aimed at helping prevent people from getting into situations such that they could be exploited in that way or prevent their kids from being exploited in those ways. That's really one of the challenges.

I think one of the other areas that is a big challenge, though, is that these platforms are designed to be barrier free in a lot of cases. One of the famous Internet memes, again from the New York Times, is actually that, “On the Internet, nobody knows you're a dog.” Because people are so anonymous, you have no clue who is behind that. That's one of the things with online harms. How do you balance that fact with who is interacting with the kids, or with who is interacting with me online, etc? You can be anonymous, and that enables a lot of activity. But the broader answer to some of those questions should probably come from Public Safety Canada. From a cybersecurity perspective, we can continue to give tips and hopefully help people keep their kids and themselves safe online too.

Mr. Damien Kurek: I appreciate that. Certainly there is the prevention part and then there is the cybercrime part and then there are a whole bunch of other aspects that need to be addressed.

One of the concerns—and this goes back to the conversation about information and misinformation—is with foreign state-directed editorials and advertorials, and the threatening of or influencing of cultural groups or whatever the case may be in Canada, with foreign state actors using an online presence to try to direct influence within Canada. I am wondering if you could comment on that and on anything that could be done to help ensure that there is integrity in that side of things?

Mr. Scott Jones: I really wish my colleagues from Canadian Security Intelligence Service were here to take the lead on this. From our perspective in the cybersecurity realm, our challenge really is trying to inform people, through a national cyber-threat assessment, and to say, “look for factual information.” The Internet is designed to be open and free and to allow this type of communication. From our perspective, as the cybersecurity agency, the advice we have is really to look with a wary eye and not to just trust what you're finding online. On the other hand, I think Public Safety Canada is probably better positioned to talk about some of the actions that can be taken. From my perspective, it looks like and it is legitimate Internet traffic. I don't mean to legitimize it, but I'm trying to say that it doesn't look like it's a malicious cyber-activity. It's not malware or some other aspect like that which is trying to exploit technical aspects of cybersecurity.

● (1700)

Mr. Damien Kurek: That's fair.

Finally, we talk a lot about the cloud and how that provides a certain level of security that would not have been accessible as of late because you don't have to have servers and the physical-locked door and the various layers of cybersecurity to ensure that it could be safe. With the cloud, obviously, it's somebody else's responsibility. One of the further challenges with that is that you have a massive system that holds an unbelievable amount of data. Although there's a greater level of security, there are risks associated with this on a much larger scale, although it's much more difficult to infiltrate.

I wonder if you can comment as to how those risks are mitigated, because that especially impacts small- and medium-sized enterprises that will purchase a cloud storage option for $20 a month or $50 a month, which gives them access to the services, but the scale challenges exist there as well.

The Chair: Unfortunately, Mr. Kurek has gone way over his allocated time. If you can work your answer in some other way....

Madame Lambropoulos, are you up for a five-minute question, please?

Ms. Emmanuella Lambropoulos (Saint-Laurent, Lib.): Yes, thank you, Mr. Chair.

[*Translation*]

Thank you very much, Mr. Jones, for being with us and answering our questions.

I have two questions for you.

With all the trade agreements we've signed over the past five years, more and more Canadian companies are doing business in global markets, as you know. It's great for the Canadian economy, it's convenient and it's good for business.

In the domestic cyber threat assessment, you indicated that the threat of online espionage is certainly much higher for Canadian companies doing business abroad or working directly with foreign state-owned companies.

You've already touched on the subject and given suggestions on how Canadians and businesses can protect themselves. I'd like to know if you have any advice for companies that have direct contact with actors who may be sponsored by foreign states that could threaten cybersecurity.

[*English*]

Mr. Scott Jones: Great. Thank you for that question. There are risks, and it depends on which country we're looking at. Specifically recall that we talked about state-owned enterprises and partnering with those.

This is where, depending on the Canadian business, there's quite a lot of advice out there. It's about understanding what the goal of the partnership agreement is. Is it a technology transfer agreement where it really is looking to transfer the technology to build, or is it about manufacturing and you're outsourcing something?

Knowing what's important to you as a company is the first step. What makes my information special? Is that intellectual property, some unique manufacturing process, tool technique design, or is is my customer base and how I interact with them, how I promote, etc.? By knowing what makes you special and unique, you know what you need to protect—that's the goal that you need to protect.

Then you go in with your eyes wide open. What's of interest to me? Is this a mutually beneficial relationship? When you start to assess this, it tells you where you need to put your cyber defences, which ultimately gets to what I'm responsible for. Are you positioning your company for a takeover? In this case you could expect to see a company looking to get information on your financials. Where are you particularly vulnerable, who are your suppliers, who's your legal counsel, etc.? You could see that in terms of a takeover bid.

If you're looking at a unique piece of technology, then you need to protect that. How am I protecting it and making sure that it isn't travelling, isn't going places where it walks out the door? Really think that through. You're thinking through the threats and then leveraging the advice that's out there.

Ms. Emmanuella Lambropoulos: Perfect. Thank you very much.

On an unrelated note, I'd like to thank my colleague, Mr. Kurek, for bringing up MindGeek, which is about a 15-minute drive from my house. It's something that hits close to home, the fact that it's taking place and that these videos are being put up from a place so close to home.

What recommendations would you give the Government of Canada to ensure that children are not being exploited in a way that they already are? I know that you said that Public Safety is already working on this, but can you give us any insights as to what can be done and what can be enforced at the government level?

● (1705)

Mr. Scott Jones: I think the challenge I face here is really from a cybersecurity perspective. My advice would really be to the potential victims and how to protect things, protect themselves and try to keep themselves from getting into that situation, and really thinking before you share information. Once it's on the Internet, it's there forever. How are you sharing it? What apps are you using? The example of face apps that estimate someone's age was used, but similarly there is photo sharing, etc., as well, and the need not to place oneself in a position where you're vulnerable to that type of harm.

The next would be to get Canadians thinking about how they are using the technology base and asking if they really understand the harms they can get themselves into by slowly being drawn in. Then it's about minimizing the harms and dealing with them.

I'm just not positioned well to talk about the different tools that are placed, because that wouldn't be something that we would be doing from a cybersecurity perspective.

It's certainly something that, as a citizen, I would love to see dealt with harshly and quickly, and that it be resolved, but it's not something that we're in a position to really talk about from a cybersecurity perspective.

The Chair: Thank you, Madame Lambropoulos.

We have gone through three rounds, colleagues. We still have 20 minutes left. I believe that the Conservatives want Madam Stubbs to be next, but before we get to that round, I have a couple of questions that I would like to ask. Maybe the Liberals could indicate to the clerk whom they would like to have. I'm proposing five minutes for the Conservatives and the Liberals; then two and a half for the NDP and the Bloc; and then a further five minutes, which should take us to two minutes for the Liberals and two for the Conservatives. Please indicate to me whom you want to be the questioners.

I want to circle back on Mr. Van Popta's question on the allocation of risk.

A couple of years ago, we had Desjardins here to talk about a data breach. It was based upon what they called a “rogue” employee. What I didn't understand was how a customer of Desjardins would be put at substantial risk of their data going into the dark web, and yet, apparently, Desjardins had no liability for any harm that would happen to one of its customers. I just wonder if, in the context of your cybersecurity centre, that has been a discussion and, if so, where you think that discussion is going.

Mr. Scott Jones: That's an interesting question.

I think we're faced with the challenge that an insider threat, which is really what we're talking about, is something that kind of hits different facets. One is that the person is in a position of trust and does do have access to types of data and information, especially if it's related to their position. Then what controls are put in place from an information security perspective? That's a case of understanding one of the things we say in our top ten, which is to segment and separate information.

There are things at CSE that I just don't need to know. Yes, I'm one of the senior executives there, but that doesn't mean I need to know everything. I don't have access to security files for security clearances. I don't need to know; I don't need to access them. We segment information away, and we protect it. That's for privacy reasons, but it's also for security reasons.

Even in the cyber centre, there are things where there's a limited group of people who have exposure to certain information. We do that deliberately to protect it.

Those are some of the cybersecurity elements that we would say are part of our general advice and guidance, but you first have to know what needs to be protected. That's one of the things, and also what that information could be used against. A lot of times, what I say to businesses is not to think about the harm that it can cause to you; think of the harm somebody could do with the information that you have. Who could they give it to that would harm you?

The Chair: Mr. Jones, shouldn't the onus be on the financial institution? The financial institution has a lot more resources available to it to protect me than I have to protect myself. What I don't understand is why the onus shouldn't be on the financial service provider.

Mr. Scott Jones: I fear that's a question that gets me into legal territory, for which I am wholly unqualified.

The Chair: Well, I was inviting you to jump off the cliff there—

Voices: Oh, oh!

The Chair:—but it is something that has irritated me for a while now.

My second question has to do with passwords, and you're right to argue for passwords. What I don't understand is why all Canadians, when accessing their bank accounts, don't just simply have facial recognition technology. Isn't that the ultimate protection for passwords?

● (1710)

Mr. Scott Jones: That's a great question because it's something that we face in the government all the time. It really comes down to accessibility. Does every Canadian have the technology necessary to access using facial recognition?

It's not foolproof. It is one factor. We always say there are three factors. First is something you know, and a password is something that you know. Second is something you are, which would be facial recognition; a fingerprint is another example. Then third is something you have.

I always think, when I walk into the building at the CSE, that something I know is my PIN code to get in. Something I have is my badge, and something I am is my photo and my face that our security guards check as I pass through the different gates. Those are the physical-world examples of what's there.

Yes, that would add another factor. Passwords would be something you know. Something you have are things like hardware tokens, but those, again, are about accessibility. It really is about finding that balance, but it does add a factor of authentication and something that's important—

The Chair: In the scaling of security, surely to goodness facial or thumbprint recognition technology is far more secure than whether my password is “123” or “321”.

Mr. Scott Jones: Absolutely, it's a much higher hurdle to jump over than if you have a simple and easily guessed password and you reuse your password.

The Chair: Okay.

My final question—and I'm really straining the patience of my colleagues, but who cares—

Voices: Oh, oh!

The Chair: —has to do with an example of a friend of mine who made a commentary on several of the countries that you have named. He has a legitimate fear about threats, both cyber and other. He is a member of a diaspora community.

When he took a threat to the local police force, they said it was an RCMP matter. Then when he took it up to the RCMP, they said, “No, that's a CSIS matter.” When he tried to take the matter to CSIS, there was dead silence on the other end.

I think one of the reasons why the diaspora community doesn't report all of the threats out there is that there is no clear way to report these. Do you have advice for my friend, or for Canadians generally, who are actually threatened by foreign state actors, both on a cyber basis and on a physical basis?

Mr. Scott Jones: I'll have to stick to the cyber advice, which would be our expertise.

First, if you do see something, whether it's a text message that seems to be spam or an email, report that. There are various ways to do it to your service providers. If you fill in 7726, which spells “SPAM” on your phone, and you send your spam text messages there, those go in and they deal with those. In some cases, they do share that information.

Certainly, if people are seeing malicious and threatening emails, or that contain malware or look suspicious, there are ways to submit them in safe ways. People tend not to do that, but there are ways to do it.

Make sure that your systems are always up to date if you feel that you're under threat with regard to cybersecurity. The biggest vulnerability is the system's being out of date—or unpatched, depending on if I slip into techy terms or not.

The Chair: Thank you, Mr. Jones. I'm going to have to end it there or else I'll be facing impeachment by my colleagues.

[*Technical difficulty—Editor*]

The Chair: Oh, it's nice to hear some music.

We're having a breach of our own security here.

● (1715)

Mr. Glen Motz: Chair, I'm voting for impeachment.

Some hon. members: Oh, oh!

The Chair: With that, we'll go to Madame Stubbs, for five minutes, please.

Mrs. Shannon Stubbs: Thanks, Chair. Your last question was actually extremely important.

I have questions on two topics, and if there's still time and you're amenable, I think my colleague Tako might have a question. I could split my time, if that's possible.

The Chair: Anything is possible.

Mrs. Shannon Stubbs: Okay, thanks, Chair.

Mr. Jones, you identified China, Russia, North Korea and Iran as threats to Canada. You probably know that recently Israeli and U.S. researchers found that China was rerouting Internet traffic through state-controlled services.

Would you comment, if you can, on whether you think that's espionage or theft of intellectual property, and what the purpose would be, and also whether CSE has acted or what action CSE has taken to stop China from rerouting Canadian Internet traffic?

Mr. Scott Jones: A bit of some of that might touch on some classified issues, but I can certainly talk about it and hope I answer your question fully.

There are a few things. Typically, what we're talking about here is that the way the Internet routes itself is that it works on what is the cheapest route, usually meaning fastest. You can pretend to be the cheapest route and fastest, which forces the Internet to direct across it. The technique for that is called “BGP hijacking”, but I won't go into all the techy grossness of it.

That's one of the things that we've been working on in partnership with telcos. I talked about innovation before, and we do look at ways to innovate and work with our telcos to detect this type of activity, and moreover, to ask what are the defensive ways we can do things to prevent this?

It isn't something that happens a lot, but it is something that can happen and it's something that we're looking for. We're looking for ways to mitigate and defend against it, but at the same time, though, not reduce the reliability of the Internet.

It is something where you're talking about big shifts, so it is a bit of a concern. Really, you're talking about being able to mass all the data that's going from one place to another, so encryption is a great defence against that.

With our apps, right now for example we are on an encrypted Zoom channel. You can't publicly just tap into this; you have to be able to sign in, and so on. There's encryption there. When I send a message over any of the messaging apps, and so on, that's encrypted.

Our websites are all encrypted now as well for the government, and hopefully, more and more commercial sites are fully encrypted. That immediately puts a barrier to actually using that information for anything, other than getting a whole bunch of encrypted data that you can't do anything with.

Those are some of the defences.

Mrs. Shannon Stubbs: Thank you.

Related to a topic we had touched on earlier, I note that our government's critical infrastructure strategy hasn't been updated since 2009. Therefore, relative to this potential ransomware targeting of large enterprises and critical infrastructure, I wonder whether you can expand with more specifics and more detail about the nature or depth of the relationships you have built with operators of critical infrastructure, those in the private sector, and whether there are established relationships with those in power to make decisions in those organizations in an official way.

Mr. Scott Jones: Absolutely. We started with the telecommunications sector, where we see from a cybersecurity perspective that they're the root of so much, but then we've expanded that into the energy sector, particularly concentrating on the electricity sector from coast to coast. So we do have partners that we're working with and have absolutely contacted the senior levels of those companies. We always look to grow those partnerships. I just described the work we did with the telecommunications companies. We're looking at doing something similar with the electricity companies—co-development, where they invest with us on how to combat this—to address some of the threats they're facing in research development. One of the criteria is that as we learn things, it has to be shared with everybody in the sector.

If we work with one specific company, we are very conscious never to create a competitive advantage for them. We want to make sure it's going to the whole sector. We're the government; our goal is to make sure that it's coast to coast to coast, and also shared openly so we can all benefit from it no matter where you are. There are bigger companies in Canada, and they have more resources. We've seen them step up. We've seen their senior executives step up. We work with them. I have fairly regular meetings with senior executives from the energy companies, for example, and also from the telcos, just to make sure that we're on track and are addressing the biggest threats. They have a very good understanding of risks. That's growing, but it still needs to grow.

To your point, critical infrastructure is large. There are a number of providers. It is very dispersed in Canada. We are looking for some leaders, but also for organizations like industry associations to bring all of their members to the table and represent them to us.

● (1720)

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

Who is the next Liberal questioner?

Madam Khera.

Ms. Kamal Khera: Thank you, Chair.

Thank you, Mr. Jones.

I represent the riding of Brampton West, and you may or may not know that back in 2019 we worked really closely with Ryerson University to be a partner to secure a cybersecure catalyst for them. Part of it was funded by the Canadian government as well, and it's a national centre for innovation and cybersecurity in Brampton. The catalyst drives collaboration to empower businesses and to look at the very things you're talking about—innovations, and to get them to tackle these issues.

Do you know about this centre and are there are any opportunities for partnership or collaboration with this catalyst?

Mr. Scott Jones: Absolutely, we know about them. It's always good to see any organization stand up. We have never claimed to have a monopoly on innovation or on addressing this problem. We try to come humbly to the table with our knowledge, knowing that others have expertise and will come at the problem from a different perspective.

There's always opportunity. We are trying to put out some of our challenges. We've done them through research challenges. CSE has published them. We worked with the NRC to publish some of our research challenges for the more research type of pieces than the development pieces. Then we also have events where and hosted something called GeekWeek in October. Organizations can come and apply. It was virtual this year, of course. Normally it's in person. Over 200 cybersecurity professionals from Canada, academia, industry, government and international come together to start to tackle those problems together. That would be another area where we could contribute and collaborate on research projects.

Finally, we're always open to good ideas. I have a partnership group that looks for places that we can work with together on things like collaborative cyber defence. We're always looking for great ideas and hearing what people have to say.

Ms. Kamal Khera: That's great. Thank you for that.

Perhaps you can talk a little about the fact that your agency is relatively new, having come into force in 2018. Can you perhaps talk a little about what the approach was to addressing and raising awareness of cyber-threats before 2018? Where were some of the limitations and the successes of this approach in working to prevent and address cyber-attacks?

Mr. Scott Jones: This is going to come across as a little bragging. These organizations all existed. Public Safety Canada, for example, had the Get Cyber Safe campaign ahead of time. At CSE we've had the IT security branch since the late forties or early fifties, primarily based on cryptography but growing into cybersecurity. Then, of course, Shared Services Canada had security operations. We brought all of those together, because we needed to start addressing this whole-of-economy thing.

In terms of what we've done, there's really been a collaborative approach with industry and partnerships. It's not, “We're the federal government and we're here to help.” Rather, it's, “We're the federal government and we want to work with you. You have knowledge and expertise as well.”

The second thing is that we've tried to make our advice and guidance practical. All our guidance, not only for small and medium-sized enterprises, is being rewritten to say, realistically, what should be done by a normal Canadian, not a computer scientist with a Ph.D. We wrote our advice and guidance to be almost inaccessible, and it's now accessible. I'm just really pleased to hear all the comments on the report. I really appreciate the feedback that it is accessible. It was written for every one of us to be able to read.

Third, we have done a lot on collaborative cyber defence, working with industry partners to say that we can solve this problem together. We bring certain expertise to the table. The Government of Canada has very good defences in place that we've built over the last decade. How can we apply those lessons learned? Canadian Shield is an example of that with the Canadian Internet Registration Authority. We do things with our telecommunications companies, critical infrastructures providers and of course the provinces and territories. That's an area where we're still developing our relationships, but we've certainly seen various provinces come to the table and say that we should work together. I can't think of a province or a territory where we don't have some ongoing relationship right now. One of the goals is to make sure there is a pan-Canadian approach.

● (1725)

Ms. Kamal Khera: Thank you for that.

Do I have any more time, Mr. Chair?

The Chair: You have 30 seconds.

Ms. Kamal Khera: I'll give that to my friend Ms. Damoff.

Ms. Pam Damoff: Thanks, Kamal.

My question is really simple: Is the COVID app safe, yes or no?

Mr. Scott Jones: Yes.

Ms. Pam Damoff: All right.

The Chair: You still have 15 seconds.

Ms. Pam Damoff: Thank you, Chair.

The Chair: Madame Michaud.

[*Translation*]

Ms. Michaud, you have two and a half minutes.

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

I'll conclude with a less simple question. I'll leave you plenty of time to answer it.

If, at this time, the government isn't taking specific action to address the cyber threat to protect citizens, businesses and government infrastructure, do you think this could pose a danger to our democracy? What measures should be taken?

There seems to be some shared responsibility between individuals and companies, but that responsibility is also shared by public authorities. I'd like to hear your thoughts on that.

What are your expectations regarding the publication of this report?

You are a fairly new organization. Are there any specific steps that should be taken?

[*English*]

Mr. Scott Jones: I think there are a few things. We are taking quite a bit of action to try to raise that bar on cybersecurity, some them very public and some of them private. We are doing things. We have things that we call “strategic mitigation plans”, which directly address the threats mentioned in the report, one on cybercrime and one on protecting critical infrastructure. “Defending democracy” was the first one. Beyond that is the operations plan and then actual operations, which could involve defensive cyber operations to protect and take action, if we need to. That's really leveraging the mandate that Parliament has given us as part of the CSE Act and making sure we are doing it in a holistic way.

The second piece for us, though, is to make sure we're also getting practical information out to folks and working with them so that they can take action on their own. That's what the report was about, to say that these are the threats we're facing. If Canadians read the report, which I hope they do—I'd be thrilled—they can take some of those basic actions. They can follow Get Cyber Safe. Small and medium-sized organizations can read our advice and guidance on small and medium-sized organizations and look at whether or not they're addressing their cyber risks. Then that goes to CyberSecure Canada, a program that Innovation, Science and Economic Development Canada launched. It's something they can leverage to say, “Hey, I've done these things. I have a cybersecurity checkmark.” That's something I would like to see us use as a bit of a measure for Canadian companies, as a bit of a competitive advantage. They have this checkmark. They've done this.

Those are things that could be done directly from the report: Understand the threat, know where you're at risk, and then take action to reduce that. We have a lot of information out there that hopefully empowers Canadians to make those choices.

The Chair: Sort of like an ISO marking for a company, is that what you have in mind?

Mr. Scott Jones: It's a program that's in place now. It can be looked at that way, but at a rate that is affordable for a small or medium-sized organization to attain. The ISO standards tend to be unaffordable for other than the largest organizations.

The Chair: Okay.

Mr. Harris. for two and half minutes.

Mr. Jack Harris: Thank you.

So it's more like an organic gardening check mark.

Voices: Oh, oh!

Mr. Jack Harris: Mr. Jones, I have a question that comes from a recommendation of this committee in 2019 when it looked cybersecurity in the financial sector as a national security issue.

The recommendation number nine says:

> The Committee recommends that the Government of Canada explore ways to ensure all sensitive data moved within Canada has a domestically routed path, ensuring data packets are not exposed to foreign network infrastructure.

My question really is what has Canada done to act on that recommendation in the last year or so? You did mention encryption as one protection. Are there other things that Canada should be doing?

I'm thinking of this in the context of the recent sale of a company in my riding called Verafin for a whopping $2.75 billion to Nasdaq Inc. They look after the FINTRAC tracking of banks' and financial institutions' obligations.

In that context, how do we have sensitive data with a domestically routed route in order not to expose it to foreign network infrastructure?

● (1730)

Mr. Scott Jones: That's actually an issue that's near and dear to my heart. One of the things that we face in Canadian telecommunications infrastructure—and some more detail could probably be provided by colleagues at Innovation, Science, and Economic Development—is that our infrastructure tends to run north-south because of the way the Internet and the way the interconnections happen. We tend to connect to our American neighbours quite extensively, whereas the east to west connections are quite thin. That is something where we have seen some investment.

The capacity to simply route across Canada might not be there. That's something that they would be better positioned to face. We really say, how do we protect this no matter where it routes?

One of the fundamental things about the Internet is that I could be sending you an email right now and it could go all the way around the world to get to you in your riding. It doesn't necessarily stay within Canada, just because of the way the Internet works. It routes anywhere. We also say that you need to take protections. Encryption is the best protection for that. It does prevent that compromise of confidentiality.

In reality there are some things around the Internet infrastructure that certainly would make cybersecurity better from not only a sovereignty perspective but also from a reliability perspective, and this would be something that we would be interested in seeing. There is a tremendous amount of investment from the private sector required. Innovation, Science and Economic Development would probably be better positioned to answer that question.

The Chair: Thank you, Mr. Harris.

We are technically past 5:30, but we are not being pressed by anybody. I had thought we had two questions still to go, one Liberal and one Conservative.

Do you want us to go past 5:30 or do you want to end it there?

Ms. Pam Damoff: I think we can end, Chair.

The Chair: Okay.

Mr. Jones, on behalf of the committee I'm going to thank you. Your response in your report is done in an accessible way, which I think is 90% of the ball game, just to be able to explain how vulnerable we are both on a personal level and also as a nation, given all of the threats that appear in that regard.

Your security analysis has been very helpful to us. We appreciate your coming. I anticipate that we will be inviting you back.

With that, thank you, colleagues as well.

Just before I bring the gavel down, we have no indication from anybody at this point as to whether we will be able to meet next week. Stay tuned.

Thanks again.

The meeting is adjourned.

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

SPEAKER’S PERMISSION

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

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

PERMISSION DU PRÉSIDENT

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