House of Commons
Chambre des communes
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 125 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, September 20, 2018

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Thursday, September 20, 2018

● (1635)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Ladies and gentlemen, our witnesses are here. Let's reconvene.

I believe our witnesses are experienced in the ways and wonders of parliamentary committees, so I'll just say welcome to Scott and Rajiv. We'll try to be as informal as possible, but it is what it is.

Whoever is going to lead off may do so.

Mr. Scott Jones (Deputy Chief, Information Technology Security, Communications Security Establishment): Good afternoon, Mr. Chair and members of the committee.

My name is Scott Jones. It's a pleasure to be back again. I'm the deputy chief of IT security at the Communications Security Establishment and the head-designate of the soon-to-be established Canadian centre for cybersecurity.

I am joined today by Rajiv Gupta, the director of standards architecture and risk mitigation. Thank you for inviting us to discuss this very important topic.

[*Translation*]

The Communications Security Establishment is the lead technical and operational agency for cyber security in the Government of Canada. We are mandated to protect information and information infrastructures of importance to the Government of Canada.

This expertise in protecting and providing information is over 70 years in the making. The protection of government communications has been a part of CSE's mission since it was first established in 1946 as the Communications Branch of the National Research Council.

[*English*]

It goes without saying that the world of 1946 was much different from the world of today. What has not changed, however, is the need for innovative and skilled leadership to meet the challenges of an evolving world.

Canada's new national cybersecurity strategy, announced in June of 2018, recognizes this and sets out Canada's vision for security and prosperity in the digital age. Among the new measures in this strategy is the creation of the Canadian centre for cybersecurity, to be housed at the Communications Security Establishment.

Combined with the investments made in budget 2018, these efforts will enable us to remain resilient against cyber-threats and to continue to protect the safety and security of Canadians—and there's a great deal worth protecting.

[*Translation*]

Recent innovations in technology have created incredible opportunities for economic growth in Canada. The benefits of an increasingly digital society are many and should not be understated.

The Internet has brought enormous benefits to the lives of Canadians. Many federal government services are online. Budget 2018's investments in strengthening digital services demonstrate that the government is embracing new and innovative technology.

But of course, Canadians can only reap the benefits of online commerce when they can conduct their online activities with confidence and trust. These risks should not dissuade us from adopting new technologies, but they should be acknowledged and mitigated.

[*English*]

Unfortunately, we have all seen how cyber-compromises can result in significant financial loss, the loss of intellectual property and reputational damage to a company, an individual, or a government. For example, recent cases involving ransomware demonstrate the increasing threat of cybercrime and the effects of a cyber-compromise.

Today's cyber-threat actors have a variety of motivations and capabilities. They include state actors, hacktivists, criminals and terrorists capable of a broad range of disruption, from denial of service attacks to the exposure of personal information.

CSE plays an important role in stopping threat actors from achieving their goals. Our expertise helps identify, prepare for, and defend against the most severe and persistent threats to Canada's systems and networks.

[*Translation*]

There are three keys to success: partnerships, appropriate authorities and talent.

Let's begin with partnerships.

Cyber security is everyone's business. Our relationships with industry are critical to defending Canada and Canadians from cyber threats.

Equally important are our relationships with other government departments, including Public Safety Canada, Shared Services Canada, the RCMP and the Canadian Security Intelligence Service.

Beyond the government and the private sector, CSE's partnerships also extend to academia and leading-edge research groups.

● (1640)

[*English*]

The Canadian centre for cybersecurity will greatly improve our ability to work with industry, other government departments, other government partners and academia. The cyber centre will consolidate the key cybersecurity operational units of the Government of Canada under a single roof. In doing so, the cyber centre will establish a unified source of expert advice, guidance, services and support on cybersecurity operational matters, providing Canadians with a clear and trusted place to turn for cybersecurity advice.

An important part of this is ensuring continuity in the functions of the Canadian Cyber Incident Response Centre—also known as CCIRC—at Public Safety, once it becomes part of the cyber centre. Specifically, a crucial element of CCIRC's work is the notification of victims in the event of a cyber-compromise. This is an important role and one that will need to continue under the cyber centre.

[*Translation*]

Second, I would like to talk about CSE's authorities.

As you all know from debates on Bill C-59, under the proposed legislation, CSE would retain its current cyber security and information assurance mandate and would be given a new authority to defend important networks outside the Government of Canada.

The proposed Communications Security Establishment Act would also explicitly allow CSE to share cyber threat information with owners of systems outside the Government of Canada, so they can better protect their networks and information. For example, CSE could more extensively share information about specific cyber threats with the owners of critical infrastructure such as communications companies or the banking sector.

[*English*]

Finally, the CSE act would give CSE the ability to take action online to defend important Canadian networks and proactively deter cyber-threats before they reach important Canadian systems. These new authorities will better protect Canadians' most sensitive information and important cyber-networks from compromise and strengthen Canada's cyber-defences.

Third, and most key for me, is people. Among the new measures introduced as part of the national cybersecurity strategy is funding to develop Canadian cyber-talent. We are fortunate at CSE to have incredibly bright and talented Canadians working to address these tough cyber-challenges. However, to continue the success, we need to build on this talent and harness the tremendous brain power in the cyber field that exists here in Canada.

[*Translation*]

With strong partnerships, appropriate authorities and skilled people, CSE is working to address cyber threats facing Canada. However, cyber security is everyone's responsibility, and it will take all of our expertise and innovation to remain resilient.

Thank you for your invitation. We look forward to answering your questions.

[*English*]

The Chair: Thank you, Mr. Jones.

[*Translation*]

Mr. Picard, you have seven minutes.

Mr. Michel Picard (Montarville, Lib.): Thank you, Mr. Chair.

My question will be more general, so that you can provide us with a more detailed answer.

The creation of this new centre is occurring at a time when you have clearly established the risk level we are facing in cyber security, taking into account all the threats. So that new centre is being created to address a well-established problem by dealing with specific and constantly evolving threats.

On its first day, what expertise and quality tools will that centre have to deal with the current reality? As the threats it will have to face already exist, will the centre be somewhat behind? What will be its short-term goals, and what will you need to achieve them?

Mr. Scott Jones: Thank you for your question.

The first step is to establish the centre. As you said, that is something of a bureaucratic job.

● (1645)

[*English*]

What I think the key aspects of the cyber centre are going to be are building the trust and credibility to work with the private sector. We need to be very vocal about increasing all of our expectations—the private sector, the government—as we look at the security challenges we all face and start to have some of the more open discussions about the threats. All too often we concentrate on the threat after and not on the threat activity and how to raise that bar.

The first thing is increasing resilience. Canadian resilience, in general, is low. We don't talk about doing the simple things, and we're looking at defending against the most sophisticated threat. In reality, a few simple things can raise that bar for all of us and make us more immune and more resilient against basic things like cybercrime, so it's something as simple as patching our systems. Getting the message out, getting simple, straightforward advice that every Canadian can take and use is one of the first goals.

The second one is obviously establishing a centre where, if there is an incident, we are able to manage. We have done a number of exercises over the summertime to make sure we're ready to manage any incident, be it large or small, international in scope or national in scope, within the federal government or in the private sector, to make sure that we are ready to do our part so that on day one we'll be able to provide the federal lead, working with either the victim or other jurisdictions to make sure we're ready to manage an incident.

I think those are the two key things.

Mr. Michel Picard: You just mentioned patching. Is patching a system a temporary approach to the solution that you're looking at, or is it a permanent way to work, considering the system we have, instead of rethinking the system we use?

Mr. Scott Jones: Right now, with the environment we have, patching is one of the key aspects of improving our cybersecurity. Companies are releasing patches. The model in the industry is “release fast and patch what doesn't work”. The same goes for security elements as well. As they discover new things and new ways of compromising systems, vendors put out software updates. It's important that we apply those very quickly and diligently on our systems.

Mr. Michel Picard: It's been mentioned that we will allow offensive tactics in order to better protect our system.

From a diplomatic standpoint, how do you see the impact of engaging in an offensive attack instead of taking a defensive approach? We had this conversation with I don't remember what commissioner. I asked if he considered any offensive attack as an act of war.

Mr. Scott Jones: I think the key thing is that defensive cyber-operations are proposed in Bill C-59. It's a tool we can use to respond against any malicious cyber-activity.

There are a number of elements. The first one is the permission to undertake that activity. It's up to the Minister of National Defence, with consultation of the Minister of Foreign Affairs, to ensure that if there are any foreign relations aspects, they are taken into account.

But this wouldn't be the first measure, if you were taking a defensive action. You would want to increase your network defences. You would want to try to increase your resiliency against the activity. This type of activity is something that, if there were no other option, you would turn to as things escalated.

There are a number of other things we would look to do. If the activity were originating from a foreign actor, we would engage our international CCIRC community. The Canadian Cyber Incident Response Centre has relationships around the world with national computer emergency response teams to respond. We could ask them for help. We would certainly look for law enforcement, if that were a better option.

Mr. Michel Picard: This week we received Norway's justice committee. One of their concerns was the lack of expertise, of capacity to answer the threats we have.

How do you evaluate the actual expertise that is able to work with the situation from day one? How do you address the need for more and/or better expertise?

The Chair: Keep the response very brief, please.

Mr. Scott Jones: The expertise is an area in which we have to do two things.

In the short term we have to look outside of the traditional fields of computer science and engineering. There are other skills to be brought to bear here. There are skills that are very close to the cybersecurity analytic capabilities.

In the long term, it's about looking to build a coalition from universities and colleges, attracting more people into the field. We still have under-representation of women in science, technology, engineering and math. There is a large untapped market.

Enrolment in these fields is down in universities, yet a tremendous number of jobs are being created. How do we attract people into this field? It's one of the tertiary goals, but certainly I would like to see enrolment up and more people participating, in the long term.

● (1650)

The Chair: Thank you, Mr. Picard.

Mr. Motz, take seven minutes, please.

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

Thank for being here today.

Our Five Eyes allies, for example, have come out against Huawei, and I guess many people are wondering why Canada would not. As we know, their operating within Canada could obviously create some breaches in privacy that could impact our Five Eyes network.

Do we as a country, or does your establishment, have an obligation to follow suit with our allies when it comes to cyber?

Mr. Scott Jones: I think it's important, as we look at our telecommunications networks, that we take the approach that we really want to look at this as an entire system and defend against all forms of cyber-risk. We look at it really from a few different viewpoints. Number one would be how we make sure that we're increasing the resilience across, regardless of where the product comes from. We want to build in security measures no matter what.

How do you make sure the supply chain is adequately protected, for example, making sure that you are bringing in products that have good security practices, which are built in as they are building the product? How do you use the technology in a way that is secure? You could take a very secure product, for example, but if you open it up to the world, you can unsecure our technology very quickly.

We have a very well-established relationship with all of the telecommunications providers in Canada. I think it's important to work on raising the resiliency bar regardless of the vendor, regardless of where the equipment is coming from, and to work collaboratively to try to make sure that this happens. It's really trying to address all of the risks and not just one specific one.

Mr. Glen Motz: Thank you for that.

We heard from the experts in our first hour. I want to ask the question that I think was brought up by them. It would be good to get your perspective on it.

How does CSE balance the tension, the relationship tension, between defensive tactics and offensive tactics when it comes to our cybersecurity program and its impact on our infrastructure or any aspect of our Canadian practice and program?

Mr. Scott Jones: We talk about it. We make the decision is in the best interests of Canadian security. We look at the holistic piece. We want to make sure that Canada has secure, resilient networks that are able to operate in a way that provides confidence for our networks. At the same time, we realize that there are the tools that are needed for intelligence gathering and that there are the techniques that are required. We do have to strike a balance between understanding both sides of those coins.

At the end of the day, though, our system is designed to.... We will default to defence, meaning protecting Canada and making the decision. In reality, the decisions are much more clear-cut than that. We very rarely get something close to the edge. The decisions are very evident. If it's Canadian security, meaning releasing things for defence for purposes—protecting cybersecurity, updates, etc.—we're going to do that.

If it's something that lets us protect Canada from counterterrorism and gain proper foreign intelligence, we're going to make that decision, but we always know that, no matter what, it's going to be reviewed. We're going to respond to, right now, the CSE commissioner and, at the end of the day, the court of public opinion, if we make the wrong decision. We take in a number of factors that way.

Mr. Glen Motz: We heard from the Bill C-59 conversations that it's like a hockey analogy, in that it depends on the coach. They say that a good defence is a strong offence. I'm intrigued by how we always defer or default to a defensive posture when actually that defensive posture may be an offensive posture.

Mr. Scott Jones: The analogy extends to a point. Then, I think, the issue really is that if we're talking about something that's a systemic vulnerability, then we default to defence, but protecting Canada through the foreign intelligence side of things is something that we obviously care deeply about. We want to make sure that we have the intelligence we need.

● (1655)

Mr. Glen Motz: As we've seen in the election in the U.S.—it was brought up in the first hour—we are always susceptible to disinformation and misinformation from foreign actors. In our own election that's coming up within a year, how in particular do we protect ourselves from that aspect and still maintain our freedom of speech?

Mr. Scott Jones: Part of it, I think, is actually having these conversations and talking about it. It's the fact that it's now in the consciousness. It's something that we can now talk about and, as consumers of information, we can start to become connoisseurs, consumers of information who are a little more judgmental, who are not just believing what we're seeing in social media.

I think the second piece is about asking questions or looking for multiple sources. I might be putting a bit too much credit in our consumption of social media. I think the other thing is that our report that we published last year on the threat to Canada's democratic process was a little piece of that in terms of trying to start the conversation.

At the end of the day, it's about our literacy, our civic literacy in what's going on, but also, can we start to talk about this and not believe everything we see?

Mr. Glen Motz: I have two very quick questions.

For the first question, it's basically a yes or a no. Does our social media data sharing require regulation? That's one aspect of it. The other piece is what you mentioned in your presentation. How do we do this for small businesses that don't think of cybersecurity because they have a million other things to do? They're small. They have maybe 100 employees. Whatever the size is, it doesn't matter. How do we get them thinking differently than how they're thinking now?

I know. Those are two different questions. I'm trying to get them both in, with the chair's indulgence.

The Chair: The chair is not going to be very indulgent, because you only have 30 seconds.

Mr. Scott Jones: On the social media regulation piece, I'm probably not the right person. I haven't really assessed that.

On the small and medium enterprise piece, part of it is that we have to raise the general resiliency bar. I think it's unreasonable to expect them to be able to launch a cyber-defence initiative like, for example, the one we run for the Government of Canada. That's unaffordable for every small and medium enterprise.

How do we raise the tide? How do we raise the general cybersecurity in the industry that they can then take advantage of? Second, how do we partner with the larger service providers, the people who provide this, for something that small and medium enterprises can consume? I think the third piece is going to be that the insurance industry has a remarkable ability to nudge small and medium enterprises, and I think that is coupled with the small and medium enterprise program that's been announced as part of the cybersecurity strategy.

I think those can all help, but at the end of the day, we have to place a value on it.

The Chair: Thank you, Mr. Motz.

Mr. Dubé, please, for seven minutes.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you very much, Chair, and thanks to both of you for being here.

I want to ask a couple of questions related to some of the issues around transparency.

First, because the topic on everyone's mind, for both good and bad reasons, is elections, are there any protocols in place for how you divulge a potential vulnerability, infiltration or attempt to influence once the writ has dropped? In other words, if we're in the middle of a campaign—I've heard it referred to as the James Comey dilemma—how do you make sure that Canadians are aware that there's an attempt being made to interfere in an election but at the same time not break that news and then yourself influence the election in that way?

Mr. Scott Jones: That really goes to the general caretaker convention status but also to working with Elections Canada. This is something that we are talking to them about, because at the end of the day the nightmare scenario for a public servant would be to ever do anything that would interfere in the election. I can't overstate how much of a nightmare scenario that is for me right now.

Some hon. members: Oh, oh!

Mr. Scott Jones: That's something that we are talking about with Elections Canada, to make sure we respect that, and also for the Commissioner of Canada Elections, to make sure that we respect the independence. That might be the better route. That is something we're discussing right now in terms of how we're going to approach this.

It's a bit of a new world. Normally what we tend to do in the public service is that we kind of turtle. We retreat into the public service and we just do the normal things. Cyber has changed that.

Mr. Matthew Dubé: There are no existing guidelines on how to proceed in the event of that type of event occurring during a campaign.

Mr. Scott Jones: We're working through the scenarios now.

Mr. Matthew Dubé: Okay. Does Elections Canada have the expertise on their end to handle that kind of problem or do they really rely solely on you?

Mr. Scott Jones: We've been working collaboratively with Elections Canada since before the last election in 2015 in terms of augmenting cybersecurity and starting to discuss these issues. I think we're working through this as we also figure out how to engage with political parties if we find something. How do we share the information that we see if a particular political party is being targeted for activity? I think it's part of working out that protocol.

● (1700)

Mr. Matthew Dubé: There are Shared Services and then Public Safety, but Elections Canada is absent from this centre. Was there no thought of having some part of Elections Canada being part of the centre for any role that they might have to play?

Mr. Scott Jones: I think we look to liaise with them, but we're respecting their independence. Being outside of the government and more of a parliamentary agent, we look to partner with them and really follow a strict protocol and respect that.

Mr. Matthew Dubé: The other piece I want to ask about is the vulnerabilities equities process that exists within the NSA in the U.S. On the same topic of transparency, I'm wondering about this. More and more, especially with the existence of the centre, I'm assuming that there's going to be more work done to identify these vulnerabilities.

In Bill C-59, a lot of the pieces involve working with the private sector to identify the vulnerabilities and to, in some cases, even study them to a certain extent. I don't want to rehash the debate that we've had quite extensively at this committee, but is there a specific protocol that exists here, in the same way that the NSA has developed one, in order to disclose to the public and parliamentarians, etc., the existence of vulnerabilities in software and such?

Mr. Scott Jones: We absolutely have a process for that. Our standard process is that we work with the company to try to do it in a responsible way and to not create a vulnerability that somebody could then exploit. Every company takes time to prepare software patches, etc. We want to make sure that they're able to have those patches in place before any public disclosure so we don't get the cybercriminals or any actors that—

Mr. Matthew Dubé: Without getting into the details of a specific vulnerability, is the process and how it happens public?

Mr. Scott Jones: Not yet. It's something that we've been talking about—how do we share that?

Mr. Matthew Dubé: Okay. I would ask that you endeavour to do better than the last response I got, which referred me to Twitter. The last time I had CSE here they were saying, “We tweet now”, so I just hope for something a little more robust along the lines of the NSA. I can't believe I'm giving the NSA credit, but on this they deserve some, so if you could follow that example it would be greatly appreciated.

I had another question relating to private infrastructure, notwithstanding that I feel this has become a dirty word. It's interesting that in any of these issues related to specific companies, and for some of the concerns, whether it's around Huawei or others, when it comes to private infrastructure, obviously you're talking about liaising with private enterprise. You can look at private electrical grids or you can talk about a private clinic with regard to health information or something along those lines.

What's done there when there's a private infrastructure that might be foreign-owned or not clearly defined as Canadian-owned and there's a little more of that grey zone? How do you operate in that particular kind of context, especially with spectrum and things like that for telecommunications?

Mr. Scott Jones: We're always looking to provide advice and guidance in terms of just helping to raise the bar initially so that it's more secure. When you're looking at infrastructure, regardless of ownership, if it's Canadian infrastructure, in Canada, we would treat it as Canadian in terms of our work with them. If they were suffering an incident, we would certainly encourage them to report to the Canadian centre for cybersecurity so that we could try to help. At the same time, it's always a business choice in terms of what technology they use, how they implement it, and the need to balance factors—cybersecurity but also affordability and other factors.

Really, it's a combination of a few things. It's advice and guidance and helping to make it more secure. We're trying to publish more and more practical advice and guides. I'd say that in the past, some of our things were—

Mr. Matthew Dubé: I don't mean to interrupt, but my time is wrapping up.

When national security assessments are done when there are foreign takeovers of companies, I assume there's a larger cyber component in this day and age. We've often talked about natural resources in the last 10 to 15 years. Is that something you folks will be involved with in the future, going forward, when those assessments are made by the Minister of Innovation, Science and Economic Development, ISED?

Mr. Scott Jones: We're designated as part of the Investment Canada Act process. We provide advice to, in this case, the Minister of Public Safety, who then works with the Minister of Innovation, Science and Economic Development.

In terms of the Canadian companies, though, we're also looking to see how we can increase their resiliency so that they're able to defend against these types of cyber-activities. That's part of this as well. But it certainly is a consideration.

Mr. Matthew Dubé: Thank you.

● (1705)

The Chair: Thank you, Mr. Dubé.

Ms. Damoff, you have seven minutes.

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

Thank you both for being here.

Mr. Motz and Mr. Dubé both touched on Huawei. My question is maybe a little bit broader. It's about the risks posed by some of the concerns that have been expressed about that company but also the telecom industry in general and the risks we face with that. Is that something this committee could look at in terms of a study? Would that be worthwhile?

Mr. Scott Jones: The key thing for us, when we talk about suppliers, is that almost everything is manufactured around the globe. Where the final product is assembled doesn't necessarily equate to where, say, the software is written, etc. We work in a global market. That's one thing we really look at: How do we bring security into something where the product of origin, or the company that provides it, is only providing a small piece of what's actually embedded in the product?

On the telecommunications company side, it's difficult for us, because we do work under.... They provide a lot of information so that we can work very proactively in terms of what's coming in the future, so it's competitive information for them. At the same time, I've seen them make substantial investments in cybersecurity without requiring fanfare or government intervention, etc. I think they're taking security very seriously. I'm really proud of the relationship. I think we have found a good Canadian model for working between government and industry on trying to address some of the cybersecurity challenges, not from a very narrow national security threat but broader. How do we make sure we're building a very resilient telecommunications network that spans from coast to coast to coast? That's something we've really been working on.

It is a complicated issue. With cybersecurity, unfortunately, as we were saying, it's really hard to characterize this in 240 characters. That's one of the biggest challenges in the telecommunications sector. It is very complicated and it is broad.

Ms. Pam Damoff: The other one I want to ask about, which has come up a few times, is elections and the spreading of misinformation. You stated that you think the public has become more cognizant. I'll say that's true to a certain extent, except that there's still the ability to share misinformation broadly on social media. It can be placed there. I have a concern in particular with the fake accounts that have popped up over the summer. It appears to be a government official, it gets shared 5,000 times, but it's actually a fake account.

Those kinds of things are really troubling, because you have misinformation that is still being shared. I've had people come into my office, as I think probably all of us have, to talk about something they read. When I tell them that it's just not true and ask them where they got it from, they say they heard it from a friend who read it on social media.

How are you dealing with that when it's coming from another country, or even internally?

Mr. Scott Jones: In terms of directly dealing with it, that's one of the challenges we have with an open democracy that encourages communication. We simply don't monitor for that type of thing. We don't direct our activities at Canadians, and on the Internet it's hard to tell Canadians from everybody else.

I think the key thing is that the social media platforms themselves are trying to address this. One of the things is that certainly, for example, if I saw somebody trying to impersonate me—I don't know why they would, but if they did—I would certainly take advantage of the reporting tools they have. They have tried to address this, so it's been somewhat in public.

Ms. Pam Damoff: I'm just going to stop you there for a second, though, because we had Twitter come to the status of women committee, and we were talking about exactly that, and reporting. Twitter told us that Google had the same number of employees just in Ireland that they did worldwide, and they simply couldn't deal with it.

There is a bit of problem there when the social media—in particular Twitter, because I think Facebook has probably done a better job of addressing some of the things they've faced—just doesn't have the staff. They can report things, but they just don't deal with them, so it's an issue. That's an issue from a public safety standpoint, in terms of elections, if the private company is not dealing with that issue.

Mr. Scott Jones: The challenge we face is that, for us, it's very explicit. We don't direct our activities at Canadians.

When you're dealing with social media fake accounts or parody accounts—which is another thing we've seen this summer, for example—and looking at where the line between a fake account and a parody account is, the challenge we have is that those are simply not within our mandate to try to tackle. We try to increase the basic cyber-resiliency of these systems, but I think the use of social media and the constraints we would like to place on that is probably something better left to departments like the Department of Canadian Heritage, which would look at digital media and online interaction.

On the security intelligence side we would be looking for the foreign threat actors, certainly, to see if they are taking advantage of that, so we would take action. We are looking at the foreign activity that would be targeting Canada, but looking at the accounts themselves, etc., especially when you start to cross into a domestic context, would just be outside of the mandate of CSE.

● (1710)

Ms. Pam Damoff: How do you know a foreign country isn't interfering in that social media?

Mr. Scott Jones: It's a challenge in terms of how we as the government respond. We would look at our law enforcement agencies, whether the RCMP or the Canadian Security Intelligence Service and where they have domestic authority, possibly but also at how to deal with this in a more general way. Also, unfortunately, with one person, we do have this kind of model of echo chambers in which people will create the appearance of real information.

We are trying to enhance people's knowledge of what's going on and trying to draw attention to pieces of it, but at the end of the day, it is outside of our mandate to start dealing with the fake accounts themselves.

The Chair: Mr. Paul-Hus, you have five minutes.

Go ahead, please.

[*Translation*]

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): Thank you, Mr. Chair.

I thank the witnesses for being here.

Recently, Five Eyes initiated proceedings against Huawei. I would like to know why Canada did not follow suit.

[*English*]

Mr. Scott Jones: When we look at this from a Canadian perspective, it's hard for me to comment on some of the internal decisions. We don't always see the internal government debates of our Five Eyes partners, but from our perspective, we've really been trying to focus on addressing the broad cybersecurity challenges in the telecommunications space. We think we have a really effective program in terms of how we deal with the cybersecurity risks that we're facing as a country, such as the vulnerabilities that are inherent in every single telecommunications product and how we start to mitigate those.

Do you want to maybe add a few things?

Mr. Rajiv Gupta (Director, Standards Architecture and Risk Mitigation, Communications Security Establishment): Yes.

As Scott said, in Canada we take a risk-based approach, so we look at the same set of risks. We assess them within Canada. We assess our relationship with telco operators and the type of influence we have there, and we work together to address it through a risk-based approach.

We've talked a little bit about the program we have had over the past years, and we still believe that's effective in terms of mitigating the risks. It's through evaluating that program that we actually determine whether we think this is a valid way forward.

[*Translation*]

Mr. Pierre Paul-Hus: Don't you think that allowing that company to do business in Canada may undermine trust within Five Eyes? Couldn't the fact that the four other member countries are unanimous in their decision, but we are deciding to keep that company, make us lose our partners' trust?

As we know, there is no written document defining that group. It is built on an agreement based on mutual trust. Could we end up losing our partners' trust?

[*English*]

Mr. Scott Jones: One of the things we've been working on sharing with our Five Eyes partners is making sure that they're aware of our program and approach, which is very comprehensive in terms of dealing with the full risks across the telecommunications spectrum. Also, there's a productive relationship that we've built with all of Canada's telecommunications providers in terms of sharing information, sharing risks and collaboratively building solutions to cybersecurity challenges. It's something not all countries enjoy and it is a very good Canadian strength. I'm quite proud of the work the team has done. We look at risks across all vendors, but all products as well, in terms of how we layer cybersecurity and make sure it's being addressed as a systemic issue.

At the end of the day, I believe we have very secure telecommunications networks because of these relationships, but it is a complicated aspect of this issue.

In the long term, we need to look at how we systemically increase our cyber-resiliency, regardless of where our product is coming from. It's a sustainable path for starting to really look at this.

● (1715)

[*Translation*]

Mr. Pierre Paul-Hus: As analysts have stated, Canada is reaping a number of benefits from the United States' presence, as that country provides it with a lot of information.

Is Canada's contribution proportional to its economic clout? Do the Americans feel that they are giving too much and not getting enough in return?

[*English*]

Mr. Scott Jones: I can't really speak on behalf of the Americans on this piece, but from our perspective, we have a very advanced relationship with our telecommunications providers. Certainly from what I've seen, it's something that is different from most other countries.

We have a program that's very deep in terms of working on increasing that broader resilience piece, especially as we're looking at the next generation of telecommunications networks, making sure that we're able to evolve that program and looking at ways to innovate in cybersecurity but also increase the base cybersecurity of every product that's purchased, regardless of where it comes from in the world.

I think that's one of the biggest challenges we have. It's not about one piece; it's about how we make the whole system resilient. The communications environment is very complex, and we need to address it as a whole system.

[*Translation*]

Mr. Pierre Paul-Hus: I have one last question. Do I have time for it?

[*English*]

The Chair: You have 20 seconds.

It's all right, Mr. Motz will pick it up for you.

Mr. Glen Motz: I will.

The Chair: Go ahead, Mr. Spengemann, for five minutes, please.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Thank you very much.

Gentlemen, thank you for being with us.

I want to go back to the paradigm that good cybersecurity means good economic security and economic competitiveness.

We're getting a lot of questions in our ridings from corporate stakeholders, even start-ups that are involved in big data. They're asking what Canada is doing.

You seem to indicate that the model we currently have is one that you're relatively happy with. Was that specific to telecoms, or is that broadly across sectors that are engaged in big data?

Mr. Scott Jones: We started with the telecommunications sector. That's the area we addressed immediately. We think we have a model that we can grow in terms of applicability to other sectors, especially in critical infrastructure. More broadly, though, we have to start addressing things such as digital policy, so there's some work going on in consultations on that. I think it's important that we start to.... Cybersecurity is one element of this, and it's something that we're looking to bolster, but I also think we need to get out more information about practical things so that small and medium-sized enterprises can do what those innovators need to do to protect their intellectual property from a cyber-breach. We need to try to grow that relationship side. It's about increasing the resiliency bar. The model we've taken for the cyber centre is “security through collaboration”.

We don't have all the expertise in certain fields. We bring expertise in threat, in cryptography, and we bring a lot of expertise in terms of how to mitigate. For example, if you're looking at the critical infrastructure in the energy sector, they bring expertise into their environment, and so we have to work together. In terms of addressing things like big data, we'd look to work with big data and ask what your biggest challenges are and how we would work on that and secure the data.

Mr. Sven Spengemann: Through an economic lens in terms of operating costs or even capital expenses, is there is still room to pool resources as Canadian companies in partnership with Canadian branches of government to achieve a common baseline of cybersecurity that we could all share and benefit from?

Mr. Scott Jones: I think that's absolutely one of the goals. For example, the Canadian Cyber Threat Exchange is an non-profit organization that was set up by Canadian companies. We're working with it, and in fact we'll be signing our agreement shortly with it to try to make sure that we're getting information out to all Canadian companies. It's a place to pool resources in a space where we don't need to compete. We shouldn't compete on making ourselves more secure, so how do we do that?

At the same time, we're also looking at how we can foster innovation. The cyber centre will enable companies to come together to work jointly on projects so we can start to innovate around security.

We're trying to create opportunities to bring these things together. We think that occasionally there will be problems that we might not have time to tackle or that might not be ours, but I'd be really happy if we were the matchmaker. It would be a "Here's a Canadian company that has a really good solution. Here's a Canadian company with a problem. You two might want to talk" type of thing.

Mr. Sven Spengemann: Okay. Thank you for that. That's helpful.

Are there other countries that you've looked at that are slightly more ahead of the curve than we are that the committee could look at in greater detail to potentially inform our study?

Mr. Scott Jones: Certainly I would compliment my colleagues in the United Kingdom for the creation of the National Cyber Security Centre—

Mr. Sven Spengemann: Right.

Mr. Scott Jones: —and the work they've been doing on tying that in with innovation. We certainly work very closely with them. They would be kind of first.

There are my colleagues in Australia as well. The Australian Cyber Security Centre has recently changed to a different model. The U.K. is a little bit further ahead, but those would be the two shining examples.

There are some good examples in the European space as well.

● (1720)

Mr. Sven Spengemann: I have a final question for the minute and a half that I have left.

In terms of the ability of the talent pool to move fluidly back and forth between the private and public sectors, you seem to suggest that there are categories or mandates that are not hampered by security classification so that people can actually move fairly freely. To what extent is that currently the case, and how can we grow that further to make sure that the talent pool really benefits both the public and private sectors?

Mr. Scott Jones: That's one of the goals of the cyber centre: to be more open and transparent. In fact, we're making sure that we have a facility where people can come in and work. If you come and visit CSE now, we take all of your technology away because you're entering a top secret building. The cyber centre will not be that way. The physical facility for this will be a place where people can come and collaborate and, frankly, bring their stuff so we can see how it works and we can work together on things.

Also, I think we do need to be more fluid. There are opportunities and there are things to learn by working in each other's spaces.

There are draws in the public sector—our mission, a little bit of altruism, etc.—and there are draws in the private sector in terms of some of the innovation, the profit, and things like that. It just depends on people.

Mr. Sven Spengemann: Potentially there are even secondments back and forth.

Mr. Scott Jones: I would love to see that. I think it would be very creative.

Mr. Sven Spengemann: Thank you, Mr. Chair.

The Chair: Colleagues, we have ten minutes' worth of questions and seven minutes of time.

I find this conversation fascinating, and we did start a little late, so my thought would be that we would go a little bit past 5:30 if that's all right with everybody. The analysts have a couple of questions as well, so I'd like to tag those on at the end. Is that all right?

It's all right. I have to ask the analysts' questions, so it's no panic here.

Mr. Eglinski, you have five minutes, please.

Mr. Jim Eglinski (Yellowhead, CPC): I have two questions, and they're kind of related.

Under Bill C-59, you've been given the authority to lead the cyber centre, and you talk about the other government agencies: Public Safety, Shared Services, the RCMP, Canadian Security Intelligence Service, the military.

Being a former policeman and having been involved in major crimes in larger communities, I know there are always conflicts, perhaps the bullheadness of one department over another department.

You've had some time since Bill C-59 came out, and we have been discussing it in the House and around. Are your agencies getting together already and working together? Do you see that this will be a fairly easy transition and a joint effort, or do you feel that there may be some stumbling blocks and pressure back and forth maybe because you've been given the lead?

Mr. Scott Jones: The cyber centre, when it stands up in about 10 days from now, will be relatively new. However, we have long-established relationships in terms of deconflicting. For example, cybercrime is the scourge of the Internet. We'd love to see law enforcement. I'd love to see some successful prosecutions so that we could start to create a disincentive for cybercriminals. With regard to our work with the cybercrime coordination unit that the RCMP will be setting up, for example, we're looking at making sure that we're in the same building so that we can be co-located.

We have a long-standing body that sits down with the Royal Canadian Mounted Police and the Canadian Security Intelligence Service just to make sure that we're deconflicting anything operationally and that we're assigning the appropriate lead. For example, in the case of a national security investigation, I want CSIS to be able to go out and do some work on that, but we'll support in the mitigation piece. We know how to remediate the threat. We know how to work with the company and we want to see successful prosecutions. We want people to report cybercrime.

We're working it out. I've been in this long enough to know that there'll be some hiccups and that there'll likely be a little bit of posturing, but we're trying this out.

Mr. Jim Eglinski: You led into my second question.

We have a number of accredited police forces across Canada that have cybersecurity departments and details. I imagine they work very closely with the RCMP, as you are. Do you foresee developing a program to work with the other police forces—city police in Vancouver, Edmonton and Calgary, let's say—that already have these departments set up?

Do you see anywhere that you may, as a federal agency, assist these police departments financially? A lot of them are municipal police departments that are actually doing work to protect Canada. Do you see a role whereby maybe you can financially assist or help or train these other departments across Canada?

● (1725)

Mr. Scott Jones: Certainly, we'd look to work with the RCMP on that to engage all law enforcement and to follow their lead on that.

In terms of financial contributions, it's not really within our authority or remit to do those types of things, but we do offer training. We run our IT security learning centre right now, where we do offer training. For example, I know that we've had a few provincial police forces come in for training programs, etc., in terms of IT security. I think we'd really look to leverage that relationship with the RCMP and things like the national police college and do what we can to try to support training in that environment.

Certainly this is something that we see as police forces. We need to be able to work together. Also, we need to know when to get out of the way and allow the police forces to do their important work without any tainting of the evidence, right? At the end of the day, I really encourage that.

Mr. Jim Eglinski: I'm not sure which one of you mentioned this earlier, but how do we ramp up the training of our Canadian people to give them the intelligence and the ability to work within your department and other departments? I want your opinion on that. How do we go about that? We need to go about it fairly quickly.

Mr. Scott Jones: In terms of training and helping...?

Mr. Jim Eglinski: Yes.

Mr. Scott Jones: I think there are a few things. It's in cyber-literacy. It's in demystifying IT. We've made it the domain only of experts, and yet we all use it every day. Most people are scared to actually touch it when it breaks, etc. It shouldn't be that hard. As an industry, we have to get better at that.

I think the second piece is that we need to draw people into the programs. The fact is that there isn't the enrolment. We went to one of the universities that was one of the biggest recruiters in 1999 for CSE. The computer science class is a quarter of what it was that year. That doesn't bode well for being able to recruit people into the cyber-field, regardless of whether it's in government or the private sector. I think those are the things that we really have to start concentrating on.

The Chair: Thank you, Mr. Eglinski.

Ms. Dabrusin, you have five minutes.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): A lot of the conversation we've had today has been about collaborating with the private sector. You've talked a few times about low resilience and building up resilience. On your website, one of the things I noticed is that just under a year ago you launched something called “Assemblyline”. As I understand it, it can be used by private users. In fact, could you quickly describe it so that I don't mess up the description?

Mr. Scott Jones: Sure. Assemblyline is the system we use when doing malware analysis. Let's say you're getting a malicious file. How do we break it down and basically do all the cyber-analysis? We automate it. That's how we scale for the government. It wasn't done by people; it was done by automating and taking advantage of some creative things. Also, we open-sourced that. We made the code freely available to the world.

Ms. Julie Dabrusin: From that experience of having made that available, what are the lessons learned about what worked or didn't work in launching it? You're about a year in now.

Mr. Scott Jones: In terms of what worked really well, it was aimed at cybersecurity professionals, people who do this for a living, and we did see pickup around the world for it. Also, people are contributing back in.

It is a lot of work to maintain an open-source project. When we release this, we have to continually invest in it managing the open-source software, etc.

I think that on the whole it's been very good for us, not just from a public perception point of view of us putting something out there, but in trying to add a tool into the cyber-community.

My goal would be to see more people contribute to it and make it better, and see where can we use it across Canadian.... We're starting to see pickup for that. Also, how do we now start to share some of the analytic components that ride on top of it?

Ms. Julie Dabrusin: Are there ever any concerns when people are using that about their private information being made available to you? There are those types of questions, and this seems to be one of things that comes up a lot when we talk about data and protecting data. It's the privacy of that data as well.

Mr. Scott Jones: We made the tool available. We didn't make our instance of the tool available. You can download the software, install the software on your system, and run it in your own environment to protect it. It's not connected in, so you don't use our instance of the tool, and we don't collect.... It's not a data collection platform or anything like that.

Ms. Julie Dabrusin: You mentioned at the beginning, when you were talking about building resilience, that there were some simple things we can do. You mentioned patches briefly, but what are the simple things we can do to build resilience?

● (1730)

Mr. Scott Jones: Patching is number one. It really is.

The second one, depending on what infrastructure you're using, is just not logging in as administrator, not logging in with super privileges, etc. That's a simple thing. It just slows things down.

There is also backing up your data. If you have something critical, make sure you're backing it up, because if ransomware hits, then all you do is restore and you get your data back, and things like that. I'm kind of making it a little simpler than it really is in practice, but these are some basic resiliency things that we'd really look at doing.

We've put out our top 10. Those are more oriented towards larger organizations, but I can translate those into personal actions. It's also knowing what's important to you and making sure you're protecting it, such as keeping backups. For me, I care about family photos and things like that. I honestly don't care about the email I'll never read again that I get on my personal email.

Ms. Julie Dabrusin: Those are pretty simple. What you just mentioned is really simple. For instance, you talk about low resilience and how you need to build resilience, and what you talked about there is quite basic. Then what's the gap that prevents getting that out there so that people are less likely to be victims of different types of cybercrimes, or the ones you've talked about, such as ransomware and the like?

Mr. Scott Jones: In some cases, it's inconvenient. It's inconvenient to update. It's inconvenient to run the patches, etc. In other cases, people just don't see the need. They say, “It's working for me. It's good enough” or “I'm afraid I'll break it.” That's kind of an unfortunate legacy of our industry.

Right now, in some cases, it's the product itself. It's not updating itself frequently enough. When you buy into, let's say, a smart phone, you're buying into an ecosystem, so if it is the vendor who updates it, it could be a really cheap device that doesn't come with good support. Things like that all kind of factor into things. Sometimes it's manual, so some of the systems actually take a lot of manual effort to update versus some of the easier ones, for which, frankly, a little red bubble appears, and you just hit “Install” and you're good to go. It's kind of all of those factors. Sometimes we make it really hard in the industry.

Ms. Julie Dabrusin: Thank you.

The Chair: Thank you.

Mr. Dubé, go ahead for three minutes. I'll go after you.

Mr. Matthew Dubé: Thank you, Chair. I appreciate the indulgence.

There is an issue that I was kind of kicking myself for not raising with you earlier, which was just this Five Eyes communiqué that came out recently concerning the issue of backdoor encryption and lawful access. The privacy advocates are concerned with the wording of that communiqué. I was just wondering if your organization works with the private sector on any of the issues, just going back even to Mr. Eglinski's line of questioning about catching criminals and such. Is there any work being done that would undermine encryption through a back door or get us into the lawful access debate that we have had in the past?

Mr. Scott Jones: We actually have a program called the cryptographic module validation program, which we use to actually strengthen encryption and make sure it is done properly. That's something that we work with the commercial sector on in terms of making sure that the products we use in government but also the products that are available to all of us are secure and implemented properly.

One of the debates is about how law enforcement does its job in the modern world of communications, with encryption and computers becoming powerful enough now to actually do encryption. It was hard before. It was slow. What tools does law enforcement need? I think that's a policy question that's actually probably best left in your hands, in terms of how to address the need.

Mr. Matthew Dubé: I'm sure.

I don't want to have you answer for someone else's comment, but the spokesperson for Minister Goodale refers to decrypted data, access to decrypted data. For you as a specialist, what does "access to decrypted data" mean?

Mr. Scott Jones: I think if you're looking at it from the provider's point of view, there are some providers that are able to get to that data, so how do you provide that access, under what lawful authorities, etc.? You can ask, because it's not encrypted when it's, for example, on a vendor's server. It's things like that and how you get access to the data. It's a difficult challenge, especially when the encryption is on the communication between you and me versus when it goes to some central point where it's stored. It really depends on the circumstances.

Mr. Matthew Dubé: My understanding is that telecommunication providers, as we saw even with Apple with the iPhone in San Bernardino, have been reluctant to hand over any kind of access. What would be the solutions, then? If the Five Eyes public safety ministers are saying that they need to more easily gain access and those companies have been reluctant, would that involve convincing them in any way?

● (1735)

Mr. Scott Jones: I'm not sure what actually would be the method for that. I think there are a few different things, depending on the technology you're implementing. Sometimes it would be that the provider can provide the information, or they can design it. In a lot of cases they're designing it so that they don't actually see the data that traverses the network, and they're making explicit design choices. How you would address it depends on what you're actually trying to solve there. It could be technologically complex in some cases and it could be really easy for lawful access types of things.

Mr. Matthew Dubé: Thank you.

The Chair: Thank you, Mr. Dubé.

I have two questions. First, aren't you effectively creating a dependency between the private sector and the public sector through CSE or through this cyber centre? Over time, and maybe actually a short period of time, this will be a permanent dependency. This will be the new way that business gets done and that security gets analyzed.

Mr. Scott Jones: I think that's absolutely the case. We rely on private infrastructure that runs our critical infrastructure, which is built in the commercial space. Pretty much gone are the days of government-produced equipment. We can't keep up with the rapid innovation pace that the private sector is able to bring to bear. That's one of the biggest challenges in the cybersecurity sector right now. Innovation is outpacing security. How do we build the relationships so that we can work together? That's the only way to effectively start to deal with it.

The Chair: You're in effect baking in an interdependency. It's going to be there for the foreseeable future.

Mr. Scott Jones: I can't see doing this without collaborating with the private sector.

The Chair: We haven't talked at all about the role of academia. This of course has come up with Huawei again. They are fairly involved in 5G and probably other technologies that we're not even aware of. You said that you do a risk-based analysis as to where you intervene and where you don't. Frankly, that strikes me as the horse being out of the barn, and then you figure out whether this is a serious horse and whether it's a runner.

Huawei is involved in the creation of this 5G network, which will be the platform for everything. Is that within your mandate? If it's not, should it be?

Mr. Scott Jones: When we're talking specifically about 5G, meaning fifth-generation telecommunications networks, the best security outcome for anything related to 5G is really an environment with multiple vendors where you're able to put security protocols or security appliances in at different layers. That's supported by a multi-vendor approach. The international standards organizations are setting some of the emerging elements of 5G. Of course, 5G doesn't really exist yet. There are some prototypes and things like that. How do we start to bake these things in through some cybersecurity pieces?

I think the biggest thing for us is that you don't want one vendor and only one vendor. That makes you vulnerable across your entire spectrum and across all of your telecommunications companies to the exact same vulnerability. You want to build in different vendors. You want different vendors at different layers. That bakes in a large amount of security just because you can't easily traverse up and down the so-called telecommunications stack. That's one of the key elements for 5G.

Did you want to expand on it, Rajiv?

Mr. Rajiv Gupta: That's pretty much it.

We're looking for heterogeneous networks. It's always very important from a business continuity perspective as well—building the controls in, understanding what technologies are coming down the road. We're always working with all of the vendors.

You talked about a horse before it's out of the gate. We're looking down the road to see what's coming in 5G so that we can put the appropriate mitigations in now, before the telcos start deploying their networks. It's very important for us to understand these technologies and then provide that advice and guidance early on so that the risks are mitigated early on in the process, before they are deployed.

The Chair: On behalf of the committee, I thank you both.

This is incredibly complex. You've certainly given us a lot of food for thought.

Again, thank you for coming before the committee, and thank you for your thoughtfulness.

With that, 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: http://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 : http://www.noscommunes.ca