HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 163 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Wednesday, May 15, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Wednesday, May 15, 2019

● (1530)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Colleagues, I see quorum. This is the 163rd meeting of this august committee, the best committee on the Hill.

I'm pleased to welcome our guests today, all of whom have never made presentations to parliamentary committees before. I've asked my colleagues to go easy on you.

As you know, you each have 10 minutes. I'm going to ask Mr. Jarry to go first. At the end of his 10 minutes, I'll ask Mr. Gull to introduce his group and proceed with their 10 minutes.

Mr. Jarry.

[*Translation*]

Mr. Luc Jarry (Senior Advisor Cybersecurity, As an Individual): Thank you, Mr. Chair.

Good afternoon to all committee members.

My name is Luc Jarry and I'm a senior cybersecurity advisor for Cascades Inc. I'm also a lecturer and I teach industrial cybersecurity at the Polytechnique Montréal, which is affiliated with the University of Montreal.

This is my first time appearing as a witness. I spent some time reading the evidence from other witnesses and I noted that several topics were discussed. Today, I'll talk about a subject that affects virtually every domain, from financial affairs to the industrial, business and personal worlds. I'm talking about the Internet of Things, better known as IoT, which is of course associated with artificial intelligence.

What is IoT? I think the best definition is also the shortest: IoT is a direct integration between the physical world and computer systems. In the past few years, there has been an extraordinary revolution in the way objects connect to TCP-IP networks. I'm talking about the Internet. It has been estimated that by 2020, between 40 billion and 50 billion devices will be connected to the Internet. We will have to ask ourselves wether the "Internet of Things" will become the "Internet of All."

Together with artificial intelligence, the Internet of Things makes possible what was only imaginable a few years ago. Think for example of self-driving cars. They are still in the testing stage. We have all heard about them. Currently, if your car is even halfway modern, it will probably have a monitoring system that measures the pressure in your tires. If a tire's pressure is low, the monitoring system will send a message to the car's computer to warn the driver that one of the tires is low on air. The driver will then have to deal with the problem.

The same thing will happen with the Internet of Things, but in addition to informing the driver, the car itself will make an appointment at the dealership or the garage responsible for maintenance. The car will then drive itself to the dealership so the problem can be fixed, and it will then return to its point of origin. You can start seeing the potential involved. This will open up extraordinary opportunities in all areas.

Unfortunately, all these new technologies make us susceptible to new threats and vulnerabilities. However, computers, which have microprocessors and are controlled by operating systems, are virtually the only devices connected to the Internet. This makes it possible for us to implement basic cybersecurity defences. For example, I can see there are open laptops in this room. I'm sure that those computers have basic cybersecurity protections. This would involve a personal firewall turned on and probably an antivirus program—which I hope has the latest virus updates—as well as a malware scanner. There is something important to note here. These computers have a processor and are able to encrypt and decrypt data. I'm talking about encryption, a widely used strategy in cybersecurity.

The problem with the Internet of Things is that the objects have no operating system or processors. It is therefore impossible to give them basic protections, as we can do with computers. These makes them extremely vulnerable.

Over the last 15 or 20 years industries have invested heavily in mechanization and automation technologies. Today, modern factories use industrial control systems such as programmable automatons and SCADA, which communicate with each other via their own telecommunications protocols on private networks within factories. These networks are invisible to the Internet. We often refer to them as an intranet. For industries to ensure they can use and benefit from the advantages of artificial intelligence, they must connect these automatons or industrial control devices to the Internet in order to communicate with AI service providers. This makes these devices very vulnerable.

Another thing is that, based on my own observations, most industrial controls in factories are maintained and supported by electrical engineers, most of whom have no training in cybersecurity.

There are currently many factories connecting things to the Internet in a way that creates gaps in their internal networks, opening them up to possible intrusions. I'm talking about theft of information and industrial espionage, in short, unauthorized access.

There are now things worse than that. With the Internet of Things, we can imagine a hacker or even a terrorist group taking remote control of critical infrastructure such as a hydroelectric dam, a water processing or oil industry plant, a hospital and so on. Imagine all the ensuing damage and danger to public and financial security and safety.

We must also keep the privacy issue in mind. As you know, an increasing number of users are connecting devices to their own networks at home or via cellular networks. You can for example buy a smart refrigerator equipped with a tablet-like screen that takes inventory of all the food and drinks it contains, monitors their expiry dates and even suggests recipes for the food inside, thanks to artificial intelligence. It's a wonderful thing. However, from a privacy perspective, we might ask whether life insurance companies would be interested in knowing what is in their customers' fridges. The answer is yes.

In Canada, citizens are protected by privacy laws, but there is a problem. Many studies have shown that nearly 95% of users agree to terms and conditions of confidentiality without reading them. Often, people don't really know what they are agreeing to.

Still on the subject of privacy, there are now assistants that connect to the Internet and are activated by a specific sentence or word spoken by a user. You can dialogue with the assistant to obtain various kinds of information available online, such as weather forecasts or the news. If these types of devices are connected to an unsecured home network with easy access, a hacker could use a computer worm to record you. If the device has a camera, the hacker could take pictures of you. This would obviously be a breach of privacy.

I could give you several examples. The document I submitted contains a series of recommendations, but unfortunately I won't have the time to go over them all.

With your permission, Mr. Chair, I will now answer questions.

Thank you.

● (1535)

The Chair: Thank you, Mr. Jarry.

[*English*]

I'm probably going to have to get one of those fridges, because that fridge can make a meal of what's in my fridge. That will be a truly miraculous event.

Mr. Michel Picard (Montarville, Lib.): They don't make the meal for you.

The Chair: Bologna sandwiches are still bologna sandwiches, no matter who makes them.

Mr. Gull, for 10 minutes, and I'll ask you to introduce your colleagues.

Mr. Tony Gull (President, Tawich Development Corporation): Thank you.

[*Witness spoke in Cree*]

[*English*]

In my language, I thank you for hearing us out and giving us an opportunity to share with you a little in terms of opportunities we're looking at for our nation—the Cree nation—and our community, more specifically, Wemindji.

On my left are my advisers who are working on this file with us, our corporation. This is Sam Gull, an adviser; this is Jean Schiettekatte, another one of our advisers; and this is Robert Milo. They are three advisers and somewhat experts too in this field in terms of what we're trying to accomplish.

I guess the message here today from us, as you can see, is that it's a northern international fibre telecommunication highway to link Canada, Asia and Europe. It's key to assuring Canadian financial Internet cybersecurity.

For us, in terms of the corporation itself, it's wholly owned by the community of Wemindji, which is about 1,400 people. Right now the corporation, just to give you an idea, is called Tawich. Tawich means “far out”. It's a far out development corporation—that's the translation.

Just to give you perspective, right now Tawich employs over 1,000 people across Quebec, in the region of Abitibi and in certain other areas within the province. We have various companies. This is just another exciting opportunity we're looking into to basically reach the goal of convincing certain people to get into this project together.

As you know, it's basically *keskun*, which means clouds. When you're talking about cyber, Internet and talking about clouds, it's *keskun*, as it is pronounced in our dialect. Basically, it's the data centre project that we will be building on the Cree territory of our community. *Keskun* is essentially an industrial storage park and major Nordic data centres that we're looking at.

The project will initially require a power supply of about 200 megawatts. The most reliable green energy source in North America, as we all know, is the big Robert-Bourassa power station that is just a couple of hours' drive away from home. The Quebec energy board authorized the allocation of a certain amount of megawatts to calculation centres on April 29, 2019.

Right now we feel that Canada is basically limited to the U.S. for its international Internet connectivity. About 11% of Canadian international Internet traffic doesn't pass through the U.S.

We talk a lot in terms of what this gentleman just spoke about. The way I look at it is that it's a superhighway that we're trying to connect to and bring into our area. Canadian cybersecurity, including financial transactions, is dependent on the U.S.A. This is part of what we feel is kind of a weak link.

With that being said, I'll let my advisers and colleagues touch more on the project.

● (1540)

Mr. Sam Gull (Advisor, Tawich Development Corporation): *Meegwetch.*

[*Witness spoke in Cree*]

[*English*]

I want to thank you for inviting me to make this presentation.

As you see on the screen here, the biggest problem that we have here in Canada is that all of our links are in the United States. We only have 11%, which are on the Newfoundland side, to Greenland. That's our only escape route. The rest are all in the United States. This is a major issue for us.

As you see on the screen here, we have a project that we're looking at. It's called the Quintillion link. It is already serviced in Alaska—the first phase. The second phase will be service from Alaska to Japan, and the third phase will go from Alaska through the Hudson Strait to Europe. This is where we want to connect our pipeline to Wemindji because once that pipeline comes through we only have one opportunity to connect, and we don't want to miss that opportunity.

The northern link is a high-fibre.... It has six big fibre links that are connected, and two of them stay in international waters. Those are the two that we want to connect, and we believe that the security, safety and sovereignty of the Arctic are key for us as a first nation. This southern spur that's going to go to James Bay will also be linked to Montreal, Toronto and the southern network.

A Canadian northern international connectivity project must be developed to assure Canadian international connectivity and cybersecurity.

As you see on the map here, it would go through the Northwest Passage, from Alaska through the Hudson Strait. This is where we want to connect, through James Bay to the Wemindji-Tawich Development community, and from there we connect to the south, to Montreal and Toronto.

On this map you can see that 89% of Canadian data passes through the United States. The USA PATRIOT Act governs this data and governs Canadian data, and this is where we believe security is an issue. Canada's new northern fibre can change this paradigm. Data centres with access to northern international fibre connectivity and ultra-low latency connectivity, in the long haul, in milliseconds, are important. The geographic position related to financial hubs with London, New York, Tokyo, Shanghai, Montreal and Toronto is key. The inexhaustible renewable energy and ultra-reliable power in the north at a low cost, at an approximate price of 4 cents U.S. per kilowatt, is a strength on our part, and low operation costs for data centres with cooling would be a competitive advantage because the computers need a lot of cooling.

A northern link would assure the independence of international connectivity and security from the United States. As an example, one of the big advantages is that from Montreal to Tokyo, we're looking at 18 milliseconds of speed that we can gain just between those two cities. There's no real advantage into the United States. The big advantage is from Montreal and Toronto to England and Asia.

The other advantage is that Hydro-Québec has announced in their strategic plan that they would give an estimated 4 cents per kilowatt. This is a huge advantage for us in terms of power usage. Another advantage is that we're on the Canadian Shield, and there are no earthquakes. You probably know what happened in Japan and Alaska. Earthquakes are a big issue, so this could be a good location for data centres of the north.

I'll pass it to Jean Schiettekatte to make concluding remarks.

● (1545)

Mr. Jean Fernand Schiettekatte (Advisor, Tawich Development Corporation): Thanks, Sam.

Thanks, everybody, for receiving us today.

[*Translation*]

As you saw in the presentation, because of the ultra-low latency, all Canadian financial transactions will go through this link. This is an opportunity for us to offer Canadians a security solution that is not just software, but also hardware. The idea is to build an independent and international northern fibre, whose main benefit would be to enable Canadians, with the First Nations, to assert their sovereignty over this territory. This is a very important aspect that we want to see in this project.

I think that today is the last day you're meeting on this subject. We would like the Committee to consider this option. There is the Quintillion link—which is still under development, although its first segment is already in service—but there could be another Canadian project that would link to the network. As Mr. Gull said, parts of this line would stay in international waters. This could provide an international cybersecurity solution and would ensure that Canadians would have access to other markets with ultra-low latency. This would give us an advantage in our international financial transactions, and, most importantly, would enable us to assert our sovereignty over the Northwest Passage.

It would be a good idea to combine this with the connectivity of northern communities, but that should not be our primary goal. The primary goal is to ensure our security. There are of course all sorts of other benefits, such as worker training and job creation in the North, which are good for the economy.

Thank you, Mr. Chair.

The Chair: I thank you all.

[*English*]

Mr. Graham, you have seven minutes, please.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): Thank you all for being here. We have two very different witnesses.

For the *keskun* project, I find this very interesting. As you know, we've spoken about it in the past.

Monsieur Gull, if the Quintillion fibre network is built, and we don't get onto it, how hard is it to get onto later?

Mr. Sam Gull: I believe, as a Canadian, and as a Cree, that Canada has to do something, and build its own fibre. We know that the amount of information or data we use every year is increasing, and it will continue to increase. It's not ready to slow down.

If we can't connect to Quintillion, I believe Canada should step forward and build its own fibre.

Mr. David de Burgh Graham: You mentioned in your opening that this is an issue of network sovereignty. We don't currently have any network sovereignty to speak of. Quintillion, which runs from Tokyo to London, as I understand it, would provide non-U.S. sovereignty, and that's the core objective of this.

When you're talking about the use of the data centres, you're talking about an 18-millisecond speed advantage, and how it will impact the financial sector. From an investment point of view, what does that mean for the financial sector? Will they be obligated to have their data centres further north?

Mr. Tony Gull: I have just one comment before Jean responds to it a little more technically.

For me, it's about economic development—that's why I'm here. My mandate is economic development, and I believe the federal government's responsibility—and some of our responsibility—is economic development, as well. I think it will provide a lot of opportunities economically, but also, and more importantly.... Whether it's cybersecurity, or being sovereign with our own line, data is so important. It's crucial to have, and to keep.

For me, that's the impact—it's all about the economic development, because that's my mandate. This is what I do, and this is why I'm presenting here today.

Go ahead, Jean.

Mr. Jean Fernand Schiettekatte: The basic answer is very interesting. It's about that table of latency. No bank in the world could afford not to have a centre, at that point. If you're trading currency, you always need the data from the market in London, the market in Tokyo and the market in New York. We'll be the point of the hub. The main commercial transactions—the ones you talked about, where someone has hacked, or something—will be on that line, and we will control that line. That's not the case now—our transactions go by New York. When you do a wire transfer, it goes by New York; by that system.

That's why it's a key point of our position around the cybersecurity issue. If you want to address it, you must address that hardware problem.

● (1550)

Mr. David de Burgh Graham: Who controls the line?

Mr. Jean Fernand Schiettekatte: In the U.S., the NSA is looking at all your transactions.

Mr. David de Burgh Graham: They are on this side of the border too, I suspect. That leads to another point. There is a national security dimension to the Quintillion line and the *keskun* line. What can be done to protect that line from being attacked by scientific submarines in the north?

Mr. Jean Fernand Schiettekatte: I think the first step is to assert sovereignty. If you pass the line you'll be the first to occupy the territory there. If you wait for another company or another country to do it, you'll lose sovereignty. That's the idea, to monitor [*Inaudible—Editor*]. I think it's very difficult to assert the security of a satellite link, so that's why they're using link underground where they can monitor if there's a change in the property of the fibre to see if it's intercepted. That's the way to do it. I don't see any other option.

Mr. Sam Gull: To add to that, from what we understand from our discussions, the line will be buried at least three feet in the seabed because of the icebergs. That was an issue. If we bury it underground, the submarines won't be able to find it or see it.

Mr. Robert Milot (Advisor, Tawich Development Corporation): One thing for sure, once the pipeline of fibre optic is built, be it by Quintillion or anybody else, we cannot connect afterwards. It has to be done initially. Representations have been made to the Quebec government, to the Prime Minister, to several ministries, and there is a great interest.

Mr. David de Burgh Graham: That helps address a lot of problems you've dealt with in this study. We always have problems of [*Inaudible—Editor*] but this is the first time we've had a solution brought to us. I appreciate very much that you're here to do that.

I have a couple of quick questions for Mr. Jarry, if I still have any time.

[*Translation*]

Mr. Jarry, in your presentation you talked about the Internet and things.

Mr. Luc Jarry: It's the Internet of Things.

Mr. David de Burgh Graham: Okay. There was mention of a car talking to a mechanic to make an appointment. Wouldn't that leave the door wide open to the possibility that the car would go directly to a thief's house?

Mr. Luc Jarry: To a thief's house, you say?

Mr. David de Burgh Graham: Yes. I puncture a tire and then I tell the car that I'm a mechanic. It comes to my door and then I have the car.

Mr. Luc Jarry: That could be one of the vulnerabilities.

It goes without saying that these new technologies will lead to situations like that, but that's not the worst it. Right now, with your cell phone you can even control the front door of your house when you're away. You can answer the door and open it remotely. If someone gains access to your system, he or she can easily find out that you're away and then unlock your door.

Mr. David de Burgh Graham: Yesterday or the day before, there was a security breach in WhatsApp. Are you aware of that?

Mr. Luc Jarry: Yes.

Mr. David de Burgh Graham: Could you tell us a bit more about it?

Mr. Luc Jarry: Malware was remotely installed and used to spy on cell phone communications. If someone got a call, the device was infected, even if the person didn't answer. Again, this is a matter of updating the software. You are right. This made the news yesterday.

Mr. David de Burgh Graham: You said that 95% of users do not read the end user licence agreement, but I would say that number is closer to 99.99%.

Mr. Luc Jarry: The figure I provided comes from interviews conducted for a Deloitte study. I agree that that is a very conservative estimate.

Mr. David de Burgh Graham: You are no doubt aware of what PC Pitstop did in 2005. It offered $1000 to anyone who read its end user licence agreement. It was only after five months and 3,000 sales that the first person claimed the $1000.

Mr. Luc Jarry: Right.

The Chair: Thank you, Mr. Graham.

[*English*]

Mr. Motz, you have seven minutes.

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

Thank you to both groups for being here today.

I was intrigued with your plan to connect. You indicated your connectivity to the line that's being built through your fibre network is time sensitive. When do you anticipate the decision on that connection so you get in the queue to make sure you're connected prior to the line being installed?

● (1555)

Mr. Jean Fernand Schiettekatte: The time frame is two years from now.

Mr. Glen Motz: And that's when it's anticipated that line will be put through.

Mr. Jean Fernand Schiettekatte: They have to do the design to see, to have what they call a spur point to be able to connect in Hudson Strait to go down to the thing. The idea is that you have to start the design, the process. They're now working on the connection between Alaska and Japan. They did some surveying last summer and that phase is going to be executed. After that, they'll start to do the design in the two-year time frame

Mr. Glen Motz: One of the things that you mentioned, sir, in your concluding remarks, was hardware. You're obviously going to need some hardware as part of this line. How do you ensure that your hardware is secure, and that it's reliably sourced? This is a cybersecurity issue. The study we're doing for this committee is primarily focused on the financial end, but it involves lots of different components of cybersecurity. How do you intend to ensure that the hardware you receive is secure?

Mr. Jean Fernand Schiettekatte: I think it's a process of compliance within the supply of the element. The main point we're making is that if you don't have the line, you will be dependent on the U.S. The situation could not be worse. Of course, you have to make sure that your provider respects all the Canadian security standards for what they call the landing point or the landing station. There are some standards that you can use. Our military has some standards. I think they should be used to ensure you're complying with the proper hardware security issue.

Mr. Glen Motz: As your organization plans this and moves forward—and I think this is an incredible project to participate in—obviously there will be some expectations. As a proponent of this, you will be expected to ensure that the hardware you use is secure. I'm just curious to know.... That was the line of my questioning.

Mr. Jean Fernand Schiettekatte: One adviser company that we have in our team is IBM, which is very well known for doing that process, and they already have some standards, yes.

Mr. Glen Motz: In your material, Mr. Tony Gull, I think you mentioned that one of your businesses is called Creenet. I think that's an incredible business, but I suspect you had some significant challenges when you first started the process in becoming a service provider, especially in the area you're providing it. How have you been able to secure that network, given the challenges you had?

Mr. Tony Gull: Creenet started back in 1998, roughly. The idea was to basically be an Internet service provider, and to provide those types of services within the region, because they weren't present at the time.

To this point, we have faced many challenges due to market size. It's a very big, very competitive market when you want to be an ISP-type business, and you have to have the market. We were trying to chase after the Cree nation market, but in a nutshell, a regional entity was supported, which I think we have in our presentation. It's called the Eeyou Communications Network, and it is a regional entity run by the Cree nation government.

Mr. Glen Motz: In your opinion, sir, do you believe that your critical infrastructure—this and other critical infrastructure included — is sufficiently protected in the north by government? Does government take the protection of that critical infrastructure in your part of Canada as seriously as it needs to?

Mr. Tony Gull: Based on experience—hands-on, I've also managed our company for many years and now I sit at a different level—we're very vulnerable, just like anybody else. I think that security and any information for us...we've really been getting into that to try and secure ourselves, as well.

Like any other nation, like any other organization, as the gentleman spoke about, you're always vulnerable to any cybersecurity issues. You have to make sure that you always keep yourselves up-to-date, in terms of whatever software you use and whatever hardware you have to control it.

● (1600)

Mr. Sam Gull: Just to add to that, I think we know everybody who is coming into and out of the community. There's only one access road into Wemindji and one James Bay highway going north. They monitor everybody going in and out. On a road basis, it's very controllable. Wemindji, of course, has an airport, so it's accessible by air, but there's also James Bay. James Bay is very shallow. I don't think submarines can go in there; they'll hit a few rocks if they do. The bay is very shallow, and the sediments keep moving around.

Mr. Glen Motz: Mr. Jarry, my last question to you is, given your experience and your current role, do you feel governments do an adequate job in ensuring that our critical infrastructure is resilient to an attack in Canada? Is there anything, from your perspective, that we can do better?

Mr. Luc Jarry: From what I've seen, I think it's not in just Canada but all the countries in the world right now with the evolution of the Internet of things. When we talk about cyber-attacks, we're mainly talking about protecting the information. We talk about identity theft, fraud, denial of service attacks, those kinds of things. Now as we move forward with connecting objects, it's becoming more physical. That's the concern.

Did we do enough as far as cybersecurity is concerned? For an example, when there's a very sensible transaction or a command to close a certain valve, do we do enough strong authentication or biometric authentication? I don't think the answer is yes. It's probably no. It's not enough. But it's not just in Canada; it's across the world.

The Chair: Thank you, Motz.

Mr. Dubé, you have seven minutes.

[*Translation*]

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

I'd like to thank all the witnesses for being with us today.

Mr. Jarry, I have a question for you.

I'm sure you heard about the CRTC participating in an RCMP investigation of an individual who was using software known as "bots" for cryptocurrency. Everyone heard about it because it was the first time those powers, which were granted under the anti-spam legislation, were used.

That got me thinking, and it raised a question I'd like your thoughts on. If legislative and regulatory changes were to be made to address all the issues raised during this study, such as the Internet of things, would the CRTC be responsible for dealing with problems? For example, would it be better to create a new organization to enforce standards for devices? Is that something that would be looked at from both a legislative and a regulatory standpoint?

Mr. Luc Jarry: In the telecommunications industry, the CRTC definitely has an important role to play, especially in the whole area of electronic transmission security. Let's not forget wireless. Cybersecurity is not just about telecommunications; it's also about programming and development. We're also talking more and more about the physical aspect, which needs to be taken into consideration.

I think there should be an organization overseeing all those organizations, something that deals with all those fields. It's not just the CRTC.

Mr. Matthew Dubé: I understand and I agree.

What about the subject of the search warrant, who might be a cybersecurity threat? It had something to do with cryptocurrency, but we know the individual may have been engaged in other related activities. Under the act, would the RCMP or the CRTC have been able to do anything? Do we really need to update the act? As you said, do we need to be clearer about who deals with what to avoid confusion?

Mr. Luc Jarry: At the government level, I can't really answer that question, but I can tell you what I see in the industry. In my presentation, I said that electrical engineers are the ones who take care of a lot of equipment now. Those people have no cybersecurity training, but they are connecting things directly to the Internet.

To answer your question, yes, a number of things can be done. Should we have a specialized police force or response team? Maybe, but there are a number of fields involved. As I said, cybersecurity is not just about telecommunications.

● (1605)

Mr. Matthew Dubé: Gentlemen, you talked a lot about wanting to collaborate with Hydro-Québec. I'd like to look at another aspect of the issue that hasn't been raised. I'd like to know what you think about this because of the work you do.

A few years ago, the Government of Quebec, the Union des municipalités du Québec and Hydro-Québec indicated that Hydro-Québec's growing fibre-optic network, which has smart meters, might be a way to provide connectivity in more remote regions. What do you think of that idea in connection with the proposals you've made?

Mr. Jean Fernand Schiettekatte: We are talking to Hydro-Québec about using its dark fibre network, but that network is still just serving the south. It would help optimize the Eeyou Communications Network, the ECN, and enhance security for the south, but it is not a solution for the north.

We think the committee should look at that because it's a very important issue right now.

Mr. Matthew Dubé: Absolutely. You explained that well. That brings me to another question.

One of the cybersecurity concerns is the impact on our day-to-day lives because we use more and more things that could be compromised by cybersecurity attacks.

What is the reality for you, being physically far away from major centres? If there were a cybersecurity attack on a network in a major centre, the system would go down and we'd have all kinds of problems, but at least we are geographically close to other communities and other people. What impact could that have on your communities?

Mr. Jean Fernand Schiettekatte: I can answer that indirectly. Ideally, we'd be like Sweden, where the dark fibre network was installed by the government. All the providers use it and light up the same fibre. If there's a breakdown, one provider would be affected but not the others.

Our problem right now is that there is just one provider using one fibre. The goal would be to have a diversification strategy, and that's what we're talking about with government people. We want to see if there's some way to have more than one provider serving the region.

Mr. Matthew Dubé: Perfect.

I've covered all my questions, but I just want to pick up on what Mr. Graham said about how it would be good to have a concrete, forward-thinking solution rather than always focusing on current threats. That's important, but your perspective is important too.

Thank you.

[*English*]

The Chair: Mr. Picard, you have seven minutes.

[*Translation*]

Mr. Michel Picard: Thank you, Mr. Chair.

Mr. Jarry, you mentioned that you work for Cascades too.

Mr. Luc Jarry: Yes.

Mr. Michel Picard: Ever since computers have been around and companies have had electronic systems, we've had IT departments to handle software, updates, firewalls and so on.

Is the cybersecurity department just a new name for the IT department, or is there a different dimension to this that explains why private companies like Cascades now have cybersecurity departments?

Mr. Luc Jarry: The IT department is still the same, but there's now a cybersecurity group connected to governance that's not part of the IT team.

Mr. Michel Picard: What process did the company go through in setting up that cybersecurity element? Was it concerned about its equipment and afraid of service interruptions or machinery shutting down? Or was it worried about external attacks compromising its administrative data?

Mr. Luc Jarry: Sir, cybersecurity is based on three principles: confidentiality, integrity and availability of data. There is also a compliance aspect. All companies have to be in compliance now. I'm not old, but I'm experienced, and I remember a time when cybersecurity measures, though considered best practices, were only suggestions, not mandatory.

We now have mandatory laws and rules in place. Cascades was one of many companies to establish security policies and standards based on ISO 27001 and 27003. The company set up a governance group and deployed a security policy in accordance with its own standards. The policy is based on system confidentiality, integrity and availability.

● (1610)

Mr. Michel Picard: How do you ensure that your suppliers comply with the same standards to guard against being a victim of an attack within your system?

Mr. Luc Jarry: It's in the contracts. We can require suppliers to have specific certifications. For example, when our employees' personal information is involved, we require all our suppliers to have ISO 27018 certification, which covers the protection of personal information. That's one way to do it. Otherwise, we include specific standards or obligations in our contracts.

Mr. Michel Picard: My next question might seem like a trap, but I have to ask it anyway.

Let's look at things from the other way around. If Cascades were to be the victim of an outside attack on its data, would it be obligated to report that to someone, somewhere, in some way?

Mr. Luc Jarry: That depends on the kind of attack. If the attack affected personal information, then absolutely, we'd have to report the incident.

Mr. Michel Picard: Okay.

That happened at École Polytechnique Montréal and at Ryerson University. My colleague invited a representative from there, but we don't have a lot of institutions or resources in Canada with the expertise to manage our cybersecurity problems. Resources are limited, even rare. We are concerned that, as good as the expertise may be, it's not enough.

If we compare that to expertise developing elsewhere, especially the quality and scope of outside attacks, how would you compare the level of expertise and training available in Canada to those external threats?

I don't want any publicity or marketing here, but frankly, if we want to improve the situation, we need to know where we're at.

Mr. Luc Jarry: You are right. It is a concern not just in terms of training, but for all aspects of the industry. Experienced resources are becoming increasingly rare.

I have to say that more and more young people are becoming interested in cybersecurity. However, this field is still evolving. It is extremely difficult to find good resources with experience.

As I mentioned, I am a lecturer. We should not forget that this requires expertise in the subject matter taught as well as teaching skills. Those are two different things.

Mr. Michel Picard: In developing its cybersecurity strategy, is Cascades concerned that the attacks could compromise the survival of the company? Perhaps we are not yet there either?

Mr. Luc Jarry: In recent years, Cascades has modernized all its platforms. It has migrated to modern platforms, to SAP platforms, among others. With respect to availability, when these systems fail, the intolerance period is about two hours. This means that the plants start shutting down and cease operations after two hours. That is extremely expensive.

You are right. This creates a tremendous dependency. We address that with emergency plans and reconciliation tests with relays or data centres, and also with requirements we have for our service suppliers.

Mr. Michel Picard: Given the participation of Cascades—which is also a supplier—in this network ecosystem, is connectivity so sensitive that an impact at your end creates comparable difficulties for some of your suppliers?

For example, could someone compromise one of your suppliers by using your system?

● (1615)

Mr. Luc Jarry: In terms of connectivity, I would say no, not with our model.

We have dedicated links to some of our suppliers exactly because we expect greater reliability and availability. These are some of the aspects of fibre optics my colleagues are discussing.

We use protocols with different service providers in Canada and the United States with dedicated MPLS links. This is not necessary for others. We should not forget that there are levels of criticality associated with our systems: there are the "critical", "standard" and "average" levels. We put in place the measures required to ensure availability.

Mr. Michel Picard: Thank you.

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

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

My first question is for the representatives of Tawich Development Corporation.

We did some research on you. We discovered that you went to China recently and that you have photos of your meeting with the people from Alibaba.

Can you tell us if you reached agreements with them? If so, what kind of agreements?

Mr. Jean Fernand Schiettekatte: The people at Alibaba want to open data centres in Canada. They want to have data centres that meet Canadian standards. In fact, all transactions between Asia and Canada could flow through a northern fibre. This makes it interesting because it reduces the latency. Alibaba has opened several data centres in the United States.

Mr. Pierre Paul-Hus: I believe that the photograph shows the Cree nation signing an agreement with the Chinese. Have you already signed a memorandum of understanding?

Mr. Jean Fernand Schiettekatte: We have signed agreements, but not with respect to data centres. We import security equipment for mines, sweaters and things like that.

Mr. Pierre Paul-Hus: But no technology.

Mr. Jean Fernand Schiettekatte: No.

Mr. Pierre Paul-Hus: All right.

The company would be established in Quebec. Have you calculated the economic benefits for Canada or Quebec of the project you are undertaking?

Mr. Jean Fernand Schiettekatte: We are in discussions for a prefeasibility study, which would provide more solid statistics on the economic benefits. We believe that the banking data processing centres that would be established in northern Quebec would generate significant economic benefits for Quebec.

Mr. Pierre Paul-Hus: In the North, we already have the North Warning System, the Canadian portion of which is run by National Defence under NORAD. Would the proposed optical fibre telecommunication link be linked to the 47 existing radar stations?

Mr. Jean Fernand Schiettekatte: This is very interesting and something that I did not mention in our presentation, which deals more with First Nations. However, it would be important to add the Canadian military bases to this link. That is something that could be considered.

Mr. Scheer wants to ensure Canada's security and presence in the far north, and we believe that this fibre optic line is one of the tools that would make this possible.

Mr. Pierre Paul-Hus: Perfect, thank you.

Mr. Jarry, when we talk about the Internet of Things, we are also talking about the supply chain. My colleague asked a question about checking the devices that are purchased. What do you think of the Chinese corporation Huawei?

Mr. Luc Jarry: What is a little surprising about Huawei is that it has been working with Bell Canada for a long time. Now questions are being raised especially because there are concerns about security and espionage. I find it surprising that a company like Bell Canada has been doing business with Huawei for many years while other companies have backed away.

Mr. Pierre Paul-Hus: Is it the deployment of the 5G network that is problematic? The older devices were different. Could the new devices and 5G technology have a different impact?

Mr. Luc Jarry: I retired from Bell Canada after working there for many years. However, I did not directly participate in that project. What I can say is that we have concerns about security. I am talking about espionage. I was surprised to learn about that.

● (1620)

Mr. Pierre Paul-Hus: Okay.

Concerning the Internet of Things, you spoke about various remote controls for things. There are definitely some of us who have remote locking systems. These things are controlled by home automation systems. Can the equipment be programmed when installed and controlled afterwards, or must you control the automated system to control the thing?

Mr. Luc Jarry: One of the main problems with the Internet of Things is cybersecurity. Cybersecurity is not a consideration when designing and manufacturing most of the things that we want to connect to the Internet. One of my recommendations to the committee is to deal with this aspect once and for all. We now have to consider cybersecurity when connecting a device.

Let us not forget that automated systems are not new. As I mentioned, we have been investing in this area for 15 to 20 years. However, these systems were on closed networks. Now we will be able to prevent equipment breakdowns in plants with artificial intelligence.

Earlier, we talked about the availability of systems at Cascades. We will be able to operate systems 24 hours a day, seven days a week, 365 days a year. We can use artificial intelligence to anticipate equipment breakdowns. To take advantage of that we have to connect all the equipment.

We must not forget that the majority of cyber attacks that have taken place in Canada and around the world involve information and denial of service. When we connect these things, it becomes physical. In terms of security, we must now ask ourselves if this will be part of the country's military arsenal.

[*English*]

The Chair: Thank you.

Ms. Sahota, you have five minutes.

Ms. Ruby Sahota (Brampton North, Lib.): David is going to be taking my time.

[*Translation*]

Mr. David de Burgh Graham: I would like to come back to what was said earlier about the attack on WhatsApp, which was reported yesterday. According to the analyses we have learned about to date, it would seem that state actors were responsible for this attack and that the human rights sector was targeted.

In your view, are the world's greatest cybersecurity threats posed by the private sector or state actors?

Mr. Luc Jarry: Are you referring to vulnerabilities?

Mr. David de Burgh Graham: I am referring to the exploitation of vulnerabilities.

Mr. Luc Jarry: In my opinion, one of the problems with managing security incidents is that the companies are starting to communicate more of this type of information. I think it is still a little early.

To answer your question, I think it is a little of everything right now.

Mr. David de Burgh Graham: Attacks against states do take place and are fairly serious even though they are not the only attacks. What do you think of the KesKuun project that the other witnesses talked about?

Mr. Luc Jarry: I think the project is interesting. There is one thing they are absolutely right about, and that is that with respect to cybersecurity, availability is very important. In my opinion, it is important that we maintain our sovereignty in Canada, that we have our own fibre for telecommunications.

I am just hearing about this project. From a cybersecurity point of view, I fully support this type of project and approach.

Mr. David de Burgh Graham: That's good.

I will ask the other witnesses some questions.

[*English*]

Thank you.

I'd like to continue with Mr. Gull on the staging of the project. You said it's already in place in Alaska for this Quintillion project. It's already built in Alaska. What is the rollout process here?

It's in Alaska and we're trying to be a non-U.S. network. Can you explain that a bit more?

Mr. Sam Gull: The fibre that's being connected now is in service. When the line goes to Japan and to England, it's going to stay in international waters. There are going to be two pipelines that are not going into the U.S. Those are the two pipelines we're interested in, to stay at an international level. The U.S. won't be connected to that line.

Mr. David de Burgh Graham: Do you have any idea when Quintillion expects to finish construction of the third stage?

Mr. Sam Gull: It all depends on our winters. The Northwest Passage still freezes. Their concern, too, is the timing of putting that line through the Northwest Passage. That's why they're doing that last. There are certain places where it's very shallow and with the icebergs they really have to take their time and study that part.

● (1625)

Mr. David de Burgh Graham: When you talk about getting the Quintillion line connected to Canada via James Bay to have full network sovereignty, is there any way we can connect it to the west and east coasts as well? Can we connect it as a domestic network and not just an international network for us? Do you have any thoughts on that?

Mr. Jean Fernand Schiettekatte: Yes, that could be done.

There is a project for a line to go up to Yellowknife. That line could be connected on that side also. That's why our recommendation is basically to have a Canadian team develop that project in the north. I think this should be a recommendation of this committee.

Mr. David de Burgh Graham: It's a priority to get us connected to that line.

Mr. Jean Fernand Schiettekatte: Yes. The priority of Tawich is, for sure, the development of northern Quebec.

Mr. David de Burgh Graham: Sorry, but the priority of this committee is the cybersecurity. From that angle, I think it is fascinating to have this solution. Not only that, but to have it brought forward by the Cree first nation is really interesting for all of us to see.

I have only a few seconds left, I believe.

The Chair: If Mr. Eglinski is going to have any time at all, you'll probably have to be really brief.

Mr. David de Burgh Graham: I'll say one more thing to Mr. Jarry, and then I'll give it Mr. Eglinski. That's security by design.

Mr. Luc Jarry: What do I think about security by design?

Mr. David de Burgh Graham: Yes.

Mr. Luc Jarry: How many minutes do I have?

The Chair: You don't have any minutes at all.

It's a good question. We'll have to work on the answer.

We'll go to Mr. Eglinski for the final five minutes.

Mr. Jim Eglinski (Yellowhead, CPC): Thank you.

I'd like to thank our witnesses for being here today.

I'll start with this line you're proposing through the High Arctic and over to China. It's going to Japan? Good. All right.

Why would you have gone along the Arctic and not crossed along the bottom of Hudson Bay and then come across Canada, when there's been a lot of talk of a transportation corridor along the northern provinces and the bottom of the Northwest Territories, and connect it in...? It seems that there's a lot of extra work to go up toward the top and around, when you could tie into the bottom of Alaska and then follow the Aleutians out. It's the same with connecting to your European....

Was there a rationale for wanting to go so much higher up?

Mr. Jean Fernand Schiettekatte: There was a rationale around it. You can see it when you take a plane. All the flights that go from Toronto or Montreal to Asia basically go by the north. If you look at the distances, it's shorter to go by the north than by the south of Canada. That's where you gain the latency; there's a technical reason that is related to the business case. That's how you would attract the financial institution investor.

That's the first reason. The second reason is that we are for sure in the north, so we're pushing the development of the north; that's the mandate of Tawich. It's thus an interest of ours, but I think it's an interest of Canadians as a whole, especially given the discussion you saw in the news involving our neighbours in the U.S. who want to assume sovereignty over Canada.

I think it's very important that if you buy that line, you would mark with a substantial development the north of Canada. If you don't occupy the territory, at one point you can lose sovereignty over it.

Mr. Jim Eglinski: I'm glad to hear that coming from the business community, because it is a concern. It's a concern with our caucus that the sovereignty of the north must be looked after. Thank you for planning that in your strategy.

You talk about the power you need—some parts here say 300 and then 200 megawatts. Is that to feed the power to the line all the way across, or are you going to have to add more power as it continues? That's quite a distance that we're shooting, from your part of the country right around the top.

Mr. Sam Gull: The main point for the power from the La Grande dams is to feed the data centres. It's the data centres that consume a lot of energy because of the size of these data centres. It doesn't take too many data centres to consume 200 megawatts, even though we have all the natural cooling systems in the north, which reduce the cost of operating data centres. I visited data centres in Silicon Valley, and their main issue is the cost of cooling their computers.

● (1630)

Mr. Jim Eglinski: I take it from what you're saying here that your data centres will be located in your traditional territorial lands and then you'll be feeding that data back into Canada and other locations.

Mr. Sam Gull: Yes.

Mr. Jean Fernand Schiettekatte: To answer your question, yes, that's why there will be opportunity to connect some remote communities from which you'll get some power to do the repeaters. A design has been done to have a couple of communities feeding the line in the north of Canada. This is an occasion to feed. It could also be a military base that might be used to allocate the thing. I think it's a very interesting project.

Mr. Jim Eglinski: Thank you.

Mr. Jarry, in your professional experience, do you think we everyday users of the Internet services can protect ourselves adequately? Are there proper programs that we can buy to protect our home security, or is that just a fallacy of someone selling me a product that probably is not going to do the job?

Mr. Luc Jarry: Security is about two things, mainly. It's about training and about awareness. I mentioned earlier that many people agree to some confidentiality and haven't read the agreement.

To answer your question, yes, you can definitely improve your security. Now, is it 100% foolproof? I can compare it to driving a car. Putting on your seatbelt and having your ABS brakes and all those security systems enabled will probably prevent your getting hurt, if you get into an accident. But do you still have a chance of having an accident? You still do, yes.

Mr. Jim Eglinski: Security is only as good as the service that is being provided to Canadians, and in parts of Canada we know that the service is terrible, or almost to the point of rotten, whereas in other areas you have a very good service.

The Chair: Thank you, Mr. Eglinski.

Before I let you go, whose is the money behind Quintillion?

Mr. Jean Fernand Schiettekatte: From what we know, because we don't know them, it's a U.S. company that is basically supporting this project.

The Chair: So this is U.S. money and a U.S. company—

Mr. Jean Fernand Schiettekatte: Yes.

The Chair: —and this will be a project to protect us from going through the U.S.

Mr. Jean Fernand Schiettekatte: Yes, that's why we say we would like to have a Canadian team, but the Cree, we have some money, but we don't have enough to do it alone.

The Chair: Would a Canadian entity, whether it's you, somebody else or some combination, own it up through James Bay and Hudson's Bay up to the connection point, or would you own it all the way over to Alaska?

Mr. Jean Fernand Schiettekatte: We would like to own it up to Alaska and up to Europe. We would basically like to own phase three.

The Chair: What is the significance of being in international waters as opposed to domestic waters? You know there is a dispute over the Northwest Passage. Canada regards it as domestic. Mr. Pompeo regards it as international. What would be the significance of whether it's domestic or international to your project?

Mr. Jean Fernand Schiettekatte: It's basically not to be submitted through the PATRIOT Act and all the laws that regulate it. You want to try to be out of the reach of the NSA system. That's a concern that I think Canadians should be aware of. If I talk to the question that was asked of Mr. Jarry about who is doing the spying, it's a very good question.

The Chair: Finally, is your project subject to Canadian security review?

Mr. Jean Fernand Schiettekatte: Yes, it would be.

The Chair: Has that been initiated?

Mr. Jean Fernand Schiettekatte: No, we're still in the study phase. If you look on the Internet, you won't find too much information about what we're doing. Now is the first time we've publicized what we're doing. Yes, we have had some contacts, but there is still a lot of work to be done.

The Chair: Thank you for that.

I'm sorry to interrupt what is a really good and interesting conversation, but with that, we are going to adjourn, and I want to thank you again for your presentation to the committee.

We are suspending, not adjourning, and then we are going in camera. Thank you.

[*Proceedings continue in camera*]