HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

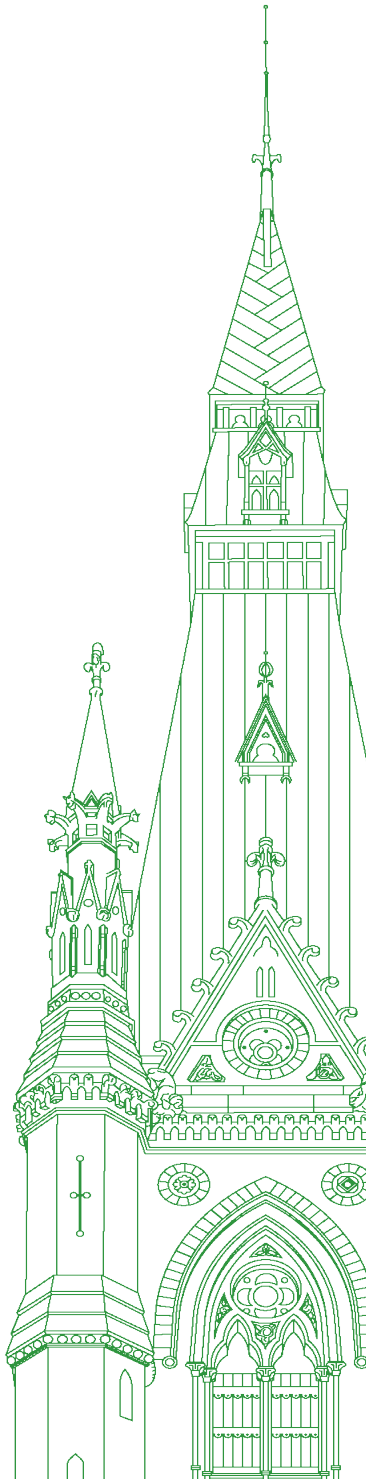
44th PARLIAMENT, 1st SESSION

Standing Committee on Industry and Technology

EVIDENCE

NUMBER 016

Tuesday, April 5, 2022



Chair: Mr. Joël Lightbound

Standing Committee on Industry and Technology

Tuesday, April 5, 2022

● (1530)

[*Translation*]

The Chair (Mr. Joël Lightbound (Louis-Hébert, Lib.)): Good afternoon, everyone.

I call this meeting to order.

I would like to start by thanking the witnesses joining us today using the Zoom application.

Welcome to meeting number 16 of the Standing Committee on Industry and Technology.

Pursuant to Standing Order 108(2) and the motion adopted by the committee on Tuesday, March 1, 2022, the committee is meeting on quantum computing.

Today's meeting is taking place in a hybrid format, pursuant to the House Order of November 25, 2021. Members are attending in person in the room and remotely using the Zoom application. I would ask all those attending in person to observe the health regulations in effect.

Before we hear from the witnesses who are here today, I would just like to address one small matter with respect to committee business.

We have two budgets to pass. One is for our quantum computing study and the other is for our critical minerals study. This will allow the clerk to initiate the expenditures.

Do I have unanimous consent among committee members to approve both budgets?

I see that all committee members agree.

Then, with no further ado, I will introduce the witnesses.

We welcome Gilles Brassard, professor at Université de Montréal's Department of Computer Science and Operations Research; Shohini Ghose, professor at Wilfrid Laurier University; Kimberley Hall, professor of physics at Dalhousie University's Department of Physics and Atmospheric Science; Marie-Pierre Ippersiel, president and CEO of PRIMA Québec; and Olivier Gagnon-Gordillo, executive director at Québec Quantique.

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

Mr. Brassard, you have the floor for five to six minutes.

Dr. Gilles Brassard (Professor, Department of Computer Science and Operations Research, Université de Montréal, As an Individual): Thank you, Mr. Chair.

Good afternoon, everyone.

Is it better if I speak in English?

The Chair: Mr. Brassard, interpretation is available in both official languages. So please feel free to speak French or English.

Dr. Gilles Brassard: Perfect.

My name is Gilles Brassard. I am a professor in the Department of Computer Science and Operations Research at Université de Montréal.

[*English*]

Let me speak in English and give my credentials, so that you know about me a little bit. I was involved in quantum information, *informatique quantique*, in the late 1970s, so I was the earliest person in Canada working on this topic. I invented, with Charles Bennett of IBM, quantum cryptography in the early 1980s and quantum teleportation.

That being said, my position about quantum information science, *informatique quantique*, is that it indeed should be a priority by the government for funding and research and development. This is a golden opportunity for Canada to remain at the top. Again, I was there with Charlie Bennett when there was essentially no one else in the world doing this type of research. Therefore, Canada was from the start leading the world in this discipline.

I want to tell you why it's so important to develop quantum information in all of its manifestations. One is that quantum computing poses a very significant threat to security. I'm sure you've heard it already, but I will say it again. Quantum computers, when they are built and we finally have a full-scale quantum computer, as opposed to the toys that are currently available.... These are fantastic technological feats, but at the moment they cannot really do anything useful that we would not do classically. But it is only a matter of time. Once full-scale quantum computers become available, then all of the security on which the Internet is based—not only the Internet, but essentially all of the cryptographic infrastructure on which we rely—will collapse, because of an algorithm invented by Peter Shor that essentially breaks all of the cryptography that is currently used on the Internet.

Let me be more precise on key establishment. Once a key is established, then it is used with more and more conventional systems, which are not so much threatened by quantum computing, but key establishment is. The reason why this is so serious is that whenever this happens it's not that secure communication will no longer be possible, but that all past communications become vulnerable. This is because nothing prevents what we call the “harvest now and decrypt later” strategy, which consists of taking down all of the information that goes on the Internet and storing it, even though the encryption cannot be broken yet. When a quantum computer comes along, then you can just go back, take all of that from your discs and decrypt retroactively. In other words, everything that's been sent on the Internet since essentially the beginning of time will become an open book when a quantum computer is available. Therefore, there's no way to try to protect the past. The past is gone forever—forget about it. But we can still hope to protect the future. This can only be done if we realize the importance of quantum secure communication.

There are two ways to do that. One is to use classical, ordinary cryptography and hope it is secure against quantum computing, which we will never be able to prove. All we know is that our currently used systems are vulnerable. Some new systems are being developed that may be secure, but we won't be able to prove that.

Or, you can use quantum cryptography. Of course, I have a vested interest in quantum cryptography, having invented it, but I have no commercial interest. Quantum cryptography is an alternative in which instead of using mathematics we use physics to protect the information in a way that is provably, unconditionally secure, regardless of the eavesdropper's computing power and technological sophistication. Quantum cryptography is secure even against a quantum computer and should be considered very seriously.

At the moment, China is deploying a large-scale quantum cryptographic network. They already have a network that links Beijing to Shanghai, which is used for real already with a satellite that they launched to experiment with long-distance space quantum cryptography. Quantum crypto is very seriously considered in China. Also, it is to a lesser extent, but quite a bit, in Europe. It's much less in North America, and really not very much at all in the United States. I think Canada should get back the lead on this topic to secure communications, because our society needs it.

Quantum computers can also be used for good to do all kinds of wonderful things like develop new medications, but that's another story.

My time is up, so I'll stop here.

● (1535)

[*Translation*]

The Chair: Thank you very much, Mr. Brassard.

Ms. Ghose, you now have the floor.

[*English*]

Dr. Shohini Ghose (Professor, Wilfrid Laurier University, As an Individual): Thank you, Mr. Chair.

My name is Shohini Ghose, and I have suffered my whole life from insatiable curiosity about how the universe works. In my office hangs a poster that says, “There is no cure for curiosity.” That curiosity inevitably led me to the strange quantum world, and now, as a professor of physics and computer science at Wilfrid Laurier University, I lead a diverse research team exploring quantum computing. I get to dream about teleportation—thank you, Professor Brassard, for inventing it—and about how it can be used in a future quantum Internet. Truly, I feel like “Alice in quantum wonderland”.

My team was the first to observe a connection between chaos theory and quantum entanglement. That's a phenomenon called the quantum butterfly effect. I also hold a TED senior fellowship, which has given me a global platform. If you have 10 minutes to spare, I invite you all to view my TED talk on quantum computing. It is the most-viewed TED talk on this topic.

I'm a good example of the Canadian connected quantum ecosystem in action. Although I'm not based at a major research university, I've worked with researchers in the quantum hubs in Calgary and Waterloo. I also have ongoing collaborations with colleagues at Ryerson and in industry.

My fellow researchers have already given you a sense of the huge potential for quantum technologies to impact multiple sectors. That brings with it opportunities as well as challenges for Canada. The most pressing by far, as you have heard, is the question of data security. I'm sure we'll talk about it more during the Q and A session. For now, I'd like to focus my remarks on three areas—education, collaboration and communication.

On the education side, even if every physics major in Canada were to choose a career in quantum computing, it would probably not meet the future workforce needs of the sector. Therefore, it is critical to develop talent from adjacent fields. You don't need a Ph.D. in physics to have a career in quantum tech. In fact, quantum computing sits at the intersection of physics, computer science, mathematics, chemistry, engineering and even biology. For example, for the past decade, I have been teaching a very successful undergraduate course on quantum computing for all science majors. It does not require any prior knowledge of quantum mechanics. Similar courses are now offered in other institutions.

A structured effort to build a unique broad-based curriculum that provides multiple pathways to quantum careers is needed. This could make the Canadian workforce agile and attract the best talent from elsewhere. This kind of effort would bring dividends regardless of the success or failure of a particular quantum technology.

Furthermore, there is a huge untapped pool of talent right here in Canada and around the world. Women, gender minorities and people of colour remain under-represented in science disciplines, particularly in physics, where one in five students is a woman. As of the last count, the number of black or indigenous women professors in physics in Canada was zero.

I hold one of five chairs in Canada for women in science and engineering, funded by NSERC, and the five chair-holders work together to increase the participation of women in STEM fields. I'm also the first Canadian representative to serve on the working group on women in physics of the International Union of Pure and Applied Physics, where the Waterloo charter on diversity and inclusion, which was launched here in Canada, was recently ratified. In 2019 I was the first person of colour to be president of the Canadian Association of Physicists, and I've been working to build a more diverse and inclusive physics community in Canada.

I really believe that the quantum revolution provides a unique opportunity for Canada to be a leader in building excellence through inclusion in this sector. We know how to build community in Canada, and we can show the world how to do it. This too would bring dividends regardless of the particular quantum technology being explored. Furthermore, ethics in AI has become an important and growing conversation, but quantum ethics is barely discussed. That seems to me a major gap that needs to be addressed.

The other thing I want to say is that it's a challenge to try to predict where a new technology will be used and what the applications will be. That's why a quantum ecosystem must include not just hardware and software engineers in quantum but also experts in health, finance, energy, and ethics to identify industry-specific needs and realistic quantum solutions. Interdisciplinary expertise and training will therefore be critical.

As a final point, I want to note that there is great public interest and enthusiasm for quantum computing, and a desire to know more. The Perimeter Institute in Waterloo, where I'm an affiliate, has offered many public lectures on the topic. They all sell out in minutes. My own online talks on quantum have received over five million views.

● (1540)

Now more than ever, it's clear that scientific literacy and public engagement play a key role in future societal progress. Canadian quantum scientists are already viewed as thought leaders, so they can play a major role in inspiring curious minds.

They say that curiosity killed the cat, but a quantum Schrodinger's cat is never really dead.

Thank you.

● (1545)

The Chair: Thank you very much, Professor.

We'll move to Professor Hall, for five minutes.

Dr. Kimberley Hall (Professor of Physics, Department of Physics and Atmospheric Science, Dalhousie University, As an Individual): It'll be hard to follow that.

My name is Kimberly Hall. I've been a professor of physics at Dalhousie University for the past 18 years. Throughout my career, my research has focused on various areas of quantum technology, ranging from spin-based electronics to quantum spectroscopy on energy materials and the development of what are called quantum emitters.

In my group, we use specialized lasers—very short laser pulses that we engineer—to study how to control these systems optimally when applied, for example, to quantum state initialization or quantum simulation using optical control of solid-state semiconductor qubit systems.

I have benefited from the significant early investments that Canada has made in the quantum area, like Discovery, CFI and Canada research chairs. I've had involvement with industry through contracts awarded via the offset programs with Lockheed Martin and Rockwell Collins. One of my graduate students started a company several years ago that applies some of the quantum science we have learned to solar cell technology.

I'm coming from Dalhousie University. Dal is a U15 school. It has strengths in areas such as ocean science and energy generation and storage. In the quantum area, we have a lot of room to grow. I'm one of only three faculty members focused on this area. The other two—Peter Selinger and Julien Ross—work in quantum algorithm development, which is a very different area from mine. Along with Peter and Julien, I'm an example of the very large number of quantum researchers in Canada that are leading internationally in their fields, but are not located at one of the three main hub institutions in the Canadian quantum space.

It has been said many times already that the most important role of the strategy is to support the full quantum ecosystem. In doing so, we need to keep in mind that fundamental research and commercial innovation are much more tightly linked in the quantum area than in any other field. This is because applications are being developed in lockstep with the development of an understanding of the basic physics behind them. Companies are being formed around concepts that are promising but not well-defined yet in some cases, and that are fundamentally evolving as the science evolves.

In funding this ecosystem, it is essential to support collaborations between the academic and industrial sectors. There are many crucial areas of quantum science that have a great potential for future innovation, but for which the research is not yet at a stage where direct ties to industry make sense. These must be supported as well.

I'll give you an example. We, along with groups around the world, are discovering and developing new two-dimensional materials right now. These are single atomic layers of a material in which it turns out that simply stretching this very thin layer over a very small pillar creates what's called a quantum emitter. It is a source of single photons, which are essential in many areas of quantum technology. The interesting thing is that you can actually deposit this layer of atoms using something quite similar to scotch tape. This means that we can create an entire photonic circuit using the technology we have now and introduce quantum functionality by simply peeling and sticking these layers on top.

This may turn out to be a crucial step needed to get quantum photonic circuits to the commercial stage, but at this point, we are just peeling and sticking different kinds of materials for the first time and trying to figure out why these emitters form. This is an example of something that's very promising, but clearly not ready to be spun off into a company.

Another point I want to make is that the more excellent scientists and researchers we have tackling this field in Canada, the more excellent ideas, companies and products we are going to produce as a country. Two heads are better than one and we need many more heads than two. Great ideas can come from anywhere in the country. They can come from small institutions or large ones. They can come from people of many different cultures and visibly distinct groups. A healthy quantum ecosystem must have a broad base to prepare us for the next 20 years of innovation. The funding landscape must support this broad base.

In relation to this, it is true that as a country we are investing less in quantum than some other countries, so there's been considerable discussion in these meetings of the need to spend the funds strategically. No matter what amount of funding you start with, you must dedicate some of it to supporting the broad base or the ecosystem won't be healthy and we will all lose in the long term.

We must do better at this. The key is to have open competitions where excellence is the metric and to avoid the artificial barriers that can come into play from the structure of the funding program that we choose. For instance, I believe that a quantum supplement to Discovery grants would reach excellent researchers within a much broader range of contexts than some of the other programs that have been explicitly highlighted in the strategy. This would also increase the number of quantum trainees. The NRC challenge programs are also quite good.

Finally, I just wanted say that it is fantastic that these meetings are happening and that you will all have a chance to share what you have learned here with your constituents.

● (1550)

It is crucial that the public, if not understanding how quantum tech works, at least understands why it's important to invest in. This is not easy because people think they already have fast computers. By the time you explain what an NP-hard problem is, many of those who are not in math and science will have lost interest. It is much easier to remember examples like magnetic field sensors that will mean that when you get an MRI you won't have to get into a claustrophobic chamber that takes up half a room as well as a lot of energy, the gravitational sensors that may allow us to see if a culvert is blocked without digging up the ground, or the photonic sensors that enable us to see around corners.

We all know that big money is being invested in this area because of national security, not because of these other applications, but that is not the main consideration when it comes to effective outreach. The point is, whatever words you choose to describe the value of quantum please spread those words widely.

The Chair: Thank you, Professor Hall.

We'll now move to Mr. Chong for five minutes.

Dr. Jaron Chong (Chair, Artificial Intelligence Standing Committee, Canadian Association of Radiologists): Thank you very much.

Mr. Chair, members of the committee and fellow panellists, my name is Dr. Jaron Chong. I'm the chair of the Canadian Association of Radiologists' standing committee on artificial intelligence. I'm also an assistant professor of radiology at Western University here in London, Ontario, and a body imager at Victoria Hospital.

The CAR represents Canadian radiologists and represents almost 2,900 members who provide medical imaging for millions of patients across Canada. Radiology is at the forefront of technological innovation in medicine, relying heavily on the contributions and developments of advanced technologies to enhance patient care.

These breakthroughs in imaging technology and research have led to almost an exponential growth of imaging data over the past few decades, which has then been applied back to health care questions and workflows, particularly most recently in the domain of artificial intelligence.

In 2017, the CAR established a standing committee on AI to deliberate on the practice, policy and patient care issues related to the implementation of AI in medical imaging. Through a series of highly cited white papers, contributions to scientific forums and engagement with policy-makers in Canada and abroad, the CAR has been a leader in the international conversation about AI.

I say all of this and realize that this is a session on quantum computing, and I am not an expert on mechanics or computing in that way. What I do represent, however, is what we hope will be one of the ultimate end point applications of quantum computing, particularly as it relates to AI, to help optimize health care and medical imaging.

From the health care perspective, quantum computing may not necessarily solve new classes of problems that are not currently tackled right now with conventional computing, but they may vastly accelerate the computational speeds of our most NP-hard, difficult training projects and experiments, and greatly expand the size and scope of the clinical problems we tackle. Really, we do see that conventional digital computing and quantum are mutually complementary and will almost certainly coexist for a very long time.

However, what we're most excited about is that we expect the speed at which we can train algorithms will improve by orders of magnitude. Imagine training a neural network to detect lung cancer on a CT scan in minutes instead of days to months, or—as was previously mentioned—developing a novel chemotherapy molecule for mass production in simulation, as opposed to years and years of lab experimentation.

If there's one lesson that radiology has learned about AI in the past five years, it's that the computation and the algorithms can actually change by the year and by the week, but the datasets being used to train those algorithms are a much longer-term investment, so the careful curation of datasets has remained useful from 2017 to 2022 and beyond.

Regardless of whether you're thinking about conventional or quantum computing, the amount of curated, labelled data harnessed to optimize all these patient outcomes, ensure appropriate care and enhance the efficiency of the entire system is very much a “garbage in, garbage out” metaphor. Our current work on AI right now is hindered sometimes more so by the amount of time it takes to clean and curate good data than it is by the computational capacity. I will make a metaphor: A faster car doesn't get you there faster if your roads are still full of potholes.

What we need to ask ourselves about right now is what long-term policies and investments in better data today will position Canada to be creative, competent and competitive for our health care AI needs of tomorrow, and for quantum AI, as well.

We feel that that, during the last AI revolution, investments in centres of excellence and basic science enabled Canada to play an international leadership role that was vastly disproportionate to our size and population. The real challenge is maintaining our competitive edge and retaining the benefits of our investments as these innovations are applied to various sectors. We've often seen that we invest in the short term on a cyclic manner, but the downstream benefits of those investments were oftentimes difficult to fully realize for Canadians on a population level over the long term.

From a health care perspective, we have to accept the very realistic probability that the majority of health care AI used on Canadian patients will not have been developed or trained on Canadian data. If this is the case, are we prepared to accept the consequences of imported biases, failure to perform or failure to generalize, or even the economic significance of importing them and not solely exporting applications?

In a postquantum computing landscape, we would expect that the strengths and the weaknesses of data infrastructure would be magnified. Those who have the pipelines will run faster. Those who do not will fall behind or perhaps find themselves buying from another.

If you are a decision-maker, we want you to know that we still think there's a dramatic need for investments in digitization and data collection. We need to ensure that the data we are collecting is good data that meets our current and future needs, and we need to improve our data infrastructure to facilitate data sharing to empower investigators, while also safeguarding the rights of patients and privacy.

● (1555)

We do need to continually invest in the basic sciences and fundamental research that will help make the promise of quantum computing in health care and real-world applications less of a far-off proposition. We've seen that with earlier efforts to advance AI that Canada definitely has the talent and the technical know-how to lead in this field and in many others. What will make a difference for Canadian patients and the health care system is if we can find a way to incentivize innovators to develop and implement their technologies here at home.

I welcome any questions you may have, and I look forward to the hopefully very interesting discussion coming up next.

Thank you very much.

[*Translation*]

The Chair: Thank you, Mr. Chong.

Ms. Ippersiel, you have the floor.

Ms. Marie-Pierre Ippersiel (President and Chief Executive Officer, PRIMA Québec): Mr. Chair, members of the committee, thank you for inviting me to appear before the committee.

I head up PRIMA Québec, the advanced materials research and innovation cluster.

[*English*]

PRIMA is a sectoral industrial research group. There are nine in Quebec in different sectors, which are mandated by the Quebec government to facilitate and support the advanced materials ecosystem through collaborative innovation.

[*Translation*]

We therefore bridge the gap between the research and industry communities by fostering collaborative innovation. In other words, we foster relationships between research and industry players, and we support the development of projects that we are then able to fund.

Concretely, these projects will enable companies to tap into research expertise so they can innovate, be more competitive and, most importantly, stand out in the marketplace eventually.

Over the past five years, we have supported more than 90 projects with a total value of close to $90 million, which brought 190 industry partners together with 26 research partners. Most importantly, these projects led to the training of over 120 master's students and more than 275 doctoral and postdoctoral students who, as you know, will form a highly qualified and useful workforce for industry.

With respect to quantum computing, eight projects with a total value of $8 million have been initiated over the past two years, and this will cultivate talent.

[*English*]

Professor Alexandre Blais, of the Université de Sherbrooke, whom you heard on March 25, made the link between quantum and advanced materials.

Let me say a few words about advanced materials, which play a strategic role in all economic sectors. Advanced materials are new or significantly improved materials that provide a significant performance advantage, physical or functional, over conventional materials.

[*Translation*]

Physical performance refers to materials that provide improved electrical and thermal conductivity, as well as materials that have magnetic properties.

Functional performance refers to hydrophobic, icephobic and biodegradable materials, as well as self-healing and smart materials.

At the same time, I'd like to point out that advanced equipment is key when developing advanced materials, and this plays a critical role in terms of a company's capacity to innovate.

The advanced materials sector is primarily made up of innovative small and medium-sized enterprises, or SMEs, which, although they are active in research and development, don't always have the internal resources to carry out characterization tests, material synthesis, surface treatment or scaling.

As a result, access to equipment and related expertise is critical, not only to seal the transition from technology to innovation, but also to help businesses gain access to various markets.

All of this and access to advanced equipment are equally prevalent in the quantum technologies sector.

● (1600)

[*English*]

Finally, with respect to the committee's focus, quantum is seen as an enabling force and driver in the discovery and development of new materials, processes that integrate materials, or in the development of equipment for their production or characterization. Simply put, quantum accelerates simulations and will allow us to combine all kinds of properties and functionality that we want to obtain, and do it more quickly.

[*Translation*]

To continue to meet their customers' needs, big industrial players, particularly those whose products and applications rely on solid simulation, manufacturing and characterization capabilities for new materials, must invest in modelling, developing new materials and optimizing processes to implement the materials.

As others have already mentioned, however, we will need to increase awareness of the benefits of quantum technologies among these industrial players.

I would be happy to answer your questions.

Thank you for your attention.

The Chair: Thank you very much, Ms. Ippersiel.

Mr. Gagnon-Gordillo, you now have the floor.

Mr. Olivier Gagnon-Gordillo (Executive Director, Québec Quantique): Good afternoon.

Thank you for the opportunity to appear before the committee today.

My name is Olivier Gagnon-Gordillo, and I'm responsible for the Québec Quantique initiative, which aims to make quantum science and technology an economic and social development driver for Quebec.

[*English*]

Québec Quantique started its activities about a year and a half ago. The original and basic idea is to catalyze and ensure concerted action among local players and to ensure that the Quebec ecosystem gets to shine outside of our province with a collective brand, making it easier to connect with companies, investors, researchers and talent interested in collaborating with actors from our ecosystem.

Today I will focus on two main topics that I believe to be of interest for the Canadian national quantum strategy, and I will share some examples of what Quebec is doing in line with these topics. One, I will talk about talent development, retention and attraction. It has been a much-discussed topic lately. Two, I'll discuss the adoption of quantum technologies from industry.

First, let's start with two examples of current initiatives in Quebec that do address these topics. The first example is Sherbrooke's Institut quantique, which was announced earlier in February. The recent announcement of the Sherbrooke quantum innovation hub is a great example of an initiative that needs to be supported by the federal government. The hub in itself is a $435-million project out of which $131 million is injected directly by the Quebec government to support 13 projects within that hub and that includes the purchase of an IBM quantum computer, which is the fourth outside of the U.S.

This hub will facilitate the creation of new quantum start-ups, while facilitating multi-level collaboration between vocational institutions, colleges and the university where problem-based learning and the project-based approach will serve as a reference framework for developing innovative learning situations. This initiative will play a key role in attracting and retaining talent in companies, while boosting direct investments from abroad.

The second example here is Québec Quantique, which I am the lead of. This initiative came to life to address, among others, the topics that I covered here today but on a provincial level. We are more than willing to collaborate with the rest of Canada to become more cohesive with international collaborations. Some initiatives, for example, that we are involved with are missions abroad. We were recently in New York with a Quebec mission, and we're about to go to Europe along with the federal mission in Germany. We will do a Quebec mission this spring as well in France and the Netherlands.

We're organizing a big quantum hackathon in June 2022 that aims to bridge or at least explore the gap between technical and business solutions. It's open to everyone in Canada, and similar editions will take place in Chicago and in France with QuantX. We've also offered training to Quebec delegation representatives and provided communication tools for them to promote the sector abroad. We're willing to do the same for Canadian embassies. Québec Quantique offers a common brand and central communication hub for basic educational information, news, events and even open positions in Quebec in the sector.

Now on to my first topic, talent.

The true quantum advantage lies in the talent available within an ecosystem. We need to make sure that we develop, retain and attract talented individuals to the quantum sector in Canada. Currently, although universities are doing a great job at training tomorrow's workforce in this field, a lot of that talent doesn't stay in Canada. It often leaves for bigger markets that offer more interesting conditions. The federal government can help in sponsoring programs to derisk the path towards entrepreneurship for students in the sector. This would also play a double duty in supporting the creation of more start-ups in the sector.

● (1605)

[*Translation*]

The Government of Canada has a high rejection rate for visa applications in many priority markets, particularly in French-speaking Africa. Immigration policies and processes must be adapted to facilitate international mobility rather than blocking it.

Moreover, the quantum science and technology community must address a glaring lack of diversity. Recruiting international students and workers has a central role to play in mitigating Canada's talent shortage.

[*English*]

Talent also needs to be seen in a broader spectrum as it involves people, such as me, who do not have an academic background related to quantum sciences but who can bring value to the sector. Companies and ecosystems won't be able to thrive solely on Ph.D.'s, and an effort to increase the basic knowledge of business leaders is essential to speed up the adoption of quantum technologies by industries.

Now I'll move on to my second topic. To attract companies in starting quantum-related projects, it would be necessary to highlight the possible applications and industries that could benefit from participating in this field. Use cases with a marketable approach rather than a tech push approach is a must in attracting companies to the sector. Beyond the business leaders, companies and potential users need employees who can understand what quantum can actually mean to them and help them integrate it into their business. Companies outside the field are more or less aware of the possibilities of quantum tech for their sector.

Start-ups would like to see an effort made to democratize the subject and, thus, facilitate their approach to potential customers and suppliers. Some are struggling with issues related to better understanding their potential market, knowing the players in the industry and identifying their first customers.

To conclude, the Canadian national quantum strategy comes at a critical time when investments, both from the private sector and governments, are accelerating. Canada must be agile and make the right strategic decisions to remain relevant and at the forefront of quantum sciences and technologies. Continuing to fund existing programs is a great start, but more needs to be done. Some funds should be allocated toward provincial ecosystem efforts and for a common Canadian ecosystem.

There are many key players and interesting quantum initiatives in Canada right now, but more cohesion among the provinces and various local ecosystems would help to boost the impact Canada can have on the international scene. As a country, we're often listed in the top five, but it's a fragile position if we don't invest adequately in the sector. Making the right decisions today will ensure that Canada gets to reap the social and economic benefits deriving from the development of this promising sector for generations.

As mentioned by Raymond Laflamme at a previous meeting last week, this is a marathon rather than a sprint, and sufficient long-term investments will be extremely important in this global quantum race.

I'm sorry if I spoke very quickly.

I'd love to thank you for the opportunity to talk here today.

The Chair: Thank you very much, Mr. Gagnon-Gordillo.

We'll now move to our first round of questions, with MP Gray for six minutes.

Mrs. Tracy Gray (Kelowna—Lake Country, CPC): Thank you, Mr. Chair.

Thank you to all of the witnesses for being here today.

My first questions are for Dr. Brassard.

You mentioned in your testimony that all security, on which the Internet and others are based, with the algorithms currently in place will collapse due to quantum computing and that it's very serious. You referred to “harvest now”, and you were talking about storage, going back and what would become public.

Can you describe what that means quickly? Are you referring to deleted messages or deleted emails? What exactly does that mean, if you don't mind?

Dr. Gilles Brassard: “Harvest now and encrypt later” means there's no protection on the Internet that prevents all the data packets that go around everywhere around in the world from being intercepted. They can continue on their way, so it's not noticeable, but you can take them and store them. That's what “harvest now” means. You can harvest at the moment all the information that goes on the Internet, even though some of it is protected by cryptographic systems in the current cryptographic infrastructure.

Those that are currently protected maybe—I only say “maybe”, because we don't know. Nobody knows how to decrypt them today without knowing the key. This information that is harvested includes all you'll need to decrypt it later when a quantum computer becomes available.

When there's a full-scale quantum computer, which we, hopefully, don't have yet, but there's no guarantee.... Maybe there is one running in some agency's basement somewhere. In the system, there is no full-scale quantum computer yet today, but there will be one. There is no doubt at the moment that full-scale quantum computers will finally become a reality. At that time, all of this information that has already been harvested can be taken back and decrypted retroactively.

That's what I meant when I said that everything that's been on the Internet will become an open book. There's no point trying to save the past. It's gone forever.

● (1610)

Mrs. Tracy Gray: Great. Thank you so much. We have limited time here, so I want to get through a few more questions.

How soon do you think this could be looming? Where do you think the biggest threats would be from, potentially?

Dr. Gilles Brassard: “When” is a very difficult question. There are so many technological challenges before this can be achieved.

I'm a theoretician, so I'm not the right person to ask. However, there are some people who are more knowledgeable than me, like Michele Mosca—who, by the way, should have been invited to this committee if he hasn't been. He is the most vocal person about this threat. He thinks that the priority is 1 and 2, and that within 10 years we will have this capability.

I think I can guarantee—

Mrs. Tracy Gray: Thank you for that.

Do you believe governments, as well as institutions like banks, schools, hospitals, social media platforms and apps businesses, are all aware of this emerging security risk from quantum computing?

Dr. Gilles Brassard: They're probably not.

Mrs. Tracy Gray: Okay. That's a fair answer.

What should be done to increase awareness and set off the alarm bells to ensure that they're ahead of the curve in protecting Canadians' security and privacy?

Dr. Gilles Brassard: There needs to be education.

There is no magic bullet. People are not sufficiently aware of the threat, and when they are told, they might panic.

It's like global climate change. I know that time is limited, but trying to fix the issue will cost money but nothing near as much as it will cost if we don't do anything, again, as with global climate change. I'm talking about the weather, of course.

Mrs. Tracy Gray: Thank you.

What kind of threat to national security could this pose?

Dr. Gilles Brassard: It depends what cryptographic system they are actually using. If they are depending on the systems that were developed in the eighties perhaps, then it is very much a threat. If they're using something else that they're not telling us about, then perhaps national security people have already developed stuff that would not be vulnerable to quantum computing. There's no way I can tell.

Mrs. Tracy Gray: Thank you.

What policies would government now be looking at developing in order to counter some of these looming potential security risks?

Dr. Gilles Brassard: I think there should be a culture of not encouraging banks, enterprises or what have you that do not migrate to quantum-safe technologies. If they don't want to make the effort, then they should not be trusted and people should not do business with them. If there is a consensus on withdrawing not only federal support, then that will require education of the customers. If customers understand they should keep away from vendors who are not protecting them, then perhaps that would foster a faster reaction.

The Chair: Thank you very much.

That's all the time we have.

We'll now move to MP Gaheer for six minutes.

Mr. Iqwinder Gaheer (Mississauga—Malton, Lib.): Thank you, Mr. Chair.

Thank you to the witnesses for making time for this committee.

My first question is for Mr. Brassard.

I'm especially interested in the introduction between finance and quantum computing.

How are private businesses, especially those in the finance sector, preparing for the coming risks and opportunities posed by quantum cryptography?

Dr. Gilles Brassard: In the financial sector if there is a leak of confidential data, that's a serious threat, of course; I should have said that.

However, if you can decrypt it later, it's not entirely bad, because sometimes if you can decrypt in 10 years something that came out today, maybe it's not serious. It's only a threat if the information is decrypted at the time when it is still relevant, which in the financial sector could mean only a fairly short period of time later, if I understand your world. As soon as a quantum computer is available, if financial transactions that should be kept secret become an open book to competition, that could be serious. If it involved other countries, it could be a serious problem.

Quantum computing may offer good things for the financial sector. It is conceivable that quantum algorithms would be able to solve some problems in the financial sector more efficiently than classic computers can. We should not think of quantum computers as being evil. They are in fact mostly good as long as they're used for good reasons, like most other things. Now we're afraid of their use for bad purposes, but they have much more potential for good in the longer term.

● (1615)

Mr. Iqwinder Gaheer: That's great.

Thank you.

My next question is for Madam Ippersiel.

What limitations are there to advance material research faced with classical computers? What solutions can quantum computing provide in that area?

[*Translation*]

Ms. Marie-Pierre Ippersiel: Could you repeat the question, please?

[*English*]

Mr. Iqwinder Gaheer: I will, happily.

What limitations does advanced material research face with classical computers? What solutions can quantum computing provide?

[*Translation*]

Ms. Marie-Pierre Ippersiel: Thank you for the question.

I'm not a materials expert, but I have a team that specializes in this area. Quantum computing will essentially accelerate the development of new materials. We mustn't lose sight of this. Twenty years ago, it could take 10 to 15 years to develop materials. I am exaggerating a bit, but you can see the extent of the problem. Quantum computing, and the quantum field in general, will accelerate the materials discovery process.

Similarly, we will be able to identify the physical or functional properties we want to discover for new materials. With quantum computing, we will be able to build on that to accelerate the development of new materials. I feel that's a major advantage.

I will come back to advanced equipment, because that's something very dear to us at PRIMA Québec. Advanced equipment is important. It's available in many university departments and colleges in Canada. However, not only do you need access to it, but you also need the staff with the skills to use it. This is true for what I would call classical materials, which are developed by way of existing measures and resources, but also for the quantum computing sector.

Does that answer your question?

[*English*]

Mr. Iqwinder Gaheer: That definitely helps. Thank you.

My final question is for Dr. Chong.

I'm looking at the introduction between quantum computing and medical data. How is quantum computing going to improve the analysis of medical data and what benefits could be fully realized from that?

Dr. Jaron Chong: The way I would make the metaphor effective is that the kinds of calculations that are posing these security risks depend on the specific problem. It can potentially be, as was often said in the previous answers, vastly accelerated.

In any experiment, in any new product development, and in any new AI development, there is always a component that is dedicated to computation. But not just computation, like you push a button, and you create a system out of that. A lot of the experimentations, hyperparameter optimizations, and trying different settings of a model while you're training it, all consume vast amounts of energy and time.

There is some theoretical work that would suggest that if we can convert some of these training problems for neural networks into a quantum computable problem, the same benefits that you would have for decrypting an encrypted message could actually be applied for the training of a neural network. That would enable you to run multiple computations simultaneously and vastly accelerate your training time.

The emphasis from our original opening statement was that this was just one component of the greater health care application, but it was a substantial part of it. Some of those resources, some of those calculations, are only accessible to the largest, best funded public institutions and private companies.

The ability to vastly accelerate, by several orders of magnitude, these kinds of computations is going to make what was previously hard maybe a little bit easier, and what was previously impossible, now possible.

Stepping outside of the field of radiology for a second, many of the things within them, like proteomics and genetics research, involve even larger degrees of analysis, drug discovery, and drug development, which involves protein folding. Things and applications like that, that are extremely expensive and very difficult to perform now, may become much faster. This is going to enable a whole new generation of potential treatments and potential AI systems.

● (1620)

[*Translation*]

The Chair: Thank you very much.

Mr. Lemire, you now have the floor for six minutes.

Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Thank you, Mr. Chair.

Dr. Brassard, let me begin by saying that it's an honour to welcome you to the committee. My goodness, you have such an impressive resumé.

In your opinion, what will the initial applications of quantum technology be?

What could we do in terms of the energy transition? Are there opportunities in electric vehicles, for example?

Dr. Gilles Brassard: In my view, quantum cryptography will definitely be the first application. It's not for the future, because it's already functional. As I said, China is taking it very seriously. So it's a real application that's already functional for protecting information.

With respect to quantum computing, quantum computers, the first application will likely be to simulate physical systems. Physicist Richard Feynman foresaw this application in 1981, when he introduced the concept of the quantum computer. The way he saw it, a quantum computer would have the power needed to simulate a quantum system in real time. In particular, that would include simulating a protein—we know that protein can fold—and facilitating the development of targeted drugs. I believe this will be one of the initial applications of quantum technology.

I'm sorry, but I don't see any potential applications in connection with quantum computing as far as electric vehicles go.

Mr. Sébastien Lemire: Thank you.

Do you favour one development model over another in the field of quantum computing?

If there were a government strategy to put forward, what would your priorities be?

Also, could we hear what you have to say about existing needs in the field?

Dr. Gilles Brassard: I would say that the most important thing is to let researchers expand their imaginations, because that's what makes real progress possible. As the physicist Einstein said:

[*English*]

“Imagination is more important than knowledge.”

[*Translation*]

The more you tell people what to do, the less progress you can make in the long run. So it's very important to let fundamental researchers choose for themselves and find out what's truly of interest. Some will be left in the dust, while others will make extraordinary discoveries. That's the only way to make serious progress, to make the quantum leap, if I can put it that way, as opposed to just developing the technology in small steps.

Mr. Sébastien Lemire: The Quebec government has announced plans to invest heavily in research and development, and has designated two key innovation zones, one in Bromont and the other in Sherbrooke. The Ontario government has done the same thing in that province, and several announcements have been made about this elsewhere in Canada.

Do you get the impression that money is being sprinkled all over the place and that it should instead be spent on certain aspects of quantum computing? We are talking about a $360 million investment over the next seven years.

You've been in this field for a long time. Do you feel this is an appropriate way to support the development of the industry?

Dr. Gilles Brassard: It depends on what you want to do. You may want to either develop a quantum computer or you may want to develop a quantum Internet, which another speaker mentioned. A quantum Internet would connect all countries, even the whole Earth, to be linked by a quantum network in the same way as the Internet today. If we're going to be able to do that, it's going to take a lot of resources, and it has to be coordinated—although that goes a little bit against what I was saying earlier. We have to have targeted projects and allocate a lot of resources to them.

At the same time, we also need to give some more resources to basic researchers like me, who are not connected to industry, so that they can continue their research and, with a little luck, make some fundamental discoveries. It's necessary to play both sides at the same time.

● (1625)

Mr. Sébastien Lemire: Last week, Dr. Simmons warned us to prepare for a quantum revolution. According to the government, quantum cryptography will be able to break current cryptographic mechanisms.

Do you think our industry is preparing adequately?

What are the challenges facing companies, particularly private companies, as a result of the arrival of new technologies?

Dr. Gilles Brassard: First, there is a small misinterpretation because quantum cryptography does not in any way serve to break the cryptographic mechanisms currently in use. Quantum cryptography provides an alternative, which is unquestionably secure, as has been demonstrated.

That said, conventional cryptography and quantum cryptography can be used not against each other, but together toward the same goal, which is the protection of privacy and confidentiality.

The danger to conventional cryptography is the quantum computer, not quantum cryptography. We hope that no one knows how to build it, or at least that there isn't one that's already working. However, since the 1990s, we have known how it could be used to break cryptographic systems underlying Internet security or pseudo-security today.

Mr. Sébastien Lemire: This is a little outside of my comfort zone, but I'll ask you one last question.

When do you think this computer will be built?

Dr. Gilles Brassard: As I said, we can't know. It's really

[*English*]

a guessing game.

[*Translation*]

The fear is that it will be built within 10 years. It's not guaranteed, but there's a good chance it will be, and 10 years from now is tomorrow.

Mr. Sébastien Lemire: I note that you used the word “fear”.

Thank you very much, Dr. Brassard.

The Chair: Thank you, Dr. Brassard and Mr. Lemire.

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

[*English*]

Mr. Brian Masse (Windsor West, NDP): Thank you, Mr. Chair, and thank you to our witnesses.

I'll start with Mr. Brassard and then move to other witnesses to get their input as well.

I am curious about cybersecurity. Currently, we see some companies and even some public institutions paying out ransoms for material, and we have a lack of laws related to that. You don't even have to disclose your hacking and payments and so forth.

I want to get a general sense of that field and how that might change. I know it's a little more theatrical, but perhaps I can get that. Other witnesses should please jump in soon after Mr. Brassard. I am curious about this. Cybersecurity has been something I've been pushing, along with fraud and a number of different things.

Please, Mr. Brassard, can you start the conversation on that?

Dr. Gilles Brassard: Since I'm a theoretician, I'm very comfortable with your question.

The short answer is that what I talked about at length, this “harvest now and decrypt later” strategy, is not a threat to ransomware, because to do ransomware, you need to do it today. It is not as if, in 10 years, when you will be able to decrypt messages sent today, that you can go back and ransom people who have moved on to something else already.

To ransom, you really need to be able—today on the spot—to decrypt and then get information that allows you to blackmail or what have you. This would require quantum computers being available already. If there is not one, then this is not a danger at the moment, but when it becomes available it will be a danger.

Mr. Brian Masse: Does anyone else have any comment on cybersecurity?

Dr. Shohini Ghose: If I may, I can jump in. I'll say, maybe in addition to what Professor Brassard said, that a lot of information that is current will not be vulnerable to ransomware, but it could be that there's historical data or something in somebody's past that needs to be kept safe, as perhaps it will impact their current role or current credibility and that would be something that would be vulnerable to ransom.

More generally, I just wanted to point out that, with the race to protect all of our current information and our past information, that's something that is.... It's not really a race between countries, because either we're all winners and we protect everything or we're all losers. It's kind of like vaccinations. You can't just rely on protecting or creating quantum-safe data security for Canada because Canadian banks, for example, have transactions outside of Canada. Any security system is only as strong as its weakest link. I think that's an important piece to keep in mind.

● (1630)

Mr. Brian Masse: That is an important piece. Are there any international efforts working together on that? We're just touching the surface here right now, and we have been asking some of our guests about international co-operative efforts. I'm just curious if there is anything going on in that field. I can just see the vulnerability here if what you're saying is true, which I do believe.

Dr. Shohini Ghose: Is that question for me?

Mr. Brian Masse: Yes. I'm sorry. I should have been more specific.

Dr. Shohini Ghose: As far as I know, there isn't a coordinated, large-scale international effort. I think there is collaboration at the research level for sure, but not at any kind of a national strategy or at the industrial level.

Dr. Gilles Brassard: I agree.

Mr. Brian Masse: Thank you.

I'll ask this really quickly. I don't know who's taking advantage of SR and ED tax credits. We had a good response from the last panel on that. If you are, can we get an opinion as to whether they're working or not in terms of application? Is anybody taking advantage of those research tax credits?

No. I just wanted to make sure.

If I can move to Ms. Hall then, one of the things that we've also been identifying is bringing in young people and retaining them. I think Mr. Gagnon-Gordillo mentioned this as well. What can we do to continue to have people come through our systems to stay and not be plucked from Canada as we grow quantum computing and its workplace here in Canada?

Dr. Kimberley Hall: I have a suggestion that I really think we should consider. This suggestion was actually made by somebody last week, but I do think we need to develop a pan-Canada training program that involves collaboration among the institutions and collaboration with industry. I think CDL, the Creative Destruction Lab, was mentioned as a possible centre for directing such a thing, but I think that this could really help to bring more people here.

In terms of keeping them here, I've had several international students that have been successful in staying. There's been a lot of talk about difficulty in that, but I'm not sure. My experience thus far is that as long as somebody can get a job they seem to be able to stay.

Recruiting and retaining people is one of our key challenges. I think the universities are largely competing in this space now, and we need to work together. I really feel like if we had a training program that was beyond student exchanges, beyond internships, with courses that people could give from different institutions and that could rotate, for example, and with an actual accreditation that would attract people from outside, that would be an excellent addition.

[*Translation*]

The Chair: Thank you very much, Dr. Hall.

Mr. Généreux, you have the floor for five minutes.

Mr. Bernard Généreux (Montmagny—L'Islet—Kamouraska—Rivière-du-Loup, CPC): Thank you, Mr. Chair.

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

Dr. Ghose, last week, Dr. Simmons made some rather alarming comments before the committee, which shocked me. She also talked about the possibility of Canada having an independent panel of experts to advise the government on how best to invest in sectors with development potential in Canada. This type of committee also exists in other countries.

What's your opinion about that?

If such a committee was created, what would its composition be?

Dr. Gilles Brassard: May I answer?

Mr. Bernard Généreux: Yes, but I'd like to hear from Dr. Ghose first.

[*English*]

Dr. Shohini Ghose: Thank you for the question. I think that's a really important piece of developing our national strategy. I think it was a strong message that also came out in the consultations that happened already to try to create a plan for the future.

So yes, I am a strong supporter of the advisory board idea. I feel that the composition has to include expertise not just on the technology aspect of it and not just on the quantum information processing or scientific aspect of it. We also need experts from, for example, cybersecurity and industries that will be impacted, such as health care and of course finance and energy.

Beyond that, make sure that the composition is not business as usual. Unfortunately, as I've already mentioned, we often find that we don't get a diverse enough group around the table. I feel that the scientific advisory board should be something that takes that into account.

● (1635)

[*Translation*]

Mr. Bernard Généreux: Thank you very much, Dr. Ghose.

Mr. Gagnon-Gordillo, you said earlier that you are part of a major industrial cluster in the Sherbrooke region with respect to the development of quantum computing in Quebec. You also said that you were about to buy a quantum computer.

I would ask you to clarify this for me, because, on the one hand, we're being told that the quantum computer needs to be invented, but on the other hand, you're going to buy one because it exists. I'm a little confused.

Could you clarify that?

Dr. Brassard, I'd like to hear your observations after that.

Mr. Olivier Gagnon-Gordillo: When people refer to quantum computers, many talk about buying them, while others talk about simulation. In fact, what is being bought isn't so much a computer as access to a prototype quantum computer.

The one we're talking about is IBM's EAGLE System One, which has a 127-qubit processor. What you're buying is specialized access to that computer, which allows more access to be able to test algorithms. Subsequently, access to the IBM quantum space, which already exists at the Université de Sherbrooke, will continue to exist. Access to this space is not specialized, but shared, so even if IBM comes out with new models, we will continue to have that access.

Again, when people talk about a quantum computer, they're talking about a prototype.

I'll now turn it over to Dr. Brassard, who will be able to round out my answer.

Dr. Gilles Brassard: Thank you, Mr. Gagnon-Gordillo.

That's very good, what you just said.

Yes, there are prototypes at the moment that we can buy. We can also rent specialized access time. These prototypes work with a relatively small number of qubits, or quantum bits, for example 127 qubits. If we really want to apply algorithms on a large scale, for example, to break contemporary cryptographies, we need a lot more qubits. To our knowledge, no quantum computer currently allows us to do that, but there are prototypes that allow us to start experimenting and to see how well it works on a small scale.

We can rent a prototype from IBM, but there is also a Montreal company, Anyon Systems, that manufactures quantum computers. We can even place an order, and a quantum computer will be delivered within the next year or two. So we can buy a Quebec-made quantum computer right now.

Mr. Bernard Généreux: Dr. Brassard, do you share Dr. Simmons's concern about the urgent need to act that we are currently seeing in Canada?

Dr. Gilles Brassard: I think what I've said so far has been very clear; the answer is yes. It's a catastrophe in the making. If we don't do something, it will be the apocalypse.

The Chair: Thank you very much.

Ms. Lapointe, you have five minutes.

Ms. Viviane Lapointe (Sudbury, Lib.): Thank you, Mr. Chair.

[*English*]

My questions are for Dr. Ghose.

I'll have you know I did watch your TED talk and I know that I will never flip a coin to settle a matter with a quantum computer, ever.

I want to thank you for all the work you do in supporting women in science. From your experience, I'd like to hear more about your work in implementing equity, diversity and inclusion initiatives.

Why is this lens important, and does it incorporate the principles of GBA+ analysis in the work that you do?

● (1640)

Dr. Shohini Ghose: I'll start with the reason it's important. There are many reasons. Whether you want to talk about social justice or economic progress, the point is if we wanted to really have an edge in quantum or even other areas of STEM, AI, or many other areas where there's an under-representation of women, we are just not using the full talent that is out there.

What we know already from studies is there's no actual fundamental reason why women cannot contribute to these areas. In fact, they have been, but they just haven't had the equal opportunities or resources. From that perspective, it's just not very efficient or optimal to be only tapping into part of the whole workforce. We're losing out on ideas. We're losing out on economic progress. Of course, this is a matter of social justice as well. Those are reasons why this is an important issue.

Going forward with GBA+, I know that NSERC, for example, in all of its funding applications now insists on that. There are also some additional measures in place for training for highly qualified personnel, as they're called, which are basically students and postdocs, where any kind of funding has to include some level of effort towards being more inclusive. However, these, I believe, are still at a level which are token. We need to be much more proactive about this, because the fact is the needle has not moved in over a decade.

What we are trying to advocate for is a much more structured and scientific approach, which is about applying full frameworks, setting the goals, incentivizing this kind of work, providing value for it, celebrating it and attaching dollars to it. In the end, this is just like every other goal: it needs resources and dollars.

Ms. Viviane Lapointe: I agree.

In your expert opinion, what steps need to be taken to ensure the national quantum strategy is inclusive? What would be the potential consequences to the quantum technology sector in Canada if EDI is not applied?

Dr. Shohini Ghose: I think, to answer the second part of your question first, when we don't include EDI, the effects have already been clear. For example, you could look at AI where there's all these unintentional consequences where we have built-in bias into all of these training systems. That's a clear example.

There's another test everybody could do. Go online and type in “famous physicists” on Google and just see what you get. You'll see that Google has learned all of our history of biases about who can be a scientist. Even at that fundamental level there's a huge negative impact. That answers what could happen in the quantum sector as well.

Similarly, if you look at the executive boards of most of the start-up companies in quantum today, already you're seeing a very skewed representation. This is going to impact what these technologies are going to be used for, who will get access and who will be making decisions about what these technologies will be used for. In health care, for example, are we going to be focused on women's health or not? Are we going to tailor these technologies towards all of the population? These are all questions that arise.

I know I have limited time, so I'm happy to discuss this more or submit something in writing, but I'll stop there for now.

Ms. Viviane Lapointe: Would you say that changing the structures of the workplace, along with recruitment and retention of talent to the quantum sector and STEM in general is needed, instead of just trying to change people as part of the solution?

Dr. Shohini Ghose: I think a whole spectrum of actions need to be taken, starting with recruitment and retention for sure, and also, as you said, building a classroom and a workplace environment that is inclusive.

There's lots of research about how this can be done. We need to bring experts to the table who have already provided recommendations on how, for example, to build an inclusive classroom. With my own team, for example, I find I often have students and researchers who want to work with me because they value this. There is a clear benefit to creating an environment where people feel heard and seen.

I think you're right that there are many different approaches. We need both policy level kinds of actions as well as changes in individual teams, cultures, classrooms and research environments.

● (1645)

Ms. Viviane Lapointe: Thank you.

[*Translation*]

The Chair: Thank you very much, Dr. Ghose.

Mr. Lemire, you have the floor now for two and a half minutes.

Mr. Sébastien Lemire: Thank you, Mr. Chair.

Ms. Ippersiel, I'd like to know more about PRIMA Québec's vision. Your organization represents an industry that deserves to be fully recognized in the advanced materials sector. There seems to be a growing number of companies that gravitate to PRIMA Québec. The contribution of these companies to the advanced materials sector is more than $14 billion to the advanced, a sum that is obviously significant.

Do you think there is a role for the federal government to play in attracting more private investment in research and development, particularly in Quebec?

What do you think needs to be done?

Ms. Marie-Pierre Ippersiel: Thank you for the question, Mr. Lemire.

I see that you've read our documents carefully.

In Quebec, 450 companies—mainly SMEs—are associated with the advanced materials sector. That's 45,000 jobs. I'm talking about Quebec, but that gives you an idea of what that means across Canada.

Remember that the advanced materials sector is intersectional. There are applications in various sectors, whether it be the environment, chemistry, transport or energy. In short, it's very broad.

How can the Government of Canada, or a provincial government, increase private investment?

PRIMA Québec's approach is to promote collaborative innovation projects. It must be understood that a project will always receive funding from the Government of Quebec. It can also obtain funding from the Natural Sciences and Engineering Research Council of Canada, or NSERC. The company or companies also have to put money into the project. Thanks to this collaborative innovation formula, the domestic spending on research and development that businesses put forward increase this figure, which—as you are probably aware—has been trending downwards in recent years.

More recognition of the strategic role of advanced materials could most certainly help. What we often notice is that we will think in terms of finished products. Let me give you the example of clean technologies. Several of them could not exist without the use of advanced materials. Think of sensors, membranes and filters. I think that recognition is very important.

As I mentioned in my opening remarks, advanced materials have an important role to play in the quantum sector, in equipment production, in particular. Quantum materials have quite unusual properties. One example is superconductors, which allow no loss of thermal energy. I think that's very important.

I believe that advanced materials should be promoted more by governments, whether federal or provincial, but also in the various policies. Whether it's the national quantum strategy, the hydrogen strategy, or all approaches to net-zero emissions or climate change, advanced materials have a role to play.

The Chair: Thank you very much, Ms. Ippersiel.

Mr. Masse, the floor is yours for two and a half minutes.

[*English*]

Mr. Brian Masse: Thank you, Mr. Chair.

Maybe I can get Mr. Chong involved in the conversation here.

With regard to quantum computing and artificial intelligence, can you give some practical examples of what people should expect in terms of progress on this?

I think that's part of the problem here. When I talk about the telecom industry, I often talk about the key of getting the spectrum auction under proper policy. People's eyes glaze over. They go to sleep, they don't understand and that's the end of the conversation.

Can you give us a little bit more of a taste of what this means for people's practical lives and perhaps their professions?

Dr. Jaron Chong: Yes, sure. Again, we constantly talk about the idea of acceleration. I think the technical term of NP-hard has been brought up a few times as well. The reason that we have such a difficult time communicating this computational part from an everyday perspective is that you really need to be almost on the front lines of development and training to understand how much time and energy it actually entails.

We can make the metaphor, for example, recently with COVID-19 vaccination, when you read those stories of Pfizer and AstraZeneca or any of the drugs that have been developed over there, as well. Some of those mRNA platforms were able to generate candidate molecules in the order of about 48 hours to 72 hours. Yet, if you look at our recent experience with the vaccine rollout, as well, that was on the order of months to years. A lot of that was spent in the validation phase of things.

For any of you who are not familiar with molecular or drug development, the idea that you could have a candidate molecule ready for potential trials within 48 hours is extremely unusual. If you look at the history of vaccines previously, we were always on the order of years. You can look historically at polio for example and at how long that vaccine development took. It's sort of that transformation. To many of us, from the medical establishment perspective as well, some of the developments that were done there have been extremely cutting edge in some sense.

So if I take that metaphor there of being able to develop a candidate molecule in about 48 hours for vaccination, you start applying it to nearly everything else as well. If we want to do chemical molecular testing right now, what we would ordinarily do in vivo or in vitro—meaning just on an experimental basis—takes years of development, such as for a new chemotherapy drug or molecule, and anti-microbial molecules as well. A lot of that takes a lot of coordination, effort, energy, investment by the private sector, and by the public sector as well. If you can transform that and take out this very difficult component and vastly accelerate it, the applications are going to change by quite a bit.

If I talk to voice recognition right now, I can say a trigger key word to my smartphone and start speaking to a computer there. I remember when I was in high school, as a kid, trying to get voice recognition to work on my computer. I would sit there, talk to my computer for three hours, and the accuracy would be abysmal. The idea right now that you can call out to your phone and it just automatically works all of a sudden...it was a gradual transition, but now you can actually see that application take place.

A lot of the discussion here in the committee room right now is focused on security implications, on the negative possible effects too, but that acceleration will work in both ways potentially as well. Some of those things that are taking so much time and effort to be able to do are going to be vastly accelerated, and if they are, there are going to be positive effects and negative effects. We hope to control the negatives and be able to empower the positives and make sure that they are equally representative of all the possible benefits and have Canada be part of that discussion. Some of those changes that you've seen in computing before, over the last 10 or 15 years, will hopefully, on the positive end of things, represent themselves as well, so you're going to get these massive innovations that we can hopefully harness and help many people with.

● (1650)

Dr. Gilles Brassard: I'm sorry to interrupt—

Mr. Brian Masse: That's okay.

Dr. Gilles Brassard: —I know that interrupting is not the right thing to do in your committee, but I feel I need to say something, which is that there's this myth that quantum computers are so vastly more powerful than classical computers that they can solve everything, exponentially faster. That is not true. Quantum computers will solve some problems exponentially faster than classical computers—for instance, if you want to factor numbers and break cryptography, but for other problems, in particular NP-hard problems, there is strong evidence that quantum computers cannot offer a significant advantage in solving NP-complete or NP-hard problems, no more than quadratic improvement, which is not to be sneezed at, but is very, very far from being exponential.

So, yes, some NP-hard problems could be solved faster with quantum computers, but not as spectacularly as other problems like those that allow us to break cryptography. It's not a uniform speed up for all problems when you have a quantum computer. For some problems, yes; for some others, no.

The Chair: Thank you, Mr. Brassard. We appreciate your comments.

I'll now move to Mr. Kram, for five minutes.

Mr. Michael Kram (Regina—Wascana, CPC): Thank you, Mr. Chair. I'll be mindful with my time, if I don't have that much leeway, apparently.

Dr. Brassard, some of your statements have really caught my attention. You said that if we don't take the appropriate steps, all of the cryptographic infrastructure will collapse and this is a disaster waiting to happen and even the apocalypse, if I heard you correctly.

Dr. Gilles Brassard: I said that, yes.

Voices: Oh, oh!

Mr. Michael Kram: Okay. I just want to make sure I understand. Let's say we take absolutely zero precautions over the next decade or two. What does that apocalypse look like?

Dr. Gilles Brassard: Well, it means that if nothing changes, then not only is the past an open book when a quantum computer becomes available...and as I said, there is nothing you can do to prevent that. It's gone. The past is gone. Forget about it. But if you take no action now, then in 10 years, whatever would have been sent so-called confidentially in the next 10 years will also become an open book. That's what I mean when I say that you cannot save the past but you can try to save the future.

Now, is it an apocalypse? It depends. For some things that are sent under the cover of confidentiality, if they are revealed in 10 years, nobody will care. If your credit card number becomes open in 10 years but you don't use it anymore, who cares? However, you might care to keep your medical history secret for the rest of your life. If you send anything that has to do with your medical history, and you care to have it secret for the rest of your life, forget it.

Of course, even more importantly, if national security data or whatever is sent without more protection, then yes, maybe it could be an apocalypse, depending on who the bad guys are who will use it whenever it becomes an open book.

● (1655)

Mr. Michael Kram: Let's pick up on that. If you were the special adviser to the Minister of National Defence and your objective was to just make sure that the army, the navy and the air force could communicate securely, what recommendations would you make?

Dr. Gilles Brassard: There are two answers. One is to use quantum cryptography, which is, again, provably unconditionally secure but requires infrastructure that may not be available for these applications.

The other is to use different purely classical systems that are currently being developed. Some of them are in fact fully developed but are still under scrutiny to assess their security. There is a very significant effort at NIST in the United States to try to standardize so-called post-quantum cryptography. A large number of proposals were sent to NIST from all around the world, and then there were several rounds where....

It was an open thing. It was totally open to the whole community. People submitted their proposal to NIST. All of these proposals were open. Other people, much of the same people, were taking a shot at other people's proposals, so many of them were shut down. There are still some surviving. NIST is expected at some point to make a recommendation not of one winner, as they did for AES, but in terms of “here are a few that we think look pretty good”. Again, that's knowing that there is absolutely no hope to ever prove security for these purely classical systems.

When NIST makes its recommendation of what to use, then the question becomes whether we just want to follow the recommendation given by a foreign government, even though friendly, or whether we want to have, as I think we should, more Canadian expertise. We should not take NIST's recommendation at face value and use that immediately. It would also be assessed at a Canadian scale.

But if it's urgent, I mean, still, it's not because NIST has not yet given its recommendations that security is not needed today. I guess the best thing to do is what Professor Simmons said, which is to use several of them. We don't know which ones are secure. Maybe none of them are secure. But if you use many of them for really high-security applications and use many of them to establish secret keys, and then you combine these keys in a secure way, which we know how to do, then the resulting key will be as secure as the strongest of these systems. Here's an unusual case where the security of the whole is as secure as the strongest, not the weakest, link, which is very comforting.

Now, you cannot do that on the Internet for the average person. It would take way too much time for a normal transaction. But for a national security application, that might be the way to go at the moment, until we have a better idea about which of these are more secure, really, and should be used.

At the moment, that's the best we can do—combined with quantum cryptography, if you can afford it, and if you have the infrastructure to do that.

The Chair: Thank you very much, MP Kram and Mr. Brassard.

We'll move to Mr. Dong for five minutes.

Mr. Han Dong (Don Valley North, Lib.): Thank you very much, Chair.

First, I want to say thank you to all the witnesses. As we learn more about quantum computing from the past meetings, I see a significant improvement in quality of questions and quality of testimony. We're learning even more today.

Before I forget, I wholeheartedly agree with Dr. Hall's point on a shared national training program.

On that point, Dr. Ghose, I think you said that you are currently teaching undergrads about quantum computing. Can you later submit to the committee some of the details of your program, like the curriculum and enrolment interest that you're seeing at your institution? That would be very helpful.

You also talked briefly about how there has been a lot of attention and discussion on AI ethics, but not enough on quantum ethics. Can you expand a little bit on that? What is the similarity or uniqueness of quantum ethics?

● (1700)

Dr. Shohini Ghose: Yes, sure.

Firstly, I'm happy to share my course details.

Secondly, a lot of the questions for AI ethics, technology ethics and the use of technology in general would of course also apply to quantum. I think that's important to keep in mind.

Additionally, I think that at this stage, quantum offers new kinds of potential applications that we perhaps haven't even dreamed of. We really need to have some kind of a structure to be able to not get taken aback by what will come in the future. We need to have a system in place to understand what we need to build into structures of how the technology is rolled out.

There's a second piece, which is on the security side. In fact, as Professor Brassard mentioned, quantum key distribution offers provably unhackable security. Let's say that at some point that happens and everybody has completely, one hundred per cent secure encryption. That means bad actors have that, too. I feel that there are a lot of questions around regulation and policies of how this kind of technology is used and what is acceptable and what is not.

Those are questions we need to really be careful of.

Mr. Han Dong: I saw Dr. Brassard shake his head.

Do you want to share your comments with us?

Dr. Gilles Brassard: Yes. This is another myth that I want to debunk about security versus confidentiality, where security means law enforcement.

This is a false debate. It's security against security, by which I mean that citizens have a right to privacy that outweighs almost everything else. I said almost.

It's not true that police or law enforcement use so much decryption to catch criminals. They use what you would call metadata, which is who talks to whom, much more than what is said. This is not protected by regular encryption. This intelligence is available even when the communication is encrypted and even it cannot be decrypted by law enforcement.

I am a very strong advocate of privacy as a fundamental right for citizens. Yes, in some cases it could lead to a bad person not being caught, but it's a price to pay for something that is so much more important, which is privacy.

Mr. Han Dong: I think this is all very good advice for legislators. If any panellists have more advice to add on quantum ethics that's beneficial to legislators, please send it to us afterwards.

Dr. Brassard, since I have you at the mike, I have a very specific question.

What's your opinion on what quantum computing will do to the cryptocurrency field? We've seen quite a bit of hype in that field.

Dr. Gilles Brassard: I think the two worst abominations of computer science this century have been Facebook and Bitcoin. That's just my personal opinion.

When I say Bitcoin, I don't mean that I have anything against anonymous cash, which I think can be used for bad things, but also for good things. That's not the debate. The debate is how much Bitcoin has wasted resources, like farms—

Mr. Han Dong: Bitcoin or cryptocurrencies will still exist after the—

Dr. Gilles Brassard: Sorry. To answer your question, some cryptocurrencies, like bitcoin, as it currently stands, will completely bite the dust as soon as a quantum computer is available, for two reasons.

One is that it uses, fundamentally, digital signatures, which as such is not necessarily broken by quantum computing if it's implemented properly, but it uses specifically an RSA-type digital signature, if I'm not mistaken. That is broken with a quantum computer. The entire so-called blockchain will be broken as soon as a quantum computer is available, when the root is protected by RSA signatures. That's one thing.

The other thing is that cryptocurrencies are based on the notion of proof of work. They claim that in order to mine coins, you need to work for so much time. They claim there is a fundamental obligation to work for so much time or do so much work in order to mine a new coin. This is not true because quantum computing would allow us to mine coins much more efficiently, although only quadratically more efficiently. It's back to the NP-hard question. Still, quantum computers would break the basic assumption of the proof of work that is behind most cryptocurrencies.

This doesn't mean that cryptocurrencies are dead. It means the way they are currently implemented will completely bite the dust when a quantum computer becomes available.

● (1705)

Mr. Han Dong: Thank you.

[*Translation*]

The Chair: Thank you very much.

Go ahead, Mr. Deltell.

Mr. Gérard Deltell (Louis-Saint-Laurent, CPC): Thank you very much, Mr. Chair.

Ladies and gentlemen, welcome to our committee. This is an exceptional panel of witnesses. Thank you very much for your input, and rest assured that your testimony is very helpful to our study.

Dr. Brassard, I'd like to talk to a little bit about the Montreal company you mentioned earlier, which can build quantum computers.

Can you tell us more about that without, of course, giving away any secrets?

Dr. Gilles Brassard: First of all, I wouldn't have any secrets to give away, because I don't have any privileged information about it. All I know is that the company is called Anyon Systems, and its slogan is *We make quantum computers*.

I've had the opportunity a few times to listen to presentations by representatives of this company, but I don't know them personally. All I can say about them is that they seem serious. However, I haven't tried this company's products, so I can't say whether they're any good or not.

However, they seem quite serious about building quantum computers on a small scale, at least for now, but building enough to do interesting experiments.

Mr. Gérard Deltell: Dr. Brassard, I think I heard you say earlier that you had already rented prototypes for experiments or that prototypes could be rented.

Did I understand correctly?

Dr. Gilles Brassard: I have never rented anything like this. I personally have never experimented with an actual quantum computer. I know I could if I wanted to, but I never have.

It is possible to rent time on a quantum machine from companies such as IBM and Rigetti. Several U.S. companies allow users to rent time on a quantum machine. For research purposes, user time is even free, to some extent, for smaller operations.

I don't know if Anyon Systems' first quantum computer is already available. I do know that the company is working on it and that its planning, in the next year or two at the most, to have quantum computers available for purchase. In fact, you can already place an order.

To be honest, I'm not familiar enough with this company to be able to talk about it more specifically.

Mr. Gérard Deltell: I'd like to come back to the issues of security, privacy and confidentiality. You explained the difference between these three aspects very well.

You said that in 10 years, quantum computers could allow people to access information that is currently protected, either through our emails or websites.

Isn't there a way to—

Dr. Gilles Brassard: They could have retroactive access.

Mr. Gérard Deltell: If these computers are so powerful, can we ensure that the safeguards are as powerful as they are?

Dr. Gilles Brassard: This is absolutely impossible. The important thing to understand is that it's too late. The information I'm talking about has already been stored by future wrongdoers. I'm not just talking about bad guys, because it could also be police.

In any event, the information I'm talking about has been circulated on the Internet and has already been stored. There's nothing to stop anybody who has a quantum computer and has stored this information in the past from just bringing it out of mothballs, if I can put it that way, and decrypting it retroactively.

You can't save information that has already been intercepted. You can only try to save future information. It's not a question of inventing technology to produce information. What we're talking about here is information that wasn't properly produced and that was circulated. If it has been saved, there's nothing more to do.

● (1710)

Mr. Gérard Deltell: Thank you, Dr. Brassard.

Ms. Ippersiel, you said that there were eight quantum projects under way in Quebec.

Without giving away any secrets, could you give us an example of what is being done and talk about the funding required and the collaboration between the private and public sectors, among other things?

Ms. Marie-Pierre Ippersiel: I can give you an example of a non-confidential project between SBQuantum, which specializes in magnetometer technologies, and Solmax, a company operating in the environmental sector. The aim of the project is to use quantum magnetometer technologies to increase the reliability of fault detection in various buried structures that may contain contaminants. I think it's a great project, with the Quebec government investing $747,000 out of a total budget of $1.5 million. The two companies have also invested in this project. So it's a great example of a project funded through a call for projects from the Government of Quebec.

Calls for projects are very interesting because there are different parts to them. It is possible to support a start-up, an SME, a project involving two companies like the one I just mentioned, or a project involving one or more companies in the research community.

I know it's not very attractive, but I have a fairly large list of project titles here. It includes a project to develop diamond synthesis processes for applications in quantum technology. This is always done at room temperature, as it has been understood that diamond can be a quantum material.

So these are the kinds of projects we have. I invite you to visit the Québec Quantique website. As Mr. Gagnon-Gordillo knows very well, for each of the projects funded, particularly between two companies or between research centres and companies, there is a kind of sheet that explains the objective, the problem to be solved and the amounts invested.

For some of the projects, there is sometimes a counterpart, beyond the Quebec government's investment, that is, top-up funding from granting agencies such as NSERC.

The Chair: Thank you, Ms. Ippersiel.

Mr. Fillmore, you have five minutes.

[*English*]

Mr. Andy Fillmore (Halifax, Lib.): Thanks, Chair.

Also, thanks to the witnesses today. You're painting an increasingly legible picture of a very complex landscape, and we're very grateful for that.

We've heard a lot about security, and in rather dire tones at times, and I'd like to change that a bit.

I want to come to you, Dr. Hall. It's nice to see you. I don't know if I'm your MP, but I am Dalhousie University's MP and it's very nice to see you with us today.

I went to your research website before the meeting today and was moved by the young people you are working with and how many there are, by their smiles and by the interest that is clear in the photographs you've posted there. Obviously, their imagination has been captured by something. They're thinking of the future. They're working towards something. It made me think of the 1964 New York World's Fair, where GE had “The World of Tomorrow”, the vision of tomorrow, on how electricity and gasoline and cars were going to change the world.

I wonder if we could turn to a more optimistic outlook. As you said, Dr. Hall, maybe it's not necessary that Canadians understand the technology, but they should understand why it's important. Can we talk with the panellists a bit about finding your inner future and where is all of this going, and how quantum computing or hybrid solvers are going to make our lives better?

Dr. Kimberley Hall: I do want to say that in the area of recruiting students and exciting students about this field, it's just not that difficult. I must say that we have some advantage over some other fields in the fact that quantum mechanics is so intrinsically interesting that I find the spectrum of students who are interested in this area varies from those who want to change the world, which this can do, to those who just find quantum mechanics interesting. Because you have that full spectrum of applied to extremely basic, I find this is an area in which it's really not that hard to excite students.

It's extremely important that we do excite students to go into this area, and it is important that we collaborate together as institutions to make sure that these people stay, as has been discussed many times. It's particularly important to reach people outside of the students who are already interested.

I made the point during my speech that some of the shorter-term applications, like sensing, are a lot easier to explain than NP-hard problems. I have watched all of these meetings and it is taking a lot of meetings to convey that quantum cryptography has to be the future of security. I do think there tends to be a longer-term perspective taken whenever somebody is trying to solve quantum computing, but if you can very easily solve quantum sensing, this is an area on which people should focus in terms of trying to excite people about this area.

● (1715)

Mr. Andy Fillmore: If you were going into a grade 8 science classroom—maybe you visit such classrooms—and if you were trying to recruit people to think about a career to follow in your footsteps, what would you say to excite them about the future? How would you sell quantum computing to them?

Dr. Kimberley Hall: I would sell that it's a privilege to have a job where you can think about things like deep mathematics and still do something that's useful for a possible application. This can appeal to people who vary from the small academic people who just want to play with stuff to people who actually want to change the world.

A lot of today's youth want to change the world, so it is critical to explain how quantum can change the world as part of the pitch. A lot of people are interested in energy for very good reasons, but quantum can change the world just as much as developing solar cell material can change the world. You can use a quantum computer to design solar cell material and you can use quantum spectroscopy to study energy materials.

It is really important to appeal to all of the different aspects that motivate people to go into a field. Changing the world and doing cool science covers it.

Mr. Andy Fillmore: Thank you very much, Dr. Hall.

Have I any time left?

The Chair: No.

Mr. Andy Fillmore: Okay. Thank you very much.

[*Translation*]

The Chair: Thank you.

Mr. Lemire, you have the floor for two and a half minutes.

Mr. Sébastien Lemire: Thank you, Mr. Chair.

Mr. Gagnon-Gordillo, thank you for being with us today.

In November, Luc Sirois, Quebec's chief innovation officer, gave an interview to *Québec Science* magazine, during which he said that our companies are struggling to make investments in research and development.

Similar comments were made to this committee, including by Alain Lamarre in the study on the capacity to produce COVID-19 vaccines, and by Alexandre Blais in this study.

Do you think the federal government can play a role in attracting more private investment in research and development, particularly in Quebec?

What do you think needs to be done?

Mr. Olivier Gagnon-Gordillo: That's a very broad question. I'll do my best to answer, but I'm not making any promises.

In terms of investments, we can look to the Business Development Bank of Canada, or BDC, a Crown corporation. Through its deep tech venture fund, BDC provides $200 million in funding. The quantum sector can grab a lot of that funding.

The situation in Canada has long been recognized. A small amount of pre-seed and seed money is available to early-stage businesses. This helps to launch projects, going from academic research to business start-up. Things start off well, but as soon as a business wants to move from the start-up to scale-up phase, the funding dries up. That is usually when foreign investors, mainly from the U.S., step in with venture capital and the company moves out of Canada.

Considerable support is needed on that front, especially beyond the series A round, when significantly larger venture capital investments are needed, in other words, series B and C. Those investments are necessary, and the federal government can certainly play a role.

Another consideration is how long the process takes for quantum technologies. Previously, obtaining venture capital would often take seven to 10 years, especially for cloud-based companies such as Facebook and Airbnb. In the case of quantum technologies, it's closer to 15 years. Developing a company in the quantum sector takes a lot longer and requires more patience when it comes to investment types. That is a factor. A bit more support from the federal government would make a big difference.

● (1720)

Mr. Sébastien Lemire: I have another question for you.

The Chair: Sorry, Mr. Lemire, but your time is up.

We now go to Mr. Masse for two and a half minutes.

[*English*]

Mr. Brian Masse: Thank you, Mr. Chair.

Very quickly to Mr. Brassard, are there a couple of countries out there that we should be aligning or working with? I'm interested to know who we should be focusing on. Is it the United States? Is it Australia? Is it Europe?

What do we do, as a country, in prioritizing who to work with?

Dr. Gilles Brassard: That's a difficult question. The United States is our ally, of course, and they do good things—good research, good development. I don't think we can pretend they're not there. Yes, we should collaborate with them, not that we had a choice.

Europe, as a whole, has a concerted effort to develop both quantum cryptography and a quantum Internet. It's a very concerted effort. It's going really well over there, and we would only benefit from collaborating with them.

Japan is also doing really good work, so it's take your pick. There's no single answer.

Mr. Brian Masse: Ms. Hall, you mentioned something like a pan-Canadian degree on quantum computing. If we were able to concisely get some co-operation among Canadian universities, do you think it would be palatable enough, instead of having each university fight for a slice or a specialty?

Is that what you're proposing? Is it more of a comprehensive thing that would bring everybody together to have a more robust, centralized or specifically scoped approach?

Dr. Kimberley Hall: I absolutely think everybody should come together and coordinate. That would benefit everybody, because we would stop competing for graduate students and start collaborating to include them. It would also serve to help in terms of diversity and inclusion, because you could then reach students all across the country who would be able to access this training program.

Having it be accredited is important to bring people in from outside. That is something that easily hooks students, if they know that they're going to get something at the end. There are probably barriers to this, because I don't know how easy it will be to have courses offered at UBC and courses offered at Dalhousie that can be taken by other people, but in this electronic age in which we're all very used to taking courses online, it should be possible.

Mr. Brian Masse: I did that with the disability community, instead of fighting, and it's a really interesting concept.

Thank you, Mr. Chair.

The Chair: Thank you very much.

Go ahead, Madam Gray.

Mrs. Tracy Gray: Thank you, Mr. Chair.

I have a couple of questions.

Dr. Chong, do you know if hospitals and medical organizations are updating their privacy policies to prepare for quantum computing? If you're not aware of that, do you have any recommendations?

Dr. Jaron Chong: That's a very interesting question as well.

I have not heard of those kinds of updates. Everyone's thinking about this whole notion of a Q-day that will occur at one point, when all of our public key encryption systems will be disabled or compromised in some manner, but we haven't seen that timeline, or even a potential exploit yet. This is a very far-reaching cutting edge, but I don't see that there is a policy there.

I think that the evolution of health care information or information IT would parallel the financial systems quite closely. When you see the beginnings, just in the same way that public key encryption and SSL were incorporated for online banking.... I remember a time when you did not do online banking. You didn't have a smart phone. You would call a fax number. We transitioned to a point where that was safe to perform on a computer.

I can easily imagine that those same regulations that moved for finance will also very easily apply to health care. If there is a build-up of a quantum encrypted network or any similar standards or adoptions of certain algorithms or quantum resistance, those would all move in the same way.

I'd like to see from a government or regulator perspective right now.... Once we have some indication that potential exploits are going to occur—and that certain high-risk or critical industries and fields will be, first of all, categorized as high-risk—then the regulations are synchronized between them. I think other communication industries and the IT industry are really going to benefit from that, as well, and we can all learn from the various industries together.

● (1725)

Mrs. Tracy Gray: Thank you very much.

My next question is for—

Dr. Gilles Brassard: I'm sorry to interrupt, but please allow me to answer your question as well.

Mrs. Tracy Gray: Okay, please give a really quick answer, because I have a couple of other questions.

Dr. Gilles Brassard: I'll do that. I'm sorry.

It's just that Toshiba has been very seriously working on protecting medical data with quantum cryptography. I'll stop there.

Mrs. Tracy Gray: Great. Thank you for that.

Mr. Gagnon-Gordillo, you mentioned during your intervention how Canada is having a hard time retaining students. Leger has just released a study where immigrants were asked why they would not recommend Canada to future immigrants. One of the primary key reasons was due to the cost of living here.

I just wanted to ask you what your thoughts were when you said Canada is having a hard time retaining students. The cost of living, finding housing, the cost of housing, is that playing into some of this?

Mr. Olivier Gagnon-Gordillo: I think we need to separate out it in terms of which students. If the study you're talking about is all students, then, depending on the program they study, obviously it's not the same salaries. If we're talking about in this sector normally, there would be some great salaries where the cost of living would not be an issue. In terms of retaining the talent that studies here in quantum sciences and quantum technologies, normally it would lead to careers that lead to great salaries and the cost of living, in my opinion, in Canada would not be an issue.

Mrs. Tracy Gray: Great. Thank you for that.

I have a question that anyone can respond to, so if you're interested and you have a thought on this, maybe physically raise your hand and then I can call on you.

We know the government right now is working on a quantum strategy. Are there any lessons or policies from other countries around quantum computing that is something Canada should pay attention to and replicate here in Canada? Does anyone have any thoughts on that—maybe just raise your hand—something that we would want to see in our strategy here?

Ms. Hall.

Dr. Kimberley Hall: I can say something. I think there's been some discussion about the DARPA program, and whether we should bring some kind of DARPA program to Canada. I participated in the DARPA SPiNS program years ago, so I'm somewhat familiar with the structure. I've also been a regular reviewer for DOE. I actually think that DOE challenge programs are a little bit more suitable than DARPA, in the sense that DARPA tends to have a lot of control by very few people over the process, and maybe the calls are a little bit too narrow. I very much like the challenge programs that NRC has introduced. I think these are excellent programs.

A lesson we can take from the U.S., which is different from what we're doing now, is the idea of a call for a certain topic. I think we can do that in a way that works. I think the NRC challenge programs are a good example of that working.

Mrs. Tracy Gray: Thank you, Dr. Hall. I'm out of time.

The Chair: Go ahead, Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks, Chair.

Picking up where you left off, Professor Hall, the NRC, through the challenge program, has a unique way of spending public dollars to deliver on a particular outcome and encourage competition. The proposed national strategy has a budget allocation of $360 million. Now some of that money has flowed.

This is for everyone, but let's start with you, Ms. Hall. Continuing challenge-like programs the way the NRC has begun is one way to spend those dollars. Would you have any other advice to the government in terms of how to best allocate the $360 million?

Dr. Kimberley Hall: I've sort of made this point during my speech, but the funding structure in Canada has evolved towards very large team grants, team grants like CREATE and like the CFI innovation fund. These programs are great and they have their purpose, but it's very important to note that these large team structures leave out a lot of people in Canada who are excellent scientists and just don't happen to be at the right university, for example, with a large number of people in a particular area or the critical mass. People are sometimes not included on teams because of, unfortunately, diversity and bias, which can sometimes enter into it. It's very important, if you want to fund the broad base of scientific strength in this country, that you also have open calls that are open to individuals and small teams, because these things will allow people to keep going.

● (1730)

Mr. Nathaniel Erskine-Smith: Thank you, Ms. Hall.

Professor Ghose, do you have anything to contribute in terms of how we ought to spend the $360 million over and above what Professor Hall has contributed?

Dr. Shohini Ghose: Yes, I want to agree with Professor Hall. Just adding to Alliance and CREATE and these existing NSERC programs would actually be business as usual. There is no evidence that these programs in the past have really led to including everybody who wants to contribute to this field to be able to.

I think there has to be a rethinking, a reframing, to build something that doesn't exist right now and also doesn't exist, actually, in any of these other countries, in terms of programs that really can tap into all of the potential out there. That needs some research and bringing in people around these kinds of conversations, advisers, who can talk about how to build a program that truly is inclusive. There are examples in other areas but not yet in quantum.

Mr. Nathaniel Erskine-Smith: Thank you.

Ms. Ippersiel, do you have a view of how the government can best allocate $360 million via the national strategy?

[*Translation*]

Ms. Marie-Pierre Ippersiel: I agree with what Professor Hall and Professor Ghose both said.

Of course, research is important, but the funding has to be balanced between basic research—an essential phase whose benefits do not emerge until much later—and applied research. Support for applied research is needed. It's important to make sure that issues around the adoption of quantum technologies are addressed. At the end of the day, the technology won't matter without users.

Support for the ecosystem as a whole is another key consideration. Ecosystem refers to the research community, companies, young start-ups, small and medium-sized businesses, investors, and potential users, which can be major clients.

Mr. Gagnon-Gordillo brought up the BDC and the deep tech venture fund. It's also important to support everything having to do with cutting-edge equipment.

Is the $360 million enough? When you look at what's happening elsewhere, I don't think so.

The last the thing I would draw your attention to is intellectual property. We need to find a way to effectively support intellectual property, so that research developed here can be patented and stay in the country.

[*English*]

Mr. Nathaniel Erskine-Smith: Thank you.

With the remaining time, the same question is for Mr. Gagnon-Gordillo. You were nodding your head with regard to entrepreneurship and supporting start-ups.

Could you speak to how the $360 million can be best allocated in that space?

Mr. Olivier Gagnon-Gordillo: There are a lot of funds that are also outside of that $360 million, but it's just all for research. Beyond the research, if you want to develop the ecosystem to have companies stay in Canada, there's a lot that needs to be done in terms of tech transfers and making sure there's an adoption of quantum tech in companies.

We have strong industrial sectors in Canada. Why don't we go with those strong industrial sectors? There are some that are different depending on the different provinces. In Quebec, we've identified five specific industries. We want to tackle those five industries. It's then just a matter of finding one, two, or three champions and building from there.

This could be done with all of the provinces. Working with them, we could find those early adopters that could become champions. They could then lead the way in the adoption of quantum tech, and fund those projects.

Mr. Nathaniel Erskine-Smith: I'm out of time, but it would be unfair, Dr. Brassard, to not give you an opportunity, if you have something to add.

Dr. Gilles Brassard: Thank you. I agree with all that was said, and I don't really have much to add.

Mr. Nathaniel Erskine-Smith: Thank you.

The Chair: Thank you.

Dr. Gilles Brassard: Except that I agree there's not enough money, but it's a good start.

The Chair: The witnesses have witnessed how little authority I have over time management at this committee.

I want to thank you all. This was our last meeting with witnesses, and it was a really enlightening one. It's going to help us raise awareness about quantum computing in the months ahead.

[*Translation*]

Mr. Bernard Généreux: Mr. Chair, I have one last question for Mr. Brassard.

Mr. Brassard, is teleportation technology available somewhere? Did you invent it?

Dr. Gilles Brassard: Not yet. It's going to be a while.

The Chair: If someone does invent it, that person will probably be you, Mr. Brassard. Thank you for appearing before the committee today.

Have a good rest of the afternoon.

Thank you to the witnesses and the committee members.

The meeting is adjourned.