HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

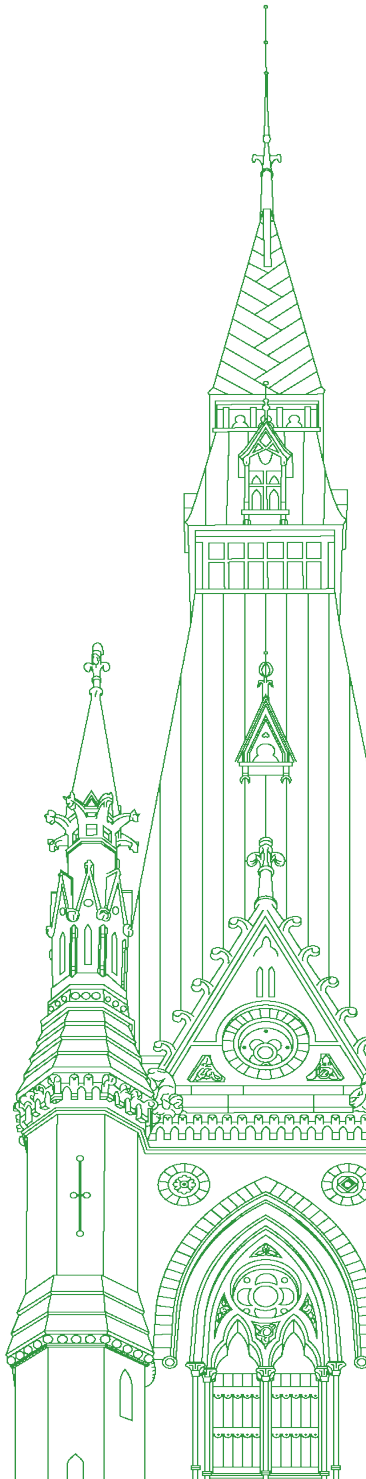
44th PARLIAMENT, 1st SESSION

Standing Committee on National Defence

EVIDENCE

NUMBER 053

Friday, March 10, 2023



Chair: The Honourable John McKay

Standing Committee on National Defence

Friday, March 10, 2023

● (0845)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Colleagues, let's call this meeting to order. It's 8:45. I see quorum. Our witnesses are in place and all sound-checked.

Colleagues, for the first hour, we'll go through the normal time frame, and then in the second hour I intend to take a few minutes at the end to pass the travel budget. Hopefully you'll use those two hours in some way or another among yourselves to arrive at an accommodation as to how this committee will travel. Maybe I live in a world of faint hope, but still....

With that, I'm going to call on Christyn Cianfarani to make her five-minute presentation. Then Mr. Callan, who is apparently online and checked, will come in by video conference.

Welcome back to the committee. We look forward to what you have to say, Ms. Cianfarani.

Ms. Christyn Cianfarani (President and Chief Executive Officer, Canadian Association of Defence and Security Industries): Good morning. Thank you again for the invitation to appear before this committee.

Today I will provide you with the perspective of the Canadian defence and security industry and the subset of companies that make up Canada's cybersecurity industry.

Canada's cybersecurity industry is world-class. According to studies carried out by ISED and StatsCan, between 2018 and 2020 the sector grew over 30% in terms of employment, R and D activity, and revenue. It's a fast-growing global sector expected to outpace traditional IT in terms of spending.

However, only 8% of the sector's revenue is derived from Canadian government contracts. The sector sells three times as much to our Five Eyes allies as it does to the Canadian government. Those numbers speak to a central challenge we face in this country when it comes to cyber. Our allies see more value in Canada's cybersecurity sector than Canada does. Something's wrong with that picture.

On one side of the coin, Canada needs to acquire more from its our own industrial base, using procurement as a policy lever to drive innovation and build scale in Canadian businesses; on the other side of the coin, Canada needs to procure at the speed of cyber. A slow procurement process is a recipe for buying out-of-date or obsolete technology. Innovation cycles in this domain are measured in months, sometimes weeks.

Resolving these issues boils down to one word: collaboration. Canada requires a much greater degree of collaboration, co-operation, knowledge sharing, and co-development between government and the private sector.

Some positive steps have been taken towards this, but we're nowhere near where we need to be. While agencies like CSE are very capable, CADSI's research has shown that our government is falling behind our allies when it comes to working with the private sector in an institutionalized way. Our allies are collaborating with industry in real time right now in Ukraine.

The Canadian government needs to establish a recurring forum for dialogue and discussion on cyber issues with all the key players—industry, DND, CAF, CSE, CCCS, GAC and Public Safety—at the table.

Canada needs improved systems for threat sharing that combine open sources with government and industry sources of information about breaches, indicators and potential responses. This will mean rationalizing what is unclassified and what remains classified and who has access to what. Again, our allies are on the forefront of this activity.

We should consider sandboxes and collaborative lab spaces to test new technologies and capabilities together at scale, as well as talent exchanges between the public and private sectors, like the U.K. Industry 100 program and the new talent exchange just launched by CSE. That could start to address the cyber-talent shortages we're all facing, because cannibalizing each other isn't going to work. Reservists with cyber and computing skills who are employed by companies could be an attractive way to support reconstitution of the CAF, so long as the government does not claim the IP and patents that reservists create while employed in the private sector.

It's also important to note that the broader defence industrial base, or DIB, which includes companies making everything from satellites to ships, has become a prime target for cyber-threat actors. Companies are increasingly incorporating technologies like artificial intelligence into their products. We know that countries like China and Russia will pursue Canada's AI through all available vectors.

Canada's DIB is closely integrated with the CAF and with the American DIB. What we do in this sector is highly valuable, and that makes us vulnerable, given that 90% of Canadian defence companies are SMEs and many lack the ability to defend themselves against a state-sponsored cyber-attack. There's a growing requirement to secure Canadian defence companies large and small. The Americans are, not surprisingly, ahead of us. Very soon, a demanding and mandatory cybersecurity standard will start appearing in Pentagon defence contracts. This is known as the cybersecurity maturity model certification, or CMMC. CADSI has argued that Canada should adopt this standard by reference. CMMC will likely become a de facto Five Eyes, if not global, standard for defence firms. Taking time to contemplate a separate standard in Canada could become a competitive disadvantage for us and a non-tariff trade barrier.

While CMMC is new, other regulations need modernization for cyber, which needs to be done with industry at the table, since we're at the technological bleeding edge and own the lion's share of the infrastructure.

● (0850)

In conclusion, effective cyber-defence at national levels is a team sport. If our allies get this, why can't we?

Thank you. I will be pleased to take your questions.

The Chair: We'll go to Mr. Callan for five minutes, please.

Mr. Tim Callan (Chief Experience Officer, Sectigo): Good morning. I thank the members of the committee for the opportunity to appear before you today.

My name is Tim Callan and I am the chief experience officer and chief compliance officer at Sectigo, which is a global leader in solutions for digital identity, public key infrastructure and digital certificates. These are foundational elements in securing digital operations and ecosystems. My experience in this technology space goes back to 2004. I have previously been a vice-president and leader at Verisign and Symantec and a member of the board of directors at DigiCert. I am co-creator and co-host of the popular IT security podcast called *Root Causes*, which focuses on digital identity, encryption and PKI.

Today, nearly every organization depends on digital processes. Even the most traditional and off-line of businesses cannot perform properly without the aid of both customer-facing and internal digital services that depend on complicated interconnected networks of servers, devices, work streams, automated programs and more. These systems have grown to feed each other in complex webs of interdependency, and, consequentially, the concept of an isolated system failure is becoming rarer and rarer, replaced instead by cascading failures that can bring down entire sets of services.

A perfect example is the multinational cellular outage of December 6, 2018. On that date, approximately 40 million users of O2, SoftBank and other cellular providers experienced an outage that lasted nearly a day. This owed itself to a single failure of a single system in a single third party service provider. This failure cascaded outward until eventually the entire data networks for multiple major mobile service providers were unavailable.

The specific failure was with a digital certificate, which is a component that proves the identity of one element of a networked system. Absent proper digital identity, malicious actors can use a variety of techniques to inject themselves into the system to steal information, take down services or co-opt processes. Digital identity is irreplaceable for defence-in-depth strategies, like zero trust network access and passwordless authentication. Digital identity is necessary to securely operate modern IT architectures, such as DevOps, public cloud and the Internet of things.

Securing digital identities occurs through public key infrastructure, or PKI. PKI is a time-proven method of exchanging cryptographic keys to verify connected systems and encrypt data. PKI prevents third parties from reading or modifying data in transit and from pretending to be legitimate actors in a digital ecosystem. Most PKI implementations depend on digital certificates, which encapsulate core cryptographic functions in a way that enables essential capabilities such as life-cycle management, human-readable identity information and automatic expiration.

The question before this committee today is how to protect Canadians against evolving sophistication in cyber-threats. The events of recent years have shown us time and again that proper and comprehensive use of digital identity is essential to providing secure digital processes across businesses, government, infrastructure, finance, transportation, health care, education and nearly all other walks of life. Unfortunately, significant implementation gaps exist in organizations of all types. They may consist of poor PKI implementation, weak cryptography or failure to deploy automated certificate management to ensure all certificates are current and correct. These failures can result in service outages or security breaches of every stripe.

Plus, the stakes are rising with the advent of quantum computers. Quantum computers will be able to easily defeat more than 99% of the world's encryption. In particular, the RSA and elliptic curve cryptography algorithms will be breakable in many orders of magnitude less time, rendering encrypted data subject to exposure by any attacker with access to a quantum computer. The response to this threat is deployment of new cryptographic primitives, known as post-quantum cryptography, or PQC. New PQC algorithms have emerged from a joint global effort among government, academia and industry, and standards bodies are now working to incorporate them. The eventual result will be PQC-enabled products from software, hardware and services providers available for deployment across IT systems everywhere.

Government and industry should begin preparing for PQC by inventorying their cryptography, implementing automated deployment and management solutions and establishing crypto-agility. Crypto-agility is the ability to monitor, understand and update all cryptography across all processes and environments, now and in the future. The time for this action is today.

● (0855)

Thank you.

The Chair: Thank you, Mr. Callan.

Mrs. Gallant, you have six minutes, please.

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): Mr. Callan, the digital ID that you mentioned, the certificates, are they just for work, or are you proposing this for everyday Canadians and personal use? Would Canadians be required by government to have them in order to access benefits and services?

Mr. Tim Callan: That is a slightly different question. Digital certificates are foundational to every digital process we have, so Canadian citizens depend on them whether they know it or not.

If your question is whether the country should demand digital ID, as is done in a lot of European countries, that certainly is a wave that the world is moving toward. It provides a lot of benefits. It makes it easy to identify that you're real and not spoofed. Used properly, it can make interaction much easier for the average citizen who doesn't necessarily have a computer science degree. These have been used successfully in a number of European countries.

There's also a pan-European standard called eIDAS, which is used broadly across the EU and the U.K. in order to do exactly that. It is a non-trivial effort to establish these kinds of things throughout government organizations, but government is a good place to start.

Mrs. Cheryl Gallant: So it's mainly for industry, but some people use it for personal....

Ms. Cianfarani, what are some of the resources your industries have that government does not have and is failing to understand that it doesn't have?

Ms. Christyn Cianfarani: When you're talking about resources, I assume you mean both services and products. The challenge right now is that much of the.... Certainly within the agencies, the resources are within the agencies and the products typically have been developed within the agencies, so there isn't a lot of bleed-over between where the capability gaps exist and the exposure of those capability gaps to the industry, because it's not in the nature of CSE to expose where it has capability gaps. That is one of the number one issues, which is that we don't know what we don't know. They do not know what we have, and we do not know where their capability gaps exist.

However, what I can say is that the industry itself, about 60% of the industry, has capability in securing networks and data infrastructure, which generally means that we look after mission assurance. Mission assurance can be for networks in threat environments, and it can also be for sensors and assets like planes, ships and tanks that operate in networked environments, as in the Canadian Armed Forces, as well as the infrastructure—like the cloud, for example—that the Canadian Armed Forces itself uses for its enterprise.

We're also very strong in niche areas like encryption, penetration testing and threat monitoring, and the space assets that we maintain, operate and deploy, such as RADARSAT-2, are used for intelligence collection and targeting.

I can tell you what we have; I just can't tell you where the capability gaps exist within the agencies.

● (0900)

Mrs. Cheryl Gallant: That was going to be my next question.

In what ways does Canada expose itself to threats when it chooses to outsource to foreign companies as opposed to supporting its domestic infrastructure?

Ms. Christyn Cianfarani: I think we are seeing a great movement by countries to secure supply chains. I referenced CMMC, which is effectively a way in which the Americans are looking at securing their entire supply chain. We would say that failure to adopt these kinds of standards or these kinds of methodologies to ensure you have a secure supply chain is leading to increased vulnerability.

We would also suggest that what you want in this particular sector, your best way of ensuring that your vulnerabilities are reduced in this particular sector, is to employ Canadian citizens with Canadian security clearances in Canadian businesses that are paying Canadian taxes and that have Canadian supply chains. That's probably the best way you can ensure that you would be reducing the vulnerabilities, as much as possible.

Mrs. Cheryl Gallant: Why do you think the government supports foreign companies instead of using Canadian industries?

Ms. Christyn Cianfarani: I think the challenge is.... It may not necessarily be adopting technologies from foreign countries. I believe it's investing most of its funds, whether that's funds for resources or funds for technology, into its own organization. CSE is increasing its resource pool and increasing the software and technologies that it creates itself, for its own purposes. That is okay. We're not against that kind of behaviour or activity. We're saying that there's a lot more that the private sector—certainly the Canadian private sector—could be bringing to the table if we look at this issue holistically.

It's something our allies have realized quite quickly. In our 2020 report, I believe, we interviewed a number of security experts from other countries, particularly the U.K. and the U.S. They identified that over 50% of their cyber-operations now are split fifty-fifty between contractors and the agencies themselves. They are moving in that direction.

The Chair: Thank you, Mrs. Gallant.

Mr. Sousa, you have six minutes, please.

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

Thank you both for your testimony.

Ms. Cianfarani, I was really encouraged by your opening comments in respect of Canadian expertise, notwithstanding the fact that Canadians aren't necessarily utilizing it to the same effect as our allies and the Five Eyes. I was also struck by your comment about the supply chain and that the speed of cyber is so fast it's hard to keep up.

How do you keep up? You're a professor in this very issue and in this very space.

Ms. Christyn Cianfarani: Well, I spend a lot of time trying to keep up. I guess it comes down to having an entire industry around me that keeps me informed. We share information and we share knowledge. We have to be open to collaborating.

Mr. Charles Sousa: I think that's part of your solution overall. That's exactly what you're trying to propose that others do in this space, and that Canada take a greater issue on trying to provide some of that sharing.

The supply chain risk that you talked about is critical. When I consider what you're saying, what would be your most immediate concern?

Ms. Christyn Cianfarani: There are a couple of things. One is securing the supply chain, which means, on one hand, adopting regulatory standards as they become available. We are concerned. Fifty per cent of the defence industrial base exports, half of those exports, go to the United States. If we want to be a trusted partner in an American supply chain, we will need to be moving in lockstep with them to ensure that we can be trusted partners and that they will be able to procure from us. That's number one. That's a pressing economic consideration for us as a country.

The second thing is just the sharing of information on threats. You would have seen in the papers recently that there have been breaches through the private sector, through critical infrastructure providers or through the defence industrial base. We need to ensure that there is tighter connectivity and sharing of those breaches in a proactive disclosure manner, so that we can leverage the technologies and agencies in order to get the best protections. It's that quid pro quo and it needs to be done in an institutionalized way. It can't be done every time an incursion occurs. There has to be a system that's already in place so we can draw back on it if and when, potentially, cyber-attacks escalate, which we have seen happening in the theatre of war in Ukraine right now.

● (0905)

Mr. Charles Sousa: That's a good point.

Mr. Callan, we just referenced something around the overarching solution to the architecture alongside the private sector. You talked about the digital issues. Can you elaborate on what kind of flexibility, alongside our current cyber-innovations...? How are we keeping up with cyber-innovations and working more collaboratively with the private sector to enable success?

Mr. Tim Callan: There is a very robust private sector that has a lot of activity in terms of industry standards bodies and co-operative organizations. Again, I referred to the post-quantum cryptography as a great example of this. People around the globe came together to build a new architecture that was going to be able to defend against an identified emerging threat. Canadian companies and academics did play a very important role in that. I dare say Canadians punched above their weight in this regard in this particular effort.

That's really what we need. Nothing can exist just inside the boundaries of one nation. The Internet and technology are bigger than any one country. We need to partner with each other to get the best, because the attackers do. They don't care about borders. They just care about getting what they want to get.

Working together with other organizations—be it governmental or private—around the world is how technology providers can give the very best security posture to enterprises and government, etc.

Mr. Charles Sousa: Christyn, it was cited in one of the reports that the manufacturing sector is most at risk, especially with regard to supply. Given that Canadian companies are primarily SMEs in some of this capacity, and that critical mass exists in the States and in other parts of the world, how do we overcome that?

Ms. Christyn Cianfarani: As we suggested, you need almost like an institutionalized method by which you can create the connections to collaborate between industry, the private sector and the agencies or the government bodies.

In part, there has been good forward motion being taken by CCCS, the Canadian Centre for Cyber Security, which has started to stand up a portion of its organization. There are, I believe, six people right now, but it can probably use a lot more, considering the number of businesses that are out there. It has started to stand up a portion of its organization that is responsible for securing portions of the industrial base. Right now the focus is on critical infrastructure, but, as we understand it, they're starting to look at the defence industrial base, which includes the manufacturing component you're talking about.

It's this slow creeping out of the idea that we need to be engaging companies. We need to make them more aware of their responsibility to have more cyber-hygiene. In return for that, we will let those companies into the secret tent a little bit more.

Mr. Charles Sousa: Yes, that's a good point.

Thank you, both.

Thank you, Mr. Chair.

The Chair: Thank you, Mr. Sousa.

Madame Normandin, you have six minutes, please.

[*Translation*]

Ms. Christine Normandin (Saint-Jean, BQ): I thank both witnesses for being with us today.

Mr. Callan, I would like to talk about the use of digital identity by governments. Sometimes there can be a breakdown of a computer system, even without the intervention of malicious external actors. In Quebec, recently, we saw that the simple implementation of a system caused difficulties for the Société de l'assurance automobile du Québec.

When there is a malicious actor, as happened in Albania, which was the target of a cyber-attack by Iran, it is problematic. The human being often seems to be the first weak link.

In Canada, is the cyber health of Canadians good enough to ensure that the rollout of a growing number of digital government services is going well?

I'd also like to get your comments on the Internet of Things. To what extent can it be a gateway for individuals with malicious intent?

● (0910)

[*English*]

Mr. Tim Callan: Yes, the human being is always a weak link in every digital system. It's very easy to build mathematically pure cryptographic solutions that can't be defeated. It's much harder to teach people not to fall for tricks. We call this social engineering. It has been going on since before there were computers, and it continues to be a very viable attack.

We can build our computer systems to help defend people against these kinds of tricks, and you do this with things like cryptography. By putting that in place, I can ensure that it is very difficult or impossible for a worker to give access unwittingly to a criminal, as long as I build the right systems in place. These are the kinds of things that government and enterprises can pay attention to and build. This is one of the areas where we see that enterprises and government continue to be remiss in not doing everything they're able to do.

In terms of the Internet of things, this is another area where things could be much stronger than they are. We can build cryptographically secure systems that prevent devices from being methods of ingress or possible areas for disruption to our systems, our infrastructure, our manufacturing, our transportation, etc. Once again, we often see that these devices do not have the best of breach security. This owes itself to problems like cost, form factor size, available power and available bandwidth, and these other factors drive enterprises or manufacturers to skimp on security. The consequences of that are potential attacks. We've seen a lot of them against automobiles. We've seen a lot of them against infrastructure.

[*Translation*]

Ms. Christine Normandin: Thank you, Mr. Callan.

As I don't have much time to speak, I would also like to ask Ms. Cianfarani some questions.

Ms. Cianfarani, I would like to hear your comments on the rigidity that the government sometimes has with regard to security clearances. For example, I've had people tell me that they applied for a position at the Communications Security Establishment and they were blocked at the last stage of verification because the Royal Canadian Mounted Police, or RCMP, was a bit strict on issuing security clearances.

Couldn't we allow ourselves to be a little more open so that there is better collaboration between the private sector and the public sector, so that people can more easily make the jump from one to the other?

Are federal security standards too strict? Aren't they simply inappropriate?

What can be fixed to ensure better collaboration?

[*English*]

Ms. Christyn Cianfarani: I assume you're talking about security clearances and classifications. I can't speak to how the agencies are screening to let in individuals with those clearances. What I can say is that because we face this on the defence file, we take a view in this country that we want the fewest security clearances possible. We think that clearing fewer people will make us safer, meaning that fewer people having access to that kind of information and knowledge will make us a safer country, because there will be perhaps fewer leaks or things like that.

Other countries have taken a very different approach now. They're starting to declassify more and more information. We've actually seen that in real time in Ukraine, where the U.K. government's GCS is declassifying information in real time to show everyone a picture of what is going on. We're seeing that as well in the updated national security strategy coming out of the United States, where they're saying they're going to declassify more information to make the public more aware.

Whether it's screening, whether it's agencies or whether it's the contract security program in this country that does it for National Defence, the lens through which we do that needs to change. I think the idea that we need to keep people out instead of bringing people in and making them more aware needs to change.

[*Translation*]

Ms. Christine Normandin: Thank you very much.

To what extent does the fact that departments work in silos prevent collaboration with the private sector?

● (0915)

[*English*]

Ms. Christyn Cianfarani: I think it greatly hinders our co-operative effort. We see it on a regular basis within government entities: DND-CAF to the security agencies, and the security agencies to the government. Not to bring in the proceedings of yesterday, but you saw it in real time in foreign interference in the government itself holistically between departments—foreign affairs and public safety. We saw it in circumstances in Ottawa in the convoy situation, where government agencies provincially and municipally, and actually across the federal government, were not harmonized on approaches or information and threat sharing. We see it and feel it on our end in the private sector, where very often we're asking ourselves what is going on, whether we need to be aware, whether the threat is increasing or decreasing.

I think our siloed behaviour is a hindrance to this country, and it's a shame, because we're such a small nation.

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

We have Ms. Mathyssen for six minutes.

Ms. Lindsay Mathyssen (London—Fanshawe, NDP): Thank you, Mr. Chair.

Thanks to the witnesses for appearing today.

Ms. Cianfarani, you talked about institutionalized standards, and of course we've seen a lot of back-and-forth overall between governments in terms of the idea of procurement and not having these longer-term, neutral, non-partisan types of plans, which has really gotten in the way of what I think you're talking about in terms of what the industry can do, what it can provide, how it can plan itself and how it can build, especially when small and medium-sized enterprises, as you said, are the majority of Canadian businesses.

Would you discuss some of the points around the fact that even now we seem to be shifting it again? We had a government that went sole-source for some procurement projects, and then it was refuted by another government saying we needed an open bidding process. That took a very long time and cost a lot of money. Now we seem to be shifting back to that idea of urgent operational requirements, and a lot of procurement projects are focusing on that to actually bypass that open-source procurement.

Can you talk about what that does to the industry overall from a cybersecurity perspective and also in defence procurement overall?

Ms. Christyn Cianfarani: We've been talking a lot, and this is under the defence policy review, the defence policy update, around a concept of continuous capability sustainment or agile procurement.

There is a time and a place for competition. Typically, nations compete when there are two foreign vendors and there is no Canadian incumbent. That is the normal way in which we see it happen around the world. When there is a Canadian incumbent—and what we're talking about here on the cyber side is that you would want to have an already trusted, curated Canadian business that you are prepared to deal with—then in that particular case, sole-sourcing is not and should not be viewed as a shortcut to the process. It should be a solution to agility.

Where it goes sideways is when you don't understand that most nations use the process of sole-sourcing or agile procurement to sustain, maintain and grow their businesses within their own country, meaning that national security is economic security. They fundamentally understand that by investing in a Canadian company, and by doing that in an agile way with trusted sources or trusted individuals, we can effectively be investing in our economy.

Ms. Lindsay Mathyssen: Wouldn't it be the case, then, that the larger companies consistently would already have an edge, but more so would eliminate the ability for those small and medium-sized enterprises to truly compete at the same level?

Ms. Christyn Cianfarani: Well, they don't compete at the same level. Small businesses are generally part of the supply chain.

There are two ways in which small businesses generally get directed contracts. Either you have a niche technology—that typically gets sought after by agencies and these are directed, very targeted purchases—or you have platforms or larger projects where you have a vendor of a chip, a plane or whatever, and that OEM has an entire supply chain. In those cases, what you want to do is get in on the ground floor in being a supply chain partner, a trusted partner to those OEMs. This means that you want to position your defence industrial base or your industrial base as players within that supply chain.

This is where we come to the idea of needing to ensure that we are trusted supply chain partners, by making sure that we have the appropriate regulations in place so that we don't end up with non-tariff trade barriers—in other words, those OEMs saying that we can't play in their sandbox because we are not certified. That's the way in which we ensure that the smaller business gets a piece of the action, if you will.

● (0920)

Ms. Lindsay Mathyssen: Okay. We are seeing quite a lot of that within procurement. One company can't do it all. They do outsource all of those pieces. They do try, especially if there are requirements in terms of Canadian procurement, indigenous procurement, for example, to meet some of those percentage standards, or what have you.

But, again, how can we ensure that those are mainly Canadian, if they are the puzzle pieces to create the overall larger standard, and that they're not actually just consumed, as we're seeing in the telecom industry, by the larger company?

Ms. Christyn Cianfarani: It can happen. There isn't a one-size-fits-all. There are various incentives you can use. In our country, we have what we call an offset policy or an industrial and technological benefit policy that is applied at the time at which you do procurement. That incentivizes prime contractors to use Canadian businesses within their supply chains in order to get Canadian government contracts. You can do those kinds of things.

You can also dictate the terms of your requirements and say, “I want you to work with that vendor, because they have that technology.” You can specify it in the way you do business. In the case of cyber and agile procurement, we would argue that you already have pre-trusted Canadian firms and you could simply source directly to them, which would expedite the process. You already have your trusted partners with the proper classifications that you need, and you would be able to go back to that base again and again.

The Chair: Thank you, Ms. Mathyssen.

Colleagues, again we're at the same problem. We're going to try to run a full 25-minute round. We may be chewing into the second hour, but I think it's appropriate that we do that.

We have Mr. Kelly for five minutes.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you, Mr. Chair.

In the CADSI report, it's noted that while in Canada we take years and sometimes decades, adversaries and allies both have demonstrated their ability to deploy new cyber-capabilities in months or weeks. Just how broken is PSPC?

Ms. Christyn Cianfarani: Well, we're trying to apply to agile procurement a model that wasn't designed for agile procurement. What we're suggesting isn't that the current model is broken. It's that the current model is being inappropriately applied to technology.

Mr. Pat Kelly: So the PSPC model is an inappropriate model for cybersecurity.

Ms. Christyn Cianfarani: Yes.

Mr. Pat Kelly: Okay. Thank you.

The urgency, from your report, is rooted in the fact that cyber-threats go faster than government decision-making processes. What does the government have to do to be able to actually make timely decisions to protect Canadians in the realm of cybersecurity?

Ms. Christyn Cianfarani: Well, in a model, time is the enemy. In our report—and the report you're referring to, I assume, is the 2021 report “Procurement at Cyber Speed”—for those of you who have it, page 18 is a good read. There are really three things that could be done.

You start to create these umbrella projects that procure capability. As I suggested, you break down those barriers, so you have trusted partners and there is a capability development and sustainment that is resident within a country, and you allocate funding at an umbrella level.

The other thing you could do is have more flexible funding. Right now, we have a whole approvals process. It goes through Treasury Board and there are about 200 steps if you take the old model. You would get rid of all that sausage making, if you will, and you would consider a vote of funding that has the flexibility of vote 1 and the ability to acquire new capability of vote 5.

Then, the last thing you could do is fast-track the approval and contracting process by, as I said, setting guidelines, which is where you have technology and services made by Canadian nationals with Canadian security clearances and trusted, curated Canadian businesses where taxes are paid in Canada and IP rests in Canada—boom. I can buy that.

● (0925)

Mr. Pat Kelly: Okay. Thank you.

A number of years ago, the government operations committee studied procurement by small and medium-sized enterprises. You talked about the differences and how so many vendors in cybersecurity and cyber-defence are in fact small enterprises. The committee heard that small enterprises just can't cope with the requirements of the current procurement system and that it is so complicated and so impossible to deal with PSPC that only niche vendors get involved, niche vendors whose whole business model is simply figuring out how to game the procurement system. You have de facto sole-source contracting because there are just no competitors.

Is that a particular issue within procurement for cybersecurity?

Ms. Christyn Cianfarani: I think you would have heard from the agencies that gave the testimony that effectively they don't procure. I believe what they're doing is looking at that system and imagining that if they had to apply that system to procuring cyber-technology, boy, would that be an impediment, which is potentially one of the reasons why they don't do it. Is the system cumbersome and somewhat unwieldy, and is there a whole cottage industry around how to use it? Absolutely. That is why we're frequently here at the table saying that this can be made much better. Particularly for cyber, there are many ways in which it can be made much better and much more agile.

The Chair: You have 20 seconds, Mr. Kelly.

Mr. Pat Kelly: Okay.

For the next 20 seconds, would you like to elaborate on the recommendation from your report on the modernization of cyber-procurement?

Ms. Christyn Cianfarani: Well, as I mentioned, there were those three things. I don't want to reiterate them more than I already have, but again, there's the concept of umbrella projects, where there's a big chunk of funding and you can allocate it to subprojects, meaning that I could buy various technologies, try them out and integrate them into my enterprise in a very expedient manner, and the funding doesn't have to go continuously up through Treasury Board for various approval levels. Once I get a base chunk of funding, I can start allocating it through projects.

Lastly, there is this fast-tracked process, by which if a subproject meets a number of criteria that we believe are good economically and security-wise, we can procure in an agile manner without having to go through all 200 steps to make that happen.

The Chair: Thank you, Mr. Kelly.

Ms. O'Connell, you have five minutes. Go ahead, please.

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

I am going to start with Ms. Cianfarani.

You spoke about the private sector and governments working with the private sector, but we've also heard testimony that there can be challenges as well where the private sector is not necessarily inclined to share with governments when there has been a security breach. There may be a reason for that. There could be trade secrets involved, or they don't want their customers or board members to know that there are vulnerabilities.

With that being said, if there is a role for government to help or do a better job in that coordination, how do you recommend or propose that we bring the private sector along to be more open and transparent about potential breaches? Doing that would also help government prepare for what's out there and what threats exist.

Ms. Christyn Cianfarani: You're very right. You have sticks and carrots—I like to look at it that way. In some cases, the sticks could be compelling businesses to disclose their breaches. Most businesses we talk to say that as long as they are involved with how that would occur and where the information would go, and as long as it is done in a proactive way such that their brand or their business is not damaged in the process.... In other words, you flip the lens and say that proactive disclosure is a good thing. No one should be ashamed that they have had a breach, because it's only a matter of time. You frame it in that way, and then you say that when they proactively disclose to you, the return they will get from that is that they will get others' vulnerabilities so that they can become a better business. It's a quid pro quo type of relationship.

I think those are the missing pieces. If you want to compel, you need to invite businesses in, to figure out how to do that in an effective way that doesn't damage their business. In the same vein, you're going to be sharing that information back, which is something we want and something that will make us better and more secure in the overall ecosystem.

● (0930)

Ms. Jennifer O'Connell: That's great. Thank you.

In your opening statement, I believe you mentioned an example from the U.K.

Ms. Christyn Cianfarani: It was Industry 100, in the U.K.

Ms. Jennifer O'Connell: Yes. Thank you.

I am just curious. Could you perhaps elaborate a bit on what that looks like? How old is it? Is it new in its inception? How could we emulate some of the best parts of that? Could you elaborate on that example?

Ms. Christyn Cianfarani: Yes. It's a collaborative model. It's not so new anymore. Essentially, it's a program that helps solve short-term labour supply shortages of specialized talent.

Industry companies put staff into the National Cyber Security Centre, on their team. That would be like us placing our resources into CSE, for example. They do that on a part-time basis. There is no separation between the industrial partners, meaning that these industrial partners could be competitors at some point in time, but when they come and moonlight at the NCSC, they are doing so together with government staff on a new, neutral territory on a non-transactional basis, so they're not paid for that activity for the common good of U.K. national security.

These individuals in the private sector can do everything from drafting white papers or developing software to being the liaison between their organization and the government entity on threats and incursions that are going on. It's a national type of activity.

Ms. Jennifer O'Connell: Thank you.

Just following up on that, when I was on the finance committee and we did our annual review of the anti-money laundering study, we travelled to the U.K. We heard that there's a different culture when it comes to this openness and security, because there are quite frequently more localized terrorist attacks, so there's more of an acceptance within the public.... Even, for example, registries for mortgages are quite common. But in Canada, and I would say maybe even North America, the culture about that information is a little bit trickier. It's harder to convince Canadians to be open in that measure.

Do you have any thoughts on that?

Ms. Christyn Cianfarani: I think that's a very true statement. We see that kind of urgency all the time. The EU is in the theatre of war right now, and while Canadians sort of feel it, we don't feel it to any great extent. That's one of the reasons we say that if there is a portion of the population or a portion of the business community that is wired to be a bit more accepting of those kinds of things, it is the defence industrial base, by its nature.

The Chair: Unfortunately, we're going to have to leave it there. There's no chance that we're going to make time here.

You have two and a half minutes, Madame Normandin.

[*Translation*]

Ms. Christine Normandin: Thank you very much.

Ms. Cianfarani, I'd like us to go back to the certification standard of the U.S. Cybersecurity Maturity Model, which you mentioned. One of your recommendations is that Canada not work on its own standard, but rather adopt that one.

Do you have any information that Canada is working on its own standard or is no work being done in that direction?

[*English*]

Ms. Christyn Cianfarani: Canada is studying CMMC right now. The Canadian embassy in the United States and, to some extent, DND, Public Safety and PSPC are actively monitoring and looking at that standard.

The challenge is that they're trying to understand whether the standard needs specific “Canadianization”. We believe that if we do that, developing the Canadianized portions of the standard will create a different standard. It will mean that Canadian companies have to have two standards, which increases costs. If we don't get it right, the Americans could be moving forward and Canadian companies could be waiting for the Canadian standard and therefore be left behind when it comes out in procurement. There's that sense of urgency.

They are working on it. We have a pathfinder program right now that is trying to pull in Canadian businesses to actually participate in the American standard as it goes through.

● (0935)

[*Translation*]

Ms. Christine Normandin: Thank you very much.

Mr. Callan, you mentioned quantum computers that are capable of defeating cryptography. Because of this capability, we should invest in post-quantum cryptography.

I'd like you to talk about how quickly we need to acquire the hardware to keep our defence capability constantly updated. I'd like you to compare that to the public procurement process.

Is this process far too slow?

[*English*]

Mr. Tim Callan: Arguably, it's already too late, in that there's an attack called “harvest and decrypt”, which means that if someone gets inside your system, they can grab blobs of encrypted data and just store them, and then at some time in the future, when they have a quantum computer, they can open that up.

For secrets that will still be valuable in 10 years, let's say, like military secrets or advanced industrial secrets, those things may already be lost. For other secrets, maybe not, but it is very urgent that we get post-quantum cryptography in place as soon as we can.

The Chair: Thank you, Ms. Normandin.

You have two and a half minutes, Ms. Mathyssen.

Ms. Lindsay Mathyssen: Obviously, one thing that's plaguing all industry in Canada and around the world is that labour side and human resource side of development.

This is for you, Ms. Cianfarani: Is Canada doing enough at the post-secondary education level to train for those future needs? You spoke about the U.K. model, but in terms of that sharing of personnel, that going back and forth, are we doing enough within colleges and universities to ensure that, going forward, we have the people who are actually building these systems and who are working within these systems? What could we do to make that better?

Ms. Christyn Cianfarani: It's hard, because I'm stepping out of my swim lane a bit. I'm not really in the university or high school models anymore, but I do think that across Canada we understand that there is a talent shortage. We also understand, I think, that we're a bit shy about being directive in terms of incentives for pushing certain classes of study or areas where we want to develop talent to have it come out the other side, meaning that we don't really do things like saying that students can get a bigger bursary if they go into this particular area of study. We want to encourage all Canadians to have equal access to education—post-secondary education, university education—and we're not very directive about what pipelines we want that education to occur in so that we can develop the talent for the future.

I do think that we could do more as a nation to have incentive programs, potentially, around directing education and talent into a variety of swim lanes, if you will, to create the next generation of individuals in the areas that we believe are critical for the country, but that comes down to setting national priorities about where you want your talent base to emerge.

The Chair: Thank you, Ms. Mathyssen.

Mr. Bezan, you have five minutes.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Thank you, Mr. Chair.

Thank you to the witnesses for being here. It's great to see Ms. Cianfarani here again.

I would follow up on what Ms. Mathyssen was just saying. You mentioned the difficulty in getting people the national security clearances and top secret clearances. When we have a shortage in the workforce, that becomes even more difficult. We're having discussions around Bill C-26 right now, and the Business Council of Canada is saying we're short 26,000 people in the cybersecurity industry as it is right now. There are that many unfilled positions.

Aside from trying to produce more people here through our education system, would it be appropriate to employ foreign nationals who are coming from Five Eyes nation partners and who have been approved through their processes?

● (0940)

Ms. Christyn Cianfarani: I think you'd have to do your appropriate due diligence and screening to ensure that they would be trusted partners. First and foremost, before we go down that path, I would say that you have a lot of veterans leaving National Defence and security agencies who have security clearance, and the day they walk out the door, they lose their clearance and it takes them two years or a year and a half to get it back.

Maybe we would want to look inside to expedite the processes and deal with the barriers that currently exist, first and foremost. After that, yes, it could certainly be a possibility to look at individuals from, most assuredly, our Five Eyes partners to provide competency and talent within our own country.

Mr. James Bezan: I love that suggestion. We definitely need to empower our veterans as they're exiting the Canadian Armed Forces. I agree with you that this is a perfect place for them to take on their new public lives as private citizens—in the cyberworld at an industrial level, in telecom companies but also with defence industries.

You talked about a holistic approach and collective cybersecurity. We've heard stories in the past from American sources that certain technologies have been hacked into when third party providers have been accessed, providers that might have access to schematics for things like F-35s or cruise missiles, which have then been proliferated on the global scene by our adversaries.

Has the Government of Canada been serious enough about that type of collective defence to ensure that we are trying to provide as much of a secure system as possible for everybody—from the government workplace and the primary contractor to the subcontractors and all employees—and doing everything possible to protect that intel?

Ms. Christyn Cianfarani: I think, as we said, we've been quite slow at it. Certainly, the agencies and even to some extent National Defence.... Our siloed approach means we look after ourselves. The agencies look after the government. The CAF looks after the CAF, and industry looks after itself. What we're learning is that the approach we use is not working.

If we want to secure supply chains from the lowest common denominator—which is where a lot of the incursions occur, because the most vulnerable is the small business or the small business provider who may or may not have the equipment or skills to be able to do the cyber-hygiene at the level necessary—then we have to create those institutions or agencies or that outreach to get them to be more cyber-aware and to have the appropriate protections. We have to make those protections available to them. We have to help protect those companies and incentivize them. Incentivizing can involve that stick and carrot, meaning that if they want to do business with the Canadian government, if they want to do business in the supply chains, they need to get their CMMC certification, for example.

We have to impose regulations on companies in order to up our game, with a quid pro quo of "Once you're inside the tent, you're inside the tent."

Mr. James Bezan: How many Canadian suppliers of cybersecurity, on both the services side and the infrastructure side, are currently competitive on the global scene? You mentioned that we do encryption and penetration well. What else do we do well, something that is valued by our partners, particularly within NORAD but for sure within the Five Eyes?

The Chair: Answer very briefly, please.

Ms. Christyn Cianfarani: As I said, about 25% of the industry...and 60% of that is along that mission assurance, so that's 60% of 25%. Please don't ask me to do math, because I'm an English major, but that portion is actively engaged in government contracts of our Five Eyes partners.

The Chair: Thank you, Mr. Bezan.

Mr. Fisher, you have the final five minutes, please.

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

Thank you to our witnesses for being here today.

We've been looking at the cybersecurity risk to critical infrastructure in the context of cyberwarfare and threats to Canada's defence and security. Manufacturing is one of the 10 critical infrastructure sectors identified by Public Safety.

Mr. Callan, how does defence manufacturing represent a target for foreign state-backed cyber-instrusions?

● (0945)

Mr. Tim Callan: It absolutely does. Defence manufacturing is critical to the defence infrastructure, and if you can poison those processes, you can hurt it. Furthermore, you can steal secrets. Stealing secrets is a big one. There's a lot to be gained there, and it will be gained for a long time. It has to do with plans for the future and existing provisioning capacity, and all of those things are very valuable as targets for what we call an "advanced persistent threat"—a state-sponsored actor, somebody who might want to hurt Canada. We can imagine who that would be.

To the degree to which the government is a target, it is, but also, the organizations, the private contractors that provide to the government, can be targets as well, and that's another way the state-sponsored actors can get the information they're trying to get.

Mr. Darren Fisher: Can you give me some examples of how industry is working or planning to work towards mitigating this risk?

Mr. Tim Callan: There is a vast raft of strategies and technologies that are needed. One of the things to understand is that you really have to build a security fortress, and any way in is a way in, so you have to look for complete comprehensive coverage, while the attacker just needs to find one gap or one hole or one vulnerability. As we mentioned, this could be things like social engineering attacks. This could be things like inadequate encryption. This could be things like firewalls and email protections that are not quite in place.

It's very complex. There are professionals who dedicate their entire lives to understanding and staying current on these activities. There are entire departments that focus on this, and there need to be.

Mr. Darren Fisher: Ms. Cianfarani, welcome back.

You said that cybersecurity is “a team sport”. I'm a big supporter of partnerships. I'm a big supporter of working together. You touched on this a bit, but maybe you can wrap it up with a bow: What opportunities exist for Canadian cybersecurity firms, traditional defence industry partners and government to work together to better protect manufacturing and our supply chains?

Ms. Christyn Cianfarani: As we talked about, 85% of the critical infrastructure in this country is actually owned and operated by the private sector, so we have a very important role in securing our own infrastructure to keep everyone safe.

Second, we have talent and expertise within our organizations and are continuously developing and innovating so that we can bring that competency to the agencies in order to keep them on the bleeding edge of what is available to protect Canada and Canadian society as well. It's that collaborative exchange where we can all be better as a nation if we're willing to open up a bit to each other.

Mr. Darren Fisher: You crammed a lot into your five-minute opening comments. You talked about the cybersecurity standard, the global standard or the need for a global standard—

Ms. Christyn Cianfarani: Yes, that's CMMC.

Mr. Darren Fisher: That's right.

Madame Normandin touched on this a bit, I think. Is Canada looking at joining a global standard or following the American standard? Is that what you're suggesting we do?

Ms. Christyn Cianfarani: They're studying the American standard, which is going through the process of becoming a standard. It will be imposed on us. It will be imposed on anyone who wants a piece of a DoD contract in the near future or in the future. We're looking at it from a.... We're in that supply chain, so we're going to have to use it anyway. We're going to have to make sure the industry is in line with it and has adopted it.

Second, do we want to adopt it in Canada so that National Defence, for example, would make reference to that standard for its own procurement of products and services? Does it need to be a “standard by reference”, meaning exactly what the Americans have, or is there something particular that we have to add for Canada?

Mr. Darren Fisher: Thank you.

The Chair: Thank you, Mr. Fisher.

Before I suspend, I just want to get some clarification on your comment about declassification. I have been privileged enough to be briefed on secret stuff, and from time to time I wondered whether I had already read about it in The Globe and Mail somewhere. It does strike me that we have an excessively cautious view of what constitutes classified information. I don't know how much thinking you've done about this, but I'd be interested in 30 seconds' worth of your thoughts on this matter.

● (0950)

Ms. Christyn Cianfarani: I haven't delved deep into the subject, but I would concur with your assessment. I think classifying things initially was a way in which people with that information kept value. When they transfer that value, they have to ask “What am I bringing to the table?”

In this country, we also fear what people will do with that information and whether it will come back to harm us. I think Canadians by nature, along with our government institutions, are a bit more risk-averse than our allies are. Perhaps that comes from the fact that we don't often feel as though we are in risky situations where we need to take risk.

I think it's kind of a self-perpetuating model, and it's not getting us as far as we need to get. I think it requires reflection. Do we need to classify all the things we classify? Can more people have access to information, and can more information be declassified so as Canadians we become smarter, better and more nuanced about what's going on? It's not about making us afraid; it's about making us more educated.

The Chair: Well put. We have been in a very different threat environment, even in the last 12 months. I'll be interested in your thoughts in the future.

Ms. Cianfarani and Mr. Callan, I appreciate your willingness to come before the committee. Both of you have shared your thoughts with the committee, and those will inform our studies.

With that, we will suspend and set up for the next panel as soon as Professor Leuprecht is available.

● (0950)

_____(Pause)_____

● (1000)

The Chair: Okay, colleagues, we've solved whatever technical issues needed to be solved. Professor Leuprecht is online.

He would usually have a five-minute opening statement, but since he is the talented individual he is and given the time constraints we have, I'll ask him to be as compact in his five-minute statement as he possibly can be.

[*Translation*]

Dr. Christian Leuprecht (Professor, Royal Military College of Canada, As an Individual): Thank you, Mr. Chair.

I will make my statement in English. However, I will be happy to answer your questions in English or French.

[*English*]

The statement was distributed to you beforehand, so I will skip some parts of it.

Harvard University's Belfer Center's cyber-power index ranks Canada in eighth place as a comprehensive global cyber-power. The CPI characterizes Canada as a high-intent, low-capacity cyber-power with notable strengths in cyber-defence, cyber-norms development initiatives and surveillance. By contrast, Canada's intent and capability to conduct cyber-enhanced foreign intelligence and offensive cyber-operations place it in the middle of the CPI pack, lagging behind Russia and China and its Five Eyes partners—in particular, the U.S. and the U.K.—as well as the Netherlands and Israel. On the one hand, CPI's evaluation of Canada reflects two decades of Canadian cybersecurity initiatives. On the other hand, the ranking shows that Canada has a strategic cyber-deficit.

For 20 years, cyber-diplomacy has largely failed to generate broad agreement on international norms to constrain malicious behaviour by state-based and state-tolerated actors in cyberspace. To deter and constrain bad behaviour, western states need to engage using active and offensive cyber-measures. This is what the U.S. doctrine of persistent engagement has been enabling since 2018. However, no U.S. ally comes close to matching U.S. resources and capabilities.

The 2019 passage of Bill C-59 expanded the role and impact Canada could have in cyberspace by authorizing CSE to conduct offensive cyber-operations. The addition of these capabilities to CSE's mandate was hailed as a major step. In theory, the combination of foreign intelligence, active cyber-operations and defensive cyber-operation mandates enables the full spectrum of cyber-espionage, sabotage and subversion operations. Canada now has the capacity but lacks the political will to demonstrate independent international leadership to reduce instability and uncertainty in cyberspace.

I propose a cyber-doctrine of functional engagement to bolster tacitly accepted cyber-norms. Regularly employing cyber-capabilities is the most effective way for Canada to reduce uncertainty in cyberspace and limit threats to its national interests.

Due to Canada's resource constraints and limited foreign policy ambitions, functional engagement prescribes that Canada employ the full range of its cyber-capabilities to establish and reinforce a limited set of clearly defined and communicated focal points to deter and constrain unacceptable behaviour.

Instead of continuously and globally employing cyber-capabilities to change the overall balance of power in the international system, functional engagement calls for Canada to employ its cyber-capabilities more narrowly, in specific instances when a malicious cyber-actor conducts activity that is antithetical to Canada's focal points, such as by directly degrading Canadian sovereignty and the security of its people; degrading or subverting international law and the integrity of international, electoral or democratic institutions; and undermining Canada's economic security, competitiveness and prosperity.

The proposed cyber-doctrine of functional engagement seeks to shape adversarial behaviour cumulatively by strengthening tacitly accepted cyber-norms within the limited resources and unique character of Canada's historical leadership on foreign policy niches as a traditional middle power.

[*Translation*]

Thank you for your attention.

● (1005)

[*English*]

The Chair: Thank you, Professor Leuprecht.

For six minutes, go ahead, Mrs. Gallant.

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

CSIS has identified so-called smart cities as emerging threats, especially for the PRC diaspora. How could these ventures put our national defence at risk?

Dr. Christian Leuprecht: The premise of smart cities is their interconnectedness and the ability to track both the content and the connections of people within that city.

This is similar to the problem, that, for instance, TikTok poses on a micro level: that an adversarial actor can learn a lot about people, even if it cannot read their content. It's understanding the edges that connect different notes—that is to say, how often you, Mrs. Gallant, are communicating with someone else in your network. In addition, the ability to extract that data would allow an actor who can decrypt it, through quantum or more primitive measures, to then build a very comprehensive picture of your behaviour, Mrs. Gallant, and then potentially deploy misinformation and disinformation campaigns that are deliberately and intentionally targeted to your specific behaviour. That's in order, for instance, to influence your current behaviour, as well as to collect that data over many years to then influence your behaviour in the future.

That is the concern with TikTok. It's the ability to both influence the generation now and keep data on those individuals so that adversarial actors can attempt to influence their behaviour once they become voting populations.

Mrs. Cheryl Gallant: A Defence Construction Canada contractor recently suffered a ransom attack. How, if at all, could this impact our national defence? Are there measures that we should be taking to better protect our defence and security organizations?

Dr. Christian Leuprecht: Well, Mrs. Gallant, I don't know what car you drive. I drive a minivan. It's about a dozen years old. Think about much of what's happening in terms of our networks within the Government of Canada as driving an old car. We're driving on old infrastructure where the government has not sufficiently invested in the actual infrastructure itself.

This is the cybersecurity part of the challenge we face. The other is the cyber-domain part, which is the risky behaviour that is created by individuals who click on links—as was likely the case in this Defence Construction Canada contract—and then inadvertently end up spilling information or making networks vulnerable.

In the previous session, you had a conversation about classification. One of the things we do in Canada is constantly and vastly overclassify material: 90% of the material we classify we probably don't need to classify. The 10% of material that remains we absolutely need to protect at all costs. What we're currently doing is classifying way too broadly instead of targeting our protection, our resources, to make sure that those elements that must never reach the outside are actually protected. Recent discussions over leaks show that, indeed, we have a lot of work to do.

● (1010)

Mrs. Cheryl Gallant: Earlier today, we heard how some encrypted technology messaging and plans could have been stolen without our knowledge already. At some point in the future, when quantum computing is available, they could be decrypted. Secret plans and technology could be revealed, especially as they apply to our missile technology, etc.

What should we be doing now, and what kinds of measures should we be taking in the meantime to protect the sensitive data? What can we do now so that when these quantum realities actually take place, the vulnerabilities aren't as exposed and we're better protected overall?

Dr. Christian Leuprecht: That is a very good question, Mrs. Gallant, because you can imagine that a hostile [*Technical difficulty—Editor*] social credit system for its 1.4 billion people would have the capabilities of building out that system for the rest of the global population. If I were a betting man, I would be saying that this particular country has already built out a fairly sophisticated profile on you, as well as your digital communications and your own data.

I think it is very critical that, precisely as you say, we think very carefully, for instance, about what sort of data we might inadvertently be sharing. Just very recently, Australia decided to pull tens of thousands of Chinese-made products out of government buildings and government networks out of concern about the sorts of surveillance capabilities they might pose.

Certainly quantum will be a significant leap. My best understanding, although this is not my area of expertise, is that it will be a bit like Big Blue. We are not going to go from one day to the next with this capability. There will be somewhat of an off-ramp, but certainly this is a future for which we need to prepare, because the encryption measures and mechanisms that we have in place today would not protect us in that future.

The Chair: Thank you, Mrs. Gallant.

Before I call on Ms. Lambropoulos, Professor Leuprecht, could you please move your mike? Thank you.

Go ahead, Ms. Lambropoulos.

Ms. Emmanuella Lambropoulos (Saint-Laurent, Lib.): Thanks, Chair.

I'd like to thank you, Professor, for being with us today to answer some of our questions.

First, what does the international cyber-governance regime currently look like in terms of international laws and norms governing state behaviour? You mentioned in your opening remarks that no other country comes anywhere near the U.S. in terms of ability when it comes to offensive cyber-measures, and you also said that Canada does have the capacity because of Bill C-59, but that we don't necessarily have the political will.

I'm wondering if you can tell us, from your perspective, what Canada can do, along with its allies, in order to strengthen this rules-based international order in the cyber-domain.

Dr. Christian Leuprecht: It's a great question. We've tried for 20 years to build norms and consensus around this, and we've made very little progress within the UN and within other bodies.

What you need to understand is that there are people who believe in the liberal rules-based international order—that's about 57 countries—there are countries that are agnostic, and then there's a subset of countries that simply do not believe in that order, so we will never get an international cyber-governance regime, at least not in the foreseeable future, but we can force hostile actors [*Technical difficulty—Editor*]. We can deter them from bad behaviour if they know that the United States and its allies lay out big, clear red lines, such that there will be serious repercussions for that actor—whether in cyberspace or kinetic, through sanctions or otherwise—for crossing those lines. My opening statement lays out precisely that sort of mechanism.

However, the Government of Canada has been extremely reticent in using the powers that were given to CSE in Bill C-59 once the act received royal assent. The challenge is, then, what is the point of providing those powers if we're not actually going to use them to advance our interests? Canada has always prided itself on being a country that builds and then enforces international norms and rules, but when it comes to cyberspace, by not using those powers we are effectively doing exactly the opposite.

Now that we have those powers, we also need to use them to defend our interests and our allies' interests. The reason we need to use them is that this is a very particular role for the state to play, because private sector actors and other public sector actors do not have active and offensive capabilities that they can employ. Only the state can deploy those capabilities, so only the state can be proactive in either interdicting or, if need be, in cyberspace, also perhaps sabotaging the capabilities of state-based or state-tolerated malicious actors.

● (1015)

The Chair: Thank you.

I'll just take a brief second here. Professor Leuprecht, could you mute yourself when you're not speaking? I appreciate that it may be a bit difficult, but if you could do that, it would help with the quality of the transmission.

Emmanuella, go ahead.

Ms. Emmanuella Lambropoulos: Thanks.

I appreciate your response. I'm wondering, because I'm not super familiar with Bill C-59, if you can let us know if there are any gaps that currently exist in that bill that create a difference, let's say, between our capabilities and those of the U.S. If it were to become strengthened in times of need in the future, in what ways can it be strengthened?

Dr. Christian Leuprecht: It's not about strengthening the bill. It's about making sure that we use effectively the capabilities we have. The U.S. has vast capabilities that it uses on a regular basis, in part to prevent a change in the international balance of power. That is not primarily Canada's objective, although Canada's objective is inherently to uphold the status quo.

Canada's outline in the last paragraph of my statement [*Technical difficulty—Editor*] three clear focal points of red lines that Canada will not tolerate and where adversaries will know that Canada will deploy, either alone or with its allies, these active or offensive measures as provided for in Bill C-59. The problem is that Canada has not been willing, by and large, to engage in these measures, with some exceptions of hunt forward teams when it comes, for instance, to issues such as those of Ukraine.

Canada needs to be a bit bolder in how it uses the powers that the agencies have been granted to defend Canadian interests.

Ms. Emmanuella Lambropoulos: Would you say that there is a benefit to acting fast, before something major happens? Do we lose some of the ability to respond to a threat if we wait longer?

Dr. Christian Leuprecht: It is a fantastic question, and it hits the nail on the head.

The problem with current political decision-making processes—not with respect to any particular government in this country—for years has been that we dither too long in making key decisions where we need to provide political authority, authorization and direction. The longer we wait, the narrower our margin to manoeuver gets and the fewer options we have in our tool box. We need decision-making processes that are more agile, and we need political decision-making processes that are faster in order to maximize the options available politically to the government and the instruments in terms of operations to achieve the effect that the government intends.

● (1020)

The Chair: Thank you, Ms. Lambropoulos.

Madame Normandin, you have six minutes, please.

[*Translation*]

Ms. Christine Normandin: Thank you, Professor Leuprecht.

It is always a pleasure to have you with us.

You talked about cyber-diplomacy, mentioning that there are states that get along with each other, that there are states that are a bit more agnostic about cyber-diplomacy, and that there are states that are outright against the international global order. For example, China, Russia, North Korea, and Iran are malicious actors, but they each have their own fairly independent ways of operating according to their own interests.

Can we think that there is some form of collaboration between these countries now?

Could there be two fronts rather than one front of allied countries tackling different actors with different views?

Could there be some sort of consolidation of the ways of dealing with rogue countries?

Dr. Christian Leuprecht: That's an excellent question, madam, because it has to do with the political culture and the strategic culture of each of these countries.

For example, Iran primarily has strategic purposes in the Middle East region. Iran is not primarily targeting Canada, the United States or European allies. One of North Korea's primary goals is to steal vast sums of money to fund its nefarious activities. Russia has global capabilities. What differentiates China and Russia from other countries is the scale of the capabilities and a strategic patience to develop those capabilities to optimize certain objectives.

For example, you may remember the computer infiltration of the SolarWinds company systems, about 18 months or two years ago. It was an attempted cyber-attack that probably took 12 to 18 months to plan. It probably took a thousand people to put all the pieces together. These actors have very different capabilities from other states. Therefore, active and offensive measures must be taken to deter them from taking actions that are against our interests.

Ms. Christine Normandin: As these actors are very different from each other, we cannot expect that there will necessarily be collaboration between them. It is not something we can consider in the short or medium term.

Is that right?

Dr. Christian Leuprecht: There is always co-operation for tactical reasons, i.e., to challenge the international political order, which Russia and China believe does not serve their interests.

Authoritarian regimes do not trust each other that much. That's why I'm not too worried about this long-term collaboration, especially on the Chinese side, because they have the capacity to act on their own and further their own nefarious interests.

Ms. Christine Normandin: Thank you very much.

From our side, we work a lot in collaboration with other countries. Doesn't that carry the risk that we become a bit dependent on them? Why not build our own expertise?

In the long run, isn't there a danger that we won't be able to act autonomously if we do too much work in collaboration with other allied countries?

Dr. Christian Leuprecht: Ms. Normandin, it's not a risk, it's a reality. That's what's happening.

Today, Canada lacks the capacity in several areas to be taken seriously by the other G5 partners, particularly the United States, the United Kingdom and Australia. As a result, Canada is excluded from certain collaborative measures in the kinetic field and in the area of cybersecurity. This reduces Canada's ability to look after its interests globally.

There is therefore an urgent need to make investments to develop and expand our country's capabilities in the area of cybersecurity.

● (1025)

Ms. Christine Normandin: Thank you very much.

In Quebec, there is a Ministry of Cybersecurity and Digital Technology, which is supported by a group of advisers. I would like to know if the equivalent exists at the federal level.

Are there any groups of cybersecurity advisers who support the work of the ministers concerned? I'm thinking primarily of the minister responsible for national defence.

If this does not exist, should it quickly be put in place?

Dr. Christian Leuprecht: I have had the pleasure of having some interactions with the Quebec team, and I find the province's efforts in these areas very interesting. The federal government could learn a number of things from Quebec.

The federal government certainly has more capacity than any province. I think there could be a lot more intergovernmental collaboration, as there is in Australia, where the Australian Signals Directorate, the equivalent of the Communications Security Establishment in Canada, or CSE, has offices in each of the Australian states.

It also seems to me that Canada could be more active. Several countries have cybersecurity ambassadors. Denmark was the first to create such a position, but the United States has as well. We don't have a cybersecurity ambassador, which shows that the way we think about the field of cybersecurity could be updated.

[*English*]

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

Thank you, Madame Normandin.

You have six minutes, Ms. Mathyssen.

Ms. Lindsay Mathyssen: Thank you, Professor, for joining us again on this committee.

I want to dig a bit into your conversation with Mrs. Gallant. You were going into a lot of detail about TikTok, the algorithms that are developed and their influential ability, and the mining of that kind of information. Would you argue that this exists across all social media platforms, whether it be Facebook, Google or any of the others?

Dr. Christian Leuprecht: Ms. Mathyssen, I wrote a book on this called *Intelligence as Democratic Statecraft*. It's a great question.

There are considerable differences here. I had for years warned Canadians, when they were very concerned about surveillance by the Canadian state, that they might want to be more concerned about surveillance by private sector companies than the Canadian state. There are considerable safeguards, accountability and transparency processes in place for state surveillance that are not in place for the private sector.

In the case of TikTok, of course, we are talking about a country that not only has no safeguards for either state surveillance or private sector surveillance, but has actively, even just very recently, reinforced its laws requiring private sector companies to share data without any sort of legal or judicial authorization, simply at the behest of the government. Moreover, it has reinforced the presence of the Communist Party of China in all Chinese enterprises.

You cannot, in China, distinguish between the private sector and the public sector the way you would, for instance, in North America. To say that the risk is the same across the private sector would be a fundamental misunderstanding of the ecosystem in which private sector companies operate in China and their relationship with the Chinese regime.

Ms. Lindsay Mathyssen: I absolutely understand that point. It's more about social media platforms overall and their being within the private sector. Ultimately, they have a specific goal that a government needs to monitor.

How can the Government of Canada better create laws to protect people against a lot of these algorithms, whether they're mining for secrets, mining for money or mining to manipulate people? Certainly people can go down a rabbit hole on Facebook in terms of misinformation and disinformation.

● (1030)

Dr. Christian Leuprecht: Facebook is a great example, Ms. Mathyssen. Look at the joint investigation by the Office of the Information and Privacy Commissioner for British Columbia and the federal Privacy Commissioner. The problem is that there are currently very limited tools for the federal government to enforce measures against companies that do not follow Canadian rules.

The question I think the committee might want to ask itself is this: What opportunities exist, and what must be done in terms of government enforcement measures? Also, what incentives, through tax incentives, regulations and so forth, may provide opportunities for the government to act?

Within very short order, you will see a report by the Council of Canadian Academies on public safety in the digital age, which will provide very concrete measures on some of this conversation.

Ms. Lindsay Mathyssen: Thank you for that.

I will go back to your comments about the streamlining of governments' making those key decisions, the inefficiencies and ensuring that governments have the powers to do so. Could you also talk about the flip side regarding some of those democratic safeguards that exist for a reason?

One of the concerns I would have in trying to get at those bad state actors we are concerned about—and you can tell me if I'm wrong—is that we don't become them.

Dr. Christian Leuprecht: I suppose there's always a concern about state intervention in this domain, particularly when it comes to content.

There's probably an opportunity to lay out clearer swim lanes and provide more transparency for the private sector, and perhaps—as I've proposed in the past—for government to lay out voluntary certification measures by which companies behave. They can then get that certification from the government. In return, users know that a company engages in certain cyber-protection or cybersecurity measures, for instance, meets certain standards and, at the same time, will not use data other than for purposes the government intends.

I think a voluntary certification mechanism would give the consumer much greater confidence and provide an opportunity for government to intervene without being [*Technical difficulty—Editor*].

The Chair: Thank you, Ms. Mathyssen.

Colleagues, we have an extension of 10 minutes. However, we're still going to run out of time. I want to devote the last five minutes to the budget for the travel. That gives us 25 minutes' worth of questions.

Mr. Bryan May (Cambridge, Lib.): Mr. Chair, I'm sorry, but a number of us will have to be in question period by then.

The Chair: Because of the technical difficulties, we were given this extra time.

Is it the will of the committee to go until 10:55, or to cut off at 10:45?

Mr. Bryan May: Can we split the difference, Mr. Chair?

The Chair: We can split the difference. That's fine.

Are we good with 10:50?

Some hon. members: Agreed.

The Chair: Colleagues, I'm going to have to be pretty harsh. Even at three minutes, I'm going to run this very hard.

With that, Mr. Kelly, you have a very short three minutes.

● (1035)

Mr. Pat Kelly: We've heard that our allies and adversaries can deploy new capabilities within weeks or months, whereas we take years or decades. How does that impact Canada's ability to use, as you urged in earlier testimony, the existing powers and offensive capabilities in cyber-defence?

Dr. Christian Leuprecht: This is what happens when you don't have a strategy, especially not a forward-looking strategy. In 2017, people like me argued that “Strong, Secure, Engaged” was already outdated the day it was released. I think this was a premonition that has proven to be true.

What we need is a bipartisan 15-year strategy to rebuild our national defence, security and, arguably, our intelligence capabilities. I think it would be helpful to stop playing politics and do as Australia and France did, where all parties get together, have a common strategy and stick with that strategy. Then, we wouldn't be constantly falling behind and trying to play catch-up on too many fronts.

Mr. Pat Kelly: How do our procurement bottlenecks impact our ability to be on top of this issue?

Dr. Christian Leuprecht: Procurement is a problem. The greater challenge is people. People are the most important asset the government has, especially in this domain. It takes a very long time to build these skill sets. They are in very high demand, and they regularly get raided by the private sector.

I think the committee would do well to think long and hard about what government can do to ensure it maintains capabilities and the people my colleagues at RMC and I, for instance, spend many years building up with very exceptional skill sets.

Mr. Pat Kelly: Your characterization of Canada driving the equivalent of a 12-year-old car, in this area, is a matter of both personnel and procurement. It's across the board.

Dr. Christian Leuprecht: The capabilities we have are very good, but they are very limited, because of personnel challenges, structural network equipment and procurement challenges, as well as challenges in updating policy and regulation. As you can imagine, a national defence organization that is struggling with the shortfalls it has doesn't have the time to update policy and regulation.

We have a host of challenges across a broad spectrum that cannot be resolved in a matter of weeks or months, or even within a couple of years.

The Chair: Thank you, Mr. Kelly.

Mr. May, you have three minutes.

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

Thank you, Dr. Leuprecht. It's a pleasure to have you here today.

If we can go back in time, about a year ago, to the outset of Russia's invasion of Ukraine, there was a lot of conversation and concern that those who supported Ukraine, and Ukraine as well, would be targeted by Russia with an onslaught of cyber-attacks, yet we have seen that this hasn't really materialized in the volume that was predicted, either for Canada or for Ukraine.

How do you explain this apparent lack of large-scale cyberwarfare in the war between Russia and Ukraine?

Dr. Christian Leuprecht: I would say that if you look at open-source reporting by Microsoft, Russia has actually been more effective at deploying cyber-capabilities than it has been given credit for, and at integrating those capabilities with kinetic offensive measures on the battlefield. What Russia has learned in Ukraine is that you cannot achieve political objectives on the battlefield through cyberspace. You need to be able to act kinetically. That is where is Russia is concentrating its resources.

However, as you know from repeated warnings from the Communications Security Establishment, Canada is at considerable risk of hostile...not just state-based actors, but in the Russian case, particularly, state-tolerated actors. Ransomware has been mentioned. This has been a major source of revenue for militia state-tolerated actors primarily concentrated in Russia.

● (1040)

Mr. Bryan May: In your opinion, the Russian cyber-efforts have been effective.

Dr. Christian Leuprecht: I would say Russia is not to be underestimated, because there isn't much of a private sector for the many highly technically skilled individuals in this domain that Russia produces. They are disproportionately drawn toward malicious state-tolerated actors, as well as intelligence, military agencies and the like. Some of them have left the country, but Russia has considerable capabilities that are not to be underestimated and that we would do well to continue to pay close attention to.

The Chair: Thank you, Mr. May.

Madame Normandin, you have one minute.

[*Translation*]

Ms. Christine Normandin: Mr. Leuprecht, you have piqued my curiosity. Let me ask you a brief question about the position of cybersecurity ambassador.

What would be the functions of this ambassador, and what would be the benefits of creating such a position?

Dr. Christian Leuprecht: We need to build links with the private sector and different stakeholders around the world, who may not be in a country per se. The field of cybersecurity is very widely distributed geographically, and establishing direct contacts requires effort.

The purpose of embassies and ambassadors is to provide the government with open information. I would say that the Canadian government currently does not have enough open information about the different stakeholders and private actors in this field.

A cybersecurity ambassador would allow us to build relationships with these important players who, in several cases, are more powerful than many of our mid-power partners.

[*English*]

The Chair: Thank you.

Ms. Mathyssen, you have one minute, please.

Ms. Lindsay Mathyssen: Thank you.

Mr. Leuprecht, you talked about the dangers of China, its relationship with TikTok and the release of information. I want you to comment on the Americans, who have the Foreign Intelligence Surveillance Act and section 702, which they're actually discussing right now in terms of being able to get information from Google, Microsoft, Apple and those companies, as we discussed before.

Can you talk about that, and whether it poses a danger in Canada? What should we be looking out for in that regard?

Dr. Christian Leuprecht: That is warranted activity that is being discussed, so it still requires an authorization through the rule of law. There are also safeguards in place with regard to how that information is subsequently used.

People will have different views on whether those authorizations and the laws in place are acceptable to them or not, and whether the oversight, review, accountability and governance mechanisms are sufficient. Certainly, though, that is an important distinction from the way any hostile authoritarian actor operates, where none of those safeguards are in place.

We need to remember that the Americans are at the top of the international security pyramid. They also have objectives that are different from ours in terms of the balance of power. As I often say, the Americans are our best friends, whether we like it or not.

The Chair: Thank you.

Mr. Bezan, you have three minutes.

Mr. James Bezan: I didn't think we were going to get a round out of this.

First of all, I want to thank Professor Leuprecht for joining us today. I know that his expertise in this field has helped a lot.

We did talk a lot about the regime in Beijing being a risk for our social media and for the broader spectrum of services we have in telecoms here in Canada, but can you also speak about how other nefarious transnational criminal organizations and/or other countries, such as the regime in the Kremlin, have attacked or can attack us here at home? How can we quickly be compromised, and how can we go about securing our own vulnerabilities so that it doesn't happen?

● (1045)

Dr. Christian Leuprecht: Mr. Bezan, that's a very good question.

I think the fundamental challenge we face is that we have focused on playing defence, and as long as you play defence, by definition, you will never be able to score. That is to say, you cannot win the game. At the very best, you can play to a draw. When you're dealing with determined, malicious, hostile actors such as China and Russia, chances are they will score on you.

This is an opportunity for the Government of Canada to be more robust and muscular in demonstrating to those adversaries that certain types of behaviour will not be tolerated in cyberspace and will draw repercussions, whether those repercussions are in cyberspace or kinetic.

Mr. James Bezan: Professor Leuprecht, what we're really talking about here is that we have to be able to shoot the archer rather than deflect the arrows. You talk about the Government of Canada, but often they're attacking civilian infrastructure, such as financial institutions and electricity grids, as we witnessed especially with what the Russians have done in Ukraine and in eastern Europe in their cyber-attacks.

Is it solely the responsibility of the Government of Canada to have the ability to attack, or do we also empower civilian organizations to be able to do it to protect their own infrastructure and Canadians at the same time?

Dr. Christian Leuprecht: Sure, resilience on the part of critical infrastructure and private sector actors is key. However, when—not if—they get overwhelmed.... The incidents will come where, for instance, the financial system of one of our banks might find itself overwhelmed by an attack. What mechanisms do we have in place so the bank can call the CSE to tell the CSE that it is overwhelmed and that the CSE needs to do something about either disabling that particular attack or perhaps entirely sabotaging the capabilities that are enabling this type of attack in order to safeguard the financial system?

I would say that, currently, we do not have appropriate mechanisms in place where critical infrastructure and private sector actors can escalate and where they know what exactly the thresholds are and what the conditions are under which they can call the government and the government will intervene. That, I think, is critical for a minister and the government to establish so that we can get the timely help in critical moments that critical infrastructure and the private sector will need.

The Chair: Thank you.

Thank you, Mr. Bezan.

The final three minutes go to Mr. Sousa.

Mr. Charles Sousa: Thank you, Mr. Chair.

Thank you for the testimony.

Let's talk about repercussions, then, with respect to some of these issues. How do we strengthen those norms of responsible behaviour? If I hear you correctly, there are concerns that we may not be adding to or effectively challenging the system in terms of enforcing it, but at the same time, we're sensitive about a state-sponsored cyber-attack that you seem to be suggesting is holding some of these countries at bay. How does Canada, in association with the Five Eyes, hold countries like Russia or China accountable for their actions? How do you impose that?

Dr. Christian Leuprecht: You impose that, on the one hand, by drawing very clear red lines, and on the other hand by demonstrating that we are prepared to use the capabilities we have to enforce against malicious behaviour. Traditionally, middle powers such as Canada have done so in concert with allies and with partners. That is the strength of our capabilities because together we still have more, far better, and more advanced capabilities than [*Technical difficulty—Editor*].

Mr. Charles Sousa: Give us an example of one of those capabilities.

Dr. Christian Leuprecht: If you think, for instance, about the NATO intelligence mechanism that is currently stood up among a host of allies and partners, that could also be used as a coordinating mechanism on active and offensive cyber-measures, but currently we don't have an effective mechanism to coordinate on active and offensive cyber-measures outside of the Five Eyes intelligence community.

Mr. Charles Sousa: We're at risk because we're not able to enforce it or we resist enforcing it. What is the U.S. doing, for example, in that case?

● (1050)

Dr. Christian Leuprecht: We are at risk of the fallacy of composition, because currently the whole is not greater than the sum of the parts.

The problem for Canada is that being able to harness and leverage that ability to co-operate with allies and to work together to establish those norms means that Canada also has to bring considerable capabilities to the table, because why would people say, “Sure, Canada, you should have a part in drawing the red lines and helping us to determine what those lines are”, when in return we're not willing to deploy the capabilities that we have or we don't actually have the capabilities or commitment to enforce those red lines?

Just as we have done in the kinetic space, where we have drawn certain red lines for kinetic behaviour that is unacceptable by states, we need to do likewise in cyberspace, and that can be done, but the Government of Canada has not shown any political will to engage in those conversations with our allies and partners.

The Chair: Thank you, Mr. Sousa.

I want to thank Professor Leuprecht for hanging in with us over these technical difficulties.

Colleagues, that does bring this time to an end.

You've received the budget for the travel. I need someone to move it.

It's moved by Mr. May, seconded by Mr. Bezan.

Is there any conversation about it?

(Motion agreed to)

The Chair: We do need some resolution among the parties in order to action this budget. I'm hoping that will happen over the next little while because the planning of the time is entirely dependent upon the co-operation of the parties. All of you can speak to your respective whips.

The final point I wanted to make is that there's going to be a “Strong, Secure, Engaged” 2.0. It's just been launched. I would appreciate it if any thinking you may have over the course of the next week or two is communicated to see whether the committee wishes to engage in that space.

With that, the meeting is adjourned.