



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

43rd PARLIAMENT, 2nd SESSION

Standing Committee on Government Operations and Estimates

EVIDENCE

NUMBER 012

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Monday, December 7, 2020



Chair: Mr. Robert Kitchen

Standing Committee on Government Operations and Estimates

Monday, December 7, 2020

• (1540)

[English]

The Chair (Mr. Robert Kitchen (Souris—Moose Mountain, CPC)): I'll call this meeting to order. Thank you, everybody, for being here.

Welcome to meeting number 12 of the House of Commons Standing Committee on Government Operations and Estimates.

The committee is meeting today from 2:37 my time, which would be 3:37 eastern time, until 5:37 p.m. We will hear from witnesses as part of the committee's study on the Nuctech security equipment contract and then we will discuss committee business in camera.

To ensure an orderly meeting, I would like to outline a few rules to follow.

Interpretation in this video conference will work very much as in a regular committee meeting. You have the choice at the bottom of your screen to choose “floor”, “English” or “French”, and we would ask you to use the language that you will be speaking.

Before speaking, please wait until I recognize you by name. When you're ready to speak, you can click on the microphone icon to activate your microphone. When you're not speaking, your microphone should be on “mute”.

To raise a point of order during the meeting, committee members should ensure that their microphone is unmuted and say “point of order” to get the chair's attention.

In order to ensure social distancing in the committee room, if you need to speak privately with the clerk or analyst during the meeting, please email them through the committee email address.

For those people who are participating in the committee room, please note that masks are required, unless seated, and when physical distancing is not possible.

We're going to have five minutes of opening remarks from our witnesses. We will go in order. I'll call your names out.

I understand, Mr. Elcock, that you aren't going to be giving a presentation, so we will start with Mr. Charles Burton.

I invite him to make his opening statement.

Dr. Charles Burton (Senior Fellow, Centre for Advancing Canada's Interests Abroad, Macdonald-Laurier Institute, As an Individual): Thank you, Mr. Chair, and good afternoon.

I would like to supplement the evidence this committee heard from civil servants on November 18 by providing information about the relationship between Nuctech and the Chinese Communist Party apparatus that is the regime of the People's Republic of China.

The Nuctech corporate organigram shows the Chinese Communist Party branch and its party secretary, Chen Zhiqiang, at the apex of Nuctech's corporate pyramid. The party branch is at the top. The Nuctech board of directors and senior executive management is therefore subordinate to direction from the Chinese Communist Party.

Indeed, party secretary Chen is also the chairman of Nuctech's board of directors. As a very senior official of the Chinese Communist Party, Mr. Chen is also currently a member of China's National People's Congress. The party secretary is thus the highest ranked and most powerful official at Nuctech.

The Chinese state heavily subsidizes Nuctech and other Chinese hardware and software development and production to make it highly competitive in global markets. That's why they tendered the cheapest bid to us. Like all Chinese state enterprises, Nuctech's *raison d'être* is not primarily economic profitability; it is also to serve other overall PRC regime purposes.

As was mentioned in the evidence in a previous meeting, China's National Intelligence Law of 2017 compels all Chinese nationals, including those working for Nuctech at home and abroad, to collaborate with agents of the Chinese state on request, to further Chinese state interests by, you know, purloining confidential data and engaging in compromise of infrastructure around the world.

This intelligence law is really just pro forma. In fact, Nuctech's connection to the Chinese party/military state is much more than a master-servant relationship; it's really a symbiotic relationship. What I mean by that is that Nuctech, like all Chinese state enterprises, is fully integrated into the PRC party, state, military and security apparatus because, as party general secretary Xi Jinping has put it, “Party, government, military, civilian, and academic, east, west, south, north and centre, the Party leads everything.”

Just as the Chinese Communist Party does not allow for true civil society or non-government sectors, there are also no industrial enterprises in China existing independently from China's party state. In terms of assessing bids, we have to understand that Nuctech is of a substantive nature utterly different from that of its foreign competitors, those existing in a civil space outside of political institutions.

This is a hugely significant distinction between Nuctech and non-Chinese security equipment concerns. Nuctech's purposes are actually the Chinese Communist Party's purposes for Nuctech. Because of its role as an integral element of the unified Communist Party regime, Nuctech's primary purpose is not to generate profits but to serve the overall interests of the Chinese Communist Party at home and abroad, including China's massive domestic and international intelligence-gathering program.

Nuctech can reciprocally draw on Chinese military and intelligence services to obtain foreign technologies and foreign data to serve its advantage. It's fully supported by the Chinese Communist Party's extensive United Front Work Department operations, coordinated out of the PRC's embassies and consulates abroad.

This is because Nuctech, like all PRC enterprises, is mobilized by the Chinese Communist Party to serve PRC regime geostrategic goals throughout the world. That's why you have the Chinese Communist Party branch party secretary, Chen Zhiqiang, as the highest ranked official of Nuctech.

The key here is to recognize that Nuctech is a function of an integrated party-state-military-civilian-market PRC regime complex whose strategic intent is severely at odds with the interests and values of the liberal democratic west, including Canada.

My conclusion will be very brief.

Canada's country-agnostic approach to procurement, while arguably politically correct, should not be applied to bids from People's Republic of China enterprises, state or otherwise. Because China routinely grossly flouts the norms of the international rules-based order in diplomacy and trade, this country-agnostic approach obscures the realities of Chinese regime enterprises and the threat they pose to Canada's national security. In short, like the Chinese Communist Party, Nuctech cannot be trusted by Canada under any circumstances.

Thank you, Mr. Chair.

• (1545)

The Chair: Thank you, Mr. Burton.

Now I'll go to Mr. Leuprecht for five minutes, please.

[*Translation*]

Dr. Christian Leuprecht (Professor, Department of Political Science, Royal Military College of Canada, As an Individual): Ladies and gentlemen, thank you for your invitation. I'll speak in English, but you may ask your questions in the language of your choice.

[*English*]

There is a written submission that hopefully you have received. I shall have to abstract from that submission. I co-authored that submission intentionally with my colleague, David Skillicorn, from the School of Computing at Queen's University, in order to lend greater heft to the actual security assessment of the technology.

We have long argued that Canada's strategic and policy engagement needs to be far more nuanced to reflect the complexity of a relationship that is evolving rapidly. On some matters China is a partner, on some a competitor and on some an adversary. These three challenges converge on matters of technology, security and procurement.

Our assessment of the security risk is that on the technical side they are moderate and manageable, although there are risks. The broader issue at stake is from a democratic government or procurement perspective of procuring such technology from China, and in particular from state-owned enterprises.

First, as Professor Burton has already pointed out, China is playing the long game and is engaging in predatory market practices in order to undercut other companies. You can find this well documented in a report released last month by the United States Senate Committee on Foreign Relations that goes into substantial detail on Nuctech and other Chinese technology companies and how exactly this works.

On principle, SOEs or partial SOEs from non-democratic regimes should be excluded from Canadian public tendering processes because they're not competing on a level playing field. In other words, this matter of Nuctech should be referred to Canadian competition authorities. In lieu of that referral, I suppose, we're here today having these meetings.

In case there's any doubt about just how arm's length Nuctech is, it was founded in 1997 by the son of former Chinese leader Hu Jintao, which makes him part of the notorious "princelings" of the "red royalty" that are widely despised across China. Doing business with Nuctech is bad for Canada's image, bad for China, and bad for Chinese and our image with the average Chinese.

Second, Canadian companies are precluded from competing for public procurement tenders in China. The principle of reciprocity suggests that companies that are either explicitly excluded from foreign tenders or that structure their markets so that foreign companies cannot compete should not be able to compete for federal public tenders in Canada.

Third, Canada should not be doing government procurement business with a country that engages in hostage diplomacy, bullies Canada and some of its closest allies, spreads blatant false information, engages in large-scale and systematic foreign interference, regularly flouts international laws, including endangering allied warships, and is responsible for large-scale human rights abuses on a scale not seen for decades. Nuctech is complicitous in this regard because its relations in selling equipment to the Xinjiang Public Security Bureau goes back well over a decade, as recently testified on July 20 before the Subcommittee on International Human Rights of the Standing Committee on Foreign Affairs and International Development. Therefore, Canada shouldn't be duplicitous in terms of doing business with a company that then on the other side engages in large-scale human rights abuses, and at the same time criticizing China for how it treats individuals of the Uighur minority in Xinjiang.

Fourth, the 21st century is really about data and technology, and China is doing both to enable and promote digital authoritarianism and undermine democratic values, and to actively compromise and interfere in sovereign decision-making. We are now witnessing this on a daily basis and every successful public tender for Chinese technology in Canada is an accelerant towards this dystopian future.

Ergo, Canada should be banning any Chinese state-owned enterprises, partial SOEs, or companies suspected of receiving undisclosed government subsidies, and all Chinese technology companies from Canadian federal public procurement, including standing offers. In cases where that would be in breach of Canada's international trade or legal obligations, the decision should rest with the minister, who should make that decision public.

Finally, and I conclude on this, this matter is indicative of broader issues that have long plagued federal public procurement in this country, especially on matters of security and defence. I remind the committee of the U.S. Department of Commerce's annual report on most difficult countries for military procurement, for U.S. companies to do procurement for U.S. military assets, and Canada ranks second on that list of countries most difficult to do procurement in.

• (1550)

That is robust outside validation of the dysfunction of procurement with which this committee should be seized. The Government of Canada has an opportunity to learn and leverage the visibility from this near-miss with Nuctech, which manifests the extent to which the broad scale and threat risk of this bilateral relationship continually outstrips the government's current tool kit in governance capacity.

This is an opportunity to realize that instead of fending off the alligator that's closest to the boat, the tool kit that enables these examples is simply not fit for purpose. However, in court we have tools to review investments against national security considerations, such as the ICA, and more are coming with respect to critical infrastructure. If there are no comparable tools in place or even under discussion for national security reviews of research and development partnerships, even for domains under the federal government's agreement, such as the tri council grant funding agencies, associate

university research and national labs, such a built-for-purpose tool kit on procurement is long overdue.

The Chair: Thank you, Mr. Leuprecht.

Now we'll go to Mr. Mulroney for five minutes, please.

Mr. David Mulroney (Former Ambassador of Canada to the People's Republic of China, 2009-2012, As an Individual): Thank you. I'll again offer a few opening comments.

On one level, what we're seeing with the Nuctech affair is the kind of disconnect that plagues bureaucracies. I was aware of the risk of disconnect when I served as ambassador to China. We had a dozen different organizations at the embassy, each working directly for managers in Canada. I used to say that my role as ambassador required me to be connector-in-chief. This was essential because failure to connect and to see the bigger picture almost always meant failure at the level of larger Canadian interests.

Some very significant Canadian interests were at risk in the Nuctech affair, and you've heard about some of them already. Briefly, it's not in Canada's interest to advance the global dominance of a Chinese state-owned technology powerhouse, or to create long-term access and partnerships in our system that could make us vulnerable in the future.

Although bureaucratic disconnects happen in normal times, these are not normal times. I was secretary to the independent panel on Canada's future role in Afghanistan, also known as the Manley panel. Canada's mission in Kandahar was failing because the Canadian Forces, Foreign Affairs and CIDA each saw the mission differently.

The very wise people on the panel said that Afghanistan was a once in a decade challenge, one that required new structures and new approaches. We needed a single vision, one that was owned and led by the Prime Minister. We needed to identify achievable objectives, to assign responsibilities clearly, to resource the challenge appropriately and, above all, to see the mission as a Canadian priority, one that transcended specific military, diplomatic or aid objectives.

The panel's focus on process was unorthodox. Ottawa is a town that is in love with policy ideas and bored to tears by policy implementation, by the details of how things actually get done. As the panel pointed out, however, attempting something of national importance without mobilizing and organizing for success is irresponsible, and a dereliction of duty to Canada and Canadians.

Managing the Canadian implications of the rise of China isn't a once in a decade challenge. It's closer to a once in a century challenge, requiring a complete rethinking of foreign and domestic policies.

The Nuctech case is more than a bureaucratic disconnect, more than a performance failure by a government that is more challenged than most when it comes to actually getting things done. The experience offers us a brief worrying glimpse of the state of China competence in a government that has had vivid daily warnings of the extent to which China poses what the Deputy Minister of Global Affairs has referred to as “a strategic challenge to Canada”. However, we’ve seen no signs of heightened awareness, no sign of increased urgency to identify and better manage anything and everything having to do with China, and no evidence of any effort to galvanize the entire government, all departments and agencies, in an effort of pressing national importance.

This isn’t actually a policy problem. It’s a problem arising from the absence of policy. The officials you’ve already heard from were well-intentioned, but they didn’t display any real sense of urgency or even much awareness of our China challenge. This isn’t their fault. It points to a failure of leadership, a lack of that sense of priority and high-level accountability required to face up to and intelligently manage what may well be a once in a century challenge.

• (1555)

The Chair: Thank you, Mr. Mulroney.

Ms. Carvin, please. You have five minutes.

Professor Stephanie Carvin (Associate Professor, Norman Paterson School of International Affairs, Carleton University, As an Individual): Thank you.

I note that my computer has glitched throughout, so hopefully I will be able to make it through. I believe you have my written testimony, and I would be happy to repeat if required.

Thank you for having me here today. Before I begin, I feel that I should disclose that I worked for the Canadian Security Intelligence Service between 2012 and 2015 as a strategic analyst. I did not, however, specifically work on this file, and my interest in the nature of Canada’s relationship with China comes from my own scholarly interests, research and activities.

In that sense, I’m very pleased to be able to speak with the committee today about this important issue. My argument is essentially this: The Nuctech contract is problematic, but not for any of the reasons that have been discussed in the media.

Yes, the scanners are made in China, but so are the computers our embassies use, and the phones and basically all the telecommunications equipment. Also, all the technologies that are made elsewhere probably contain components that are in fact made in China. For better, and quite possibly worse, it is not possible at this time to have technology that is not made in China or with parts that are somehow made in China or sourced from China.

Now, of course there is a risk here, but at the same time it’s not clear that banning all this technology is going to make us safe either. Indeed, it’s more problematic to suggest that bans on equipment make it safer. By this I mean that China is good at getting the information it wants through a variety of means, and many, if not most, non-Chinese technology firms, particularly in the telecommunications sector, have security flaws and vulnerabilities that can be and most certainly are exploited by malicious actors.

Frankly, there are many ways to spy on Canadian embassies abroad: physical surveillance, phishing attacks, insider threats and exploiting vulnerabilities in software. An X-ray machine in a non-classified area seems to me one of the clumsier ways of trying to do it. In that sense, I feel that the technical threat element has been overstated in the public discourse.

Now, I want to be clear. This does not mean that the Nuctech contract is fine. There are clear problems with it and the procurement process, which this entire matter illustrates.

The first issue is that of state-owned enterprises, or SOEs. I don’t think I need to explain to the committee why these are a problem generally, but in this particular case it is worth noting that these are firms that can normally depend on extremely generous support from the state in terms of money or strategic information often gathered through corporate espionage. These advantages give SOEs the ability to undermine any competition. Because they do not have to adhere to the normal business practices, they can bid on contracts at very low prices in order to win, without having to worry about profit or answering to shareholders. In the long term, this can lead to moves that effectively skew the market in certain strategic areas. In this sense, it is clear that some SOEs represent a geo-economic challenge to Canada and western technology firms in their ability to engage in anti-competitive practices. This behaviour should not be rewarded by the federal government.

That relates to a second concern about Canada’s procurement practices. It is worth noting that Canada is increasingly developing processes around foreign investment by SOEs generally and has recently tightened restrictions around certain sectors such as health care during the COVID-19 pandemic. However, for some reason, it appears that protective measures around foreign investment do not extend to the federal procurement process.

Based on the testimony provided to this committee on November 18, 2020, by Mr. Scott Harris, vice-president, intelligence and enforcement branch of the Canada Border Services Agency, his organization “leaned into our colleagues at CSE and elsewhere to gather their expertise” on the issue of security threats from Nuctech technology. If this consultative step was taken in the case of CBSA, why is this not standard practice across the federal government? The lack of standardized policies and procedures, where some departments seek security advice and others do not, seems to be a serious problem.

In conclusion, my recommendations are as follows:

First, Canada should have a policy in place where the procurement of goods and services provided by SOEs by any department are given additional formalized and consistent scrutiny to make sure such investments align with Canadian priorities and values. To be sure, all SOEs are different, and some are simply profit motivated. In this sense, a total ban does not make sense. However, it is something to be risk managed in co-operation with Canada's security agencies.

Second, the federal government needs to develop what is often referred to as a “defence in depth” policy when it comes to the procurement and use of technology, particularly as so much of it presently comes from China.

• (1600)

This is a layered security approach, where multiple steps emphasize measures that control physical access, technology controls that limit what adversaries can do should they get access to a system, and fundamentally for the issue before us, administrative measures that ensure the right policies are in place to prevent security breaches.

Bans will likely not solve our problems, but risk management with layered security approaches will likely be more successful in the long run.

Of course, implementing such a policy will be difficult. In our federal system, many different agencies have different slices of the security and procurement pie. CSE is responsible for the technological assessment, CSIS for the geo-economic threat context, PPSC for ensuring the best value for money, etc.

Media reporting has indicated that tensions have emerged in similar exercises by federal departments, such as the investment reviews required by the Investment Canada Act. However, our federal departments and agencies continue to work together on these new security challenges, and they are learning to get along for the greater good. There is no reason why this could not happen in the area of securing procurement for the federal government.

Thank you.

The Chair: Thank you, all, for your presentations. They are greatly appreciated.

We are now going into our questioning. [*Technical difficulty—Editor*]

The Clerk of the Committee (Mr. Paul Cardegnà): Mr. Chair?

I don't know, Mr. Chair, if you can hear me or not. We're not hearing you in the room. If you can hear me, give me a thumbs-up, please.

Hold on. We're just going to check with the technicians. We are not hearing you in the room. One moment, please, Mr. Chair.

Mr. Chair, I wonder if you could try again. We're going to check to see if we can hear you in the room.

The Chair: Certainly. I'll scream a little louder from Saskatchewan so that everyone can hear me.

The Clerk: Well, you must be screaming loudly now. We are hearing you now, so that is good.

Thank you very much, Mr. Chair. My apologies. You may continue.

The Chair: Thank you, everybody. I apologize. Please bear with us while we deal with the technology.

We will go into questions. As I have indicated, we will do the first hour as we normally do. Then for the second hour, in order to conform to time, we will go to three minutes for the Bloc, three minutes for the NDP, five minutes for the Conservatives and then five minutes for the Liberals to finish off.

We will start off the first round with Mr. Paul-Hus.

You have six minutes.

[*Translation*]

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

I would like to thank all the witnesses for their testimonies. It's quite impressive and confirms a lot.

We, in the Conservative Party, are very concerned about what is happening with China. As Mr. Mulroney mentioned, this is really the challenge of the century.

Dr. Burton, in your remarks, you talked about the direct relationship between Nuctech and the Chinese Communist Party and the links with the Chinese People's Liberation Army.

What is the direct threat to Canada's national security?

• (1605)

[*English*]

Dr. Charles Burton: Thank you, Mr. Chair.

I think that what we're really looking at is that the Chinese government has a policy of...

Mr. Chair, I'm getting the French interpretation through my headset.

The Clerk: Mr. Burton, are you sure you have selected the English channel for speaking English?

Dr. Charles Burton: Yes. It definitely says English on my screen.

The Clerk: Continue, please, and we will try again.

Dr. Charles Burton: With regard to the question of the security threat, there is no question in my mind that the Chinese government seeks capabilities that may be useable if its intent comes later. Capability plus intent is a threat.

In the installation of these very reasonably priced X-ray systems and so on, aside from the concern that CSE raised the last time about USB ports or hard drives inside, there's also just the idea that people who are possibly agents of the Chinese regime would have the opportunity to spend a lot of time in embassy premises—at the door, potentially interfering with the equipment or installing phone chips and that kind of thing—which I think in general the Chinese regime would see an opportunity, in having the ability to access the embassy.

I have heard of a Chinese-installed streetcar system in Britain in which the company found out to their surprise that in fact, on the basis that they needed to service it, the streetcar system was connected to China via a telephone link, which would allow people in the city of Nanjing to stop and start those streetcars remotely.

I think they want that kind of capability, not necessarily because they have the intent to use it immediately, but because there is the potential to make use of this as an opportunity for the Chinese state to realize its geostrategic purposes in the future.

Let me say one other thing. As someone who spent a lot of time in China—I was educated in China—if I went to an embassy and saw that I was being scanned by a Chinese-manufactured machine, I would be quite reluctant to go in, just because of the potential of using sophisticated artificial intelligence and so on to monitor, as we have seen with this kind of equipment as it's used in places such as Xinjiang against the Uighurs.

I think in general we have to be very cautious about any firm that is connected to the Chinese state.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you, Dr. Burton.

I have the impression that everyone knows this, but that many don't dare to act because of economic considerations.

As Prof. Carvin mentioned, Nuctech's embassy systems are one thing, but the systems we acquire are sometimes made in China. We let them into our government systems. We can leave the private sector out because we're here to talk about the Government of Canada facilities, but I think we're being a little careless.

We noticed a lack of consistency when we met with officials two weeks ago. There is no relationship between the different departments. A Deloitte report, commissioned by Global Affairs Canada, cost us \$60,000 per page. All this to get us to give recommendations that will not solve the problem.

What do you think the Government of Canada should do immediately to try to resolve the situation quickly?

• (1610)

[*English*]

Dr. Charles Burton: Is that question addressed to me?

[*Translation*]

Mr. Pierre Paul-Hus: Yes.

[*English*]

Dr. Charles Burton: Yes, I agree absolutely with what Stephanie Carvin has said, that we need to get better procedures in,

fully aware of the potential security risk of acquiring Chinese equipment. They bid the lowest price, similar to the way the Chinese firm Huawei was underbidding Ericsson and Nokia to the order of something like 30%.

I think we have to be aware that there is a security threat posed by companies of this nature, which as I said in my opening statement are of a substantive character completely different from that of other companies.

If you look at the difference, a Canadian company like the BlackBerry company could not draw on the resources of CSE to get information about technology being produced by their competitors or to acquire data about bidding and so on, whereas Chinese state firms absolutely have the resources of the state at their disposal, because it's an integrated, unified system.

From that point of view, awareness of this is the key, and proper procedures to ensure that this never happens again would be terrific. I also very much agree with Mr. Mulroney that our government has simply not put enough resources into getting the expertise necessary to fully understand the nature of our engagement with China, which opens up many issues that make it different from our engagement with really any other country in the world.

The Chair: Thank you, Mr. Burton.

We now have Mr. Jowhari for six minutes.

Mr. Majid Jowhari (Richmond Hill, Lib.): Thank you, Mr. Chair.

I would like to also thank all the witnesses. It was quite an informative presentation, which covered the spectrum of points of view and our relationship vis-à-vis China.

The comments that inspired me or raised my eyebrows were those made by Mr. Mulroney. I jotted a number of points down on which I'd like to get some points of view from Mr. Mulroney.

In summary, the way I took it was that there's an absence of policy vis-à-vis China or the broader relationship with China. You talked about centralized leadership, about alignment across many various departments, about mobilization of organizations for success and about a high level of accountability. What stood out was that you indicate there's an absence of policy.

Given that you worked in the embassy and represented Canada, can you share your point of view vis-à-vis the Canadian government's policy toward China over the last 10 to 15 years? We know there's been a shift in their policies. Have our policies aligned themselves with them, and specifically with regard to technology, investment, socioeconomic and foreign affairs policy?

Can you shed some light on this question?

Mr. David Mulroney: I think the first thing to remember is that China is extremely dynamic, and so it's changing. The China of Hu Jintao which was becoming more aggressive and assertive, has been replaced by the China of Xi Jinping, which is extremely aggressive and assertive. To that extent, no, we have not kept up with the changes.

A wise person in Australia once said that while Australia didn't have a China policy, China very definitely has an Australia policy. It very definitely has a Canada policy.

Let me say two things about this issue. One, I don't think it's a procurement issue. I think the real issue is a China issue. Two, we shouldn't underestimate the challenge of galvanizing and bringing the government together.

I'm not as optimistic as Professor Carvin about the ability at the grassroots of people to come together. This takes real leadership. It requires everybody in government to take note and to pause when China comes up anywhere and consult.

It requires a much higher level, a raising of the bar, when it comes to the security standards that we expect of China. This isn't just like buying a computer that may be made in China. This is a long-term relationship with a company, Nuctech, that would be across the board for all of our embassies, whereby China can find the weakest link in that chain of embassies.

By the way, they will find a weak link somewhere. This is larger.

Finally, this isn't just a Canadian problem. We have allies who are in exactly the same boat. This is where our diplomacy should be directed, to be sitting down with the Australians and the New Zealanders, with the Danes and the Swedes and the Brits, to talk about how they're dealing with this issue. I think we would find that there's common cause.

We're a long way behind. I have great faith in our ability to catch up, but it takes high-level will.

Thank you.

• (1615)

Mr. Majid Jowhari: Speaking specifically to a bilateral investment treaty that we signed back in 2012 with China, the foreign investment promotion and protection agreement, or FIPA, allowing for non-discrimination and equitable treatment of Chinese foreign investors, in general, do you think we should reconsider it, that we should re-evaluate it or amend it?

What are your thoughts on that?

Mr. David Mulroney: The thing about the foreign investment agreement that we should remember is that it applies to existing foreign investment and is about equitable treatment of existing Chinese investments in Canada and Canadian investments in China.

The government always retained the ability to block any investment in Canada that runs counter to any perception of Canadian interests and Canadian security interests in general. I don't see that as central to this issue. We've always retained that ability, and in fact we've shown the willingness to do that over time. This isn't really an investment issue; it's a procurement issue, but it's part of a larger web of concerns about China's encroachment.

Mr. Majid Jowhari: On one hand, I hear that it's not a technology issue but a procurement issue. On the other hand, I hear it's not really a procurement issue but a much bigger, fundamental issue.

Help me reconcile, any of you. Probably we can go to Mr. Burton. I know you were asked more about the security aspect, but how

would you reconcile this as not being a procurement issue or as being a procurement issue, not a technology issue, and its being a policy issue?

Can you give us your insight into that?

Dr. Charles Burton: Well, I think that certainly it is an issue of the process of procurement in the sense that, as was pointed out, the civil servants who spoke to you last time are good people who are behaving in accordance with the regulations and practices as set down.

Clearly those regulations and practices are not effective in preventing the Chinese state from putting in a low bid with all 63 of those boxes ticked off and potentially getting their equipment into embassies, thereby allowing for all sorts of possibilities for access into our diplomatic facilities by Chinese agents. I think we need a general policy on understanding the nature of procurement from the Chinese state and a very careful process of assessment of these bids by people who have the expertise to assess the security risk in the relevant government agencies. I think for the most part we won't be getting any Chinese procurement.

The Chair: Thank you, Mr. Burton.

We will now go to Ms. Vignola for six minutes.

[*Translation*]

Mrs. Julie Vignola (Beauport—Limoilou, BQ): Thank you very much.

My first question is for Dr. Burton.

Dr. Burton, I've had the pleasure of reading a few of your articles, including the one in *The Globe and Mail* on December 4. It was about the situation between China and Australia. In retaliation, China has imposed huge taxes on barley and wine that have cost Australia billions of dollars.

There are similar situations here, in Canada, such as with Huawei. In addition, Nuctech's contracts with China run until 2023, if I remember correctly.

If Canada puts its foot down, and we stop working in isolation, what could be the consequences—positive or negative—from an economic and national security perspective?

[English]

Dr. Charles Burton: Thank you. I think in that regard there is no question the Chinese regime will attempt to pressure us through diplomatic and economic coercion if they feel that will achieve their purposes. We now have the situation of the hostage diplomacy of Michael Kovrig and Michael Spavor, for example. I suspect that when Ms. Meng Wanzhou was given authority by the Chinese Communist Party to transit through Canada, the assumption was that Canada would simply ignore our obligations to the United States under the extradition treaty because there was sufficient knowledge in Ottawa that one should not be detaining Ms. Meng. Now Chinese diplomats say, “Well, the fact that you held her means that you must be punished.” So, even if Ms. Meng is eventually able to return to China under some means, a deferred prosecution agreement or withdrawal of the extradition request or determination by Justice Holmes that the extradition doesn't stand up, we're still going to be punished. The question is whether we respond.

Australia does, I think, over one-third of its external trade with China, so the \$20 billion in sanctions that China has imposed on Australia, directly connected to 14 different conditions, damages them much more. They want Australia to seek funding for the Australian Strategic Policy Institute, for example—it has found out a lot of things about Chinese espionage and influence operations—and to agree to Huawei and to stop their press from reporting negatively, and any number of things that the Chinese regime believe that we can achieve.

I think from that point of view we have to be prepared for retaliation, and the only reason this will not happen will be that the Chinese recognize that we will not be bowing to this kind of pressure and making concessions to them because they are pressuring us. Right now, by holding Kovrig and Spavor, they have managed to stop us from getting any response to Huawei 5G. We're not enacting the Magnitsky Act against Chinese officials complicit in genocide in Xinjiang, and we're not upholding our obligation to sign the British joint declaration with regard to people in Hong Kong who will be subject to persecution under what we would regard as the illegal national security law, so from the Chinese point of view, Canada's response is the one that they want.

I think it's the wrong response. I think it's time for us to make it clear to the Chinese regime that we will not be bullied and intimidated. Australia is certainly setting a very good example for us of the right way to go.

● (1620)

[Translation]

Mrs. Julie Vignola: Thank you, Dr. Burton.

I'll now go to Mr. Mulroney.

Mr. Mulroney, you said earlier that we need to stop working in isolation and that the departments need to talk to each other. We were quite surprised a few weeks ago to learn that there was no security specification on the Nuctech order form. Now we know that Nuctech has contracts that go up to 2030.

Is it now time to review our processes to make them more efficient and transparent across departments to ensure Canada's national security?

[English]

Mr. David Mulroney: Yes, absolutely, but I come back to my skepticism about the ability of the federal bureaucracy—and I'm a former federal bureaucrat—to do this on its own even with the best will in the world. The government is capable of that kind of smart connected operation for only a limited period of time on an issue as complex as China.

I mentioned the Manley panel on Afghanistan because it was the recommendation of people like John Manley, Derek Burney and Paul Tellier that government reorganize itself for special challenges and that these challenges needed to be led by the Prime Minister. I think we would need at least that level of organization around China so that every senior official in the federal government would be aware of the fact that if China is involved in whatever issue they're dealing with, they need to stop. They need to think and they need to consult. Until that happens, I'm afraid that we won't get there. We won't get there by working from the bottom up. This has to come from the top down, because it's a significant change in how government operates. You saw the results of that at your last meeting, that we didn't need Deloitte, an expensive consulting company, to tell us that the government needs to co-operate, but it won't happen without high-level leadership.

● (1625)

The Chair: Thank you, Mr. Mulroney.

Thank you, Ms. Vignola.

Mr. Green, you have six minutes.

Mr. Matthew Green (Hamilton Centre, NDP): That's actually a great segue, because I tend to agree that we don't always have to go to Deloitte to tell us things that we ought to know already.

This question, through you, Mr. Chair, is for Mr. Manley. I certainly would agree with my members on this committee that this is a fascinating opportunity here, with people with significant past experience both on the government side and on the China-Canada relations and policy side.

On November 18, Public Services and Procurement Canada confirmed that the department intended to stop doing business with Nuctech, but that “based on the standards, rules and approaches we use or the legislation, I cannot guarantee or tell you that will be the case.”

Mr. Manley, in your experience, what Canadian standards or legislation poses barriers to ending Canada's relationship with Nuctech or other companies it deems to be a security risk?

Mr. David Mulroney: I'm guessing you mean me.

It's Mulroney. Manley is the other guy. There's another Mulroney, too, but I'm the guy you have today.

Mr. Matthew Green: My apologies, Mr. Mulroney. It is definitely you.

Mr. David Mulroney: No problem.

I think there are things that come up. We see officials, with justification, talking about government procurement and regulations within the WTO, and there may be other contracting issues. With respect, this is sometimes the last refuge of the bureaucracy when it doesn't want to do something important.

As important as the government procurement regulations are in the WTO, regulations which, as Professor Burton has pointed out, China largely ignores, and as important as they are for us—and I get that—our national security is more important. We need to have an understanding within the government that China and dealing with the rise of China is a priority that requires fresh thinking, and that we won't accept as the final word, “Well, there's this government procurement regulation, so we can't do it.” We need to think this through and take more time to think it through.

Mr. Matthew Green: Mr. Mulroney, on that particular point, Mr. Jowhari raised what I think were some important questions. You perhaps disagreed.

Could it not be the case that FIPA as ratified by Canada and the ensuing 31-year term locking in seven Canadian governments might be some of these regulations or legislation that the Chinese government could use to say, under one of their clauses, that we are not in fair dealing with the country? With the way particularly the rhetoric and the red-baiting that we hear about are used, with the—quote/unquote—values compatibility and all of these things that really raise, I think, problematic analyses, quite frankly, could FIPA not be used in this regard to launch a complaint against Canada's procurement against a Chinese company?

Mr. David Mulroney: Maybe you'll explain later what you mean by “red-baiting”, because I certainly didn't engage in that—

Mr. Matthew Green: Not you, but the rhetoric.... I'll share with you, Mr. Mulroney, that the rhetoric we've heard even here today, and in fact what has been the rhetoric of the House of Commons as of late, could be considered by many a marked departure from the Chinese government that the Conservatives under Stephen Harper walked in hand in hand to for a 31-year FIPA.

As you talk about the long-term policy implications of China, in your professional opinion, what is the material change in terms of a threat? I believe that in your testimony, Mr. Mulroney, you had identified that even at that time they ought to have been considered a threat, yet the Harper government locked us in for 31 years.

Mr. David Mulroney: As I said, I think that if you look at the foreign investment promotion and protection agreement, it has to do with existing investment and the guarantee that they will be treated according to international law and the laws of the country. Even if we wanted to try to get out of the foreign investment promotion and protection agreement, I don't think it would affect our national security the way that addressing things like government procurement, which means new relationships and new technologies that are coming in, would. I'm kind of agnostic on that.

What I'm saying is that we should be setting aside excuses that don't really stand up to the importance of our national security, and I'm not seeing any willingness to do that. That willingness would have to come from higher levels, and the silence of the government on issues related to China yields exactly the kind of passivity that you saw from officials last week. That will continue until the gov-

ernment finds the courage to speak to Canadians the way they should.

● (1630)

Mr. Matthew Green: In your opinion, in terms of the ascendent power of China as a global actor, how long has it been known that they would potentially take this type of aggressive position? You used, I think, the language about foreign aggression or aggressive policies. While you were a public servant, was it your opinion at that time that they were also an aggressive actor on the global scale?

Mr. David Mulroney: I wrote a book about this back in 2015, and I talked about my darkening view of China. I said that I thought that up until about 2009 China was still using the rhetoric of international co-operation and collaboration. With the economic crisis and its success in getting through it, we saw a more assertive China, but that was stepped up radically with the arrival of Xi Jinping. We have seen China in places around the world, in the South China Sea and in India, and interfering in most western countries in a way that is unprecedented. This has ramped up in the last five years.

Mr. Matthew Green: For my last question, in your opinion, are there any other foreign state actors quite like China positioned to have the same type of aggressive policy that would potentially be a threat to Canadian national security?

Mr. David Mulroney: There are other threats to our national security, but in my view—and you might want to ask Mr. Elcock about this—China is far and away the greatest threat.

Mr. Matthew Green: Thank you so much for your time.

The Chair: Thank you.

We'll now go to the second round, starting with Mr. McCauley for five minutes.

Mr. Kelly McCauley (Edmonton West, CPC): Thanks, Mr. Chair.

Witnesses, thank you very much.

Mr. Leuprecht, in your statement, you talked about the risk from Nuctech being in our embassies as a moderate risk and manageable, but why would we even bother then if it was a small risk or a manageable risk? Why would our government bother instead of just banning it outright?

Dr. Christian Leuprecht: I think that is the overall thrust of the statement that this is a strategic challenge, but the strategic challenge then also needs to understand that, inherently, out of the umbrella remarks that have been made about the geostrategic engagement by China flow definite risks.

The problem is that we often, as Professor Carvin pointed out, start the conversation on the wrong end. We start focusing on the micro risks the particular technology poses rather than the broader macro scale, the macro elements, both in terms of strategic policy orientation as well as how that then is not reflected in adequate procurement practices and in adequate national security vetting that would then forgo having to have the micro conversation about the threats.

Make no mistake. These are real threats. As Professor Burton pointed out, any software ultimately needs to be updated, so the updates in and of themselves pose a significant risk.

This is the part that people don't get about Huawei, where people ask, "How is it that there are no back doors?" Well, there's no back door to date, no compromise today, but you need the back door built in by definition so that you can actually update the software in the actual equipment. Overnight, the hostile actor can embed malicious technology. Look, there's a lot to be learned, for instance, about traffic that comes through the embassy, the types of material and when that traffic comes in at unusual hours and so forth.

Mr. Kelly McCauley: I would think that even dissidents coming to our embassy.... You would certainly have a second thought before you would pass through Chinese security equipment if you are a Chinese dissident.

Dr. Christian Leuprecht: I think the ability to track how often these dissidents are going, how many of them are coming in and out, is a little bit like what signals intelligence agencies do. Just being able to track the traffic pattern, that in itself can give you a significant amount of information, particularly when their traffic pattern, for instance, doesn't line up with regular business hours. You can kind of go, "Well, there's something obviously up at the embassy. Now we should probably leverage some of the other technology or some of the other compromises that we have in the technology within the embassy to understand what that might be."

Mr. Kelly McCauley: Thank you.

Professor Carvin, you talked about how a total ban doesn't make sense, and then you segued into all the problems that we're going to have in procurement and the other challenges that we're going to have in addressing this.

Should we not just then have an outright ban and then start working on addressing some of these many challenges, these cross-departmental challenges, so that at least we stop the bleeding immediately and then set up proper procedures?

Prof. Stephanie Carvin: That's one possibility. My concern would be that we simply would not be able to adjust fast enough.

My issue is that we seem to be all one way and not the other. What I'm arguing for is layered security. Again, I very much respect the testimony by other colleagues, but if we take the example of the X-ray machine, you're saying that if I were a dissident, I would worry about going through an X-ray machine. Well, I would be more worried about the street cameras that were certainly surrounding me—

• (1635)

Mr. Kelly McCauley: I agree with you 100%, and I'm dumbfounded that—

Prof. Stephanie Carvin: There are so many other ways—

Mr. Kelly McCauley: It goes to your comment about layering. I was dumbfounded that witness after witness at our first meeting said, "Oh, it's not on our security list; we did the right thing." It's almost like we flew the plane into the mountain, but we checked all the checklist items, so it was a success. Common sense certainly has to have a part in it, but we seem to be lacking because we're more focused on ticking boxes than actually doing the right thing.

Should we do an outright ban until we can change our processes so that we don't have department after department turning a blind eye to our security concerns?

Prof. Stephanie Carvin: In my view, I think it would just be easier to harness the expertise that we have now within the Communications Security Establishment. They are perfectly able to provide technological reviews, as well as help with risk mitigation strategies. Certainly, that seems to have been the case with the CB-SA. In its testimony on November 18, it said that, yes, it had reached out to and consulted with the CSE when it procured and used these technologies.

I think it would just be easier, would it not, to.... We have the expertise in place. What I think is lacking is exactly that box that needs to be ticked. We need to completely re-evaluate our boxes.

Mr. Kelly McCauley: All right. One of my questions is—

The Chair: Thank you, Ms. Carvin.

Mr. Kelly McCauley: —whether the CSE should do a security analysis on them all.

The Chair: Thank you, Mr. McCauley.

We'll now go to Mr. Weiler for five minutes.

Mr. Patrick Weiler (West Vancouver—Sunshine Coast—Sea to Sky Country, Lib.): Thank you, Mr. Chair.

I'd also like to thank the witnesses for joining our committee today and for the really interesting comments and discourse we've already had.

I'd like to ask Mr. Mulroney my first question.

Given the risk that you highlighted that the PRC poses now and has posed for some time, you mentioned that we need to look at the bigger picture, and I very much agree. With that mind, I'm wondering what your opinion is of the 2012 acquisition of Nexen by a Chinese state-owned company. Do you think a national security review should have been done for this \$15-billion takeover of a Canadian natural resources asset?

Mr. David Mulroney: If I recall, what followed in the wake of that was a new policy on acquisitions by state-owned enterprises, but I'm not qualified to talk about the.... I wasn't involved in the Nexen review itself. However, we saw an evolution in policy, and certainly that evolution in policy has had to take account since then of the 2017 intelligence act in China, which Professor Burton referenced, which basically made every Chinese company an agent in the work of the Chinese Communist Party.

Mr. Patrick Weiler: Mr. Mulroney, with this in mind, going forward, how should we look at acquisitions of Canadian natural resource projects by state-owned companies?

Mr. David Mulroney: I think the policy we have that looks at net benefit to Canada and, again, looks at our national security interests should be sufficient.

I also think.... I've said this about foreign investment, foreign investment by many sources. We've seen major multinational financial institutions engaging in wrongdoing. We should be vigilant, and investment locales, notably provinces and municipalities, should also be applying the laws, rules and regulations that they have in effect.

Foreign investment involves all three levels of government, and I think that over time we're closer, particularly post 2017 and the Chinese intelligence act, to the scrutiny we need for SOEs.

Mr. Patrick Weiler: Thank you, Mr. Mulroney.

My next question is for Professor Carvin.

You mentioned in your opening statement that you thought the technical security threat over the provision of the Nuctech equipment has been overstated. I was hoping that you could let us know what you think the security risk is to Canada's consular efforts that this contract to supply X-ray machines would pose.

• (1640)

Prof. Stephanie Carvin: I think this was backed up by Christian Leuprecht's testimony, in the sense that the risk is fairly moderate. Of course, these devices do have to be updated, and there is the fact that perhaps Chinese individuals would be coming in to fix the equipment. All of these are serious risks, but I suppose the point I was trying to make with that remark is that just because you ban a technology doesn't mean the threat is gone.

I'm concerned in particular with, say, the 5G discussion, in that we talk about banning a technology and we think that's going to make us safer. It may in some ways, but the fact is that all security products have flaws in them. All these vendors have serious issues. Just because they're not Chinese doesn't necessarily mean they're secure.

We need to be doing these tech reviews on all technology, for the reason that we do know that states like China are trying to hack into our embassies and other places. To me, it's not even just the Chinese, even though I think that should be, for reasons of the problems related to SOEs that have been I think well discussed in this particular session.... We need basically all of our technologies reviewed consistently and thoroughly. Clearly, that's not something that's in the procurement right now.

Yes, this is my concern. By focusing on this narrow issue of the X-rays themselves and whether or not they're vulnerable, we overlook the broader issues with regard to malicious action, say by China, against our embassies abroad and against our government, probably as we speak. We're probably being hacked as we speak. This is the reality.

That's what I meant about that specific technical threat being overstated. It's missing so many of the other broader issues that I think this specific committee could be dealing with in regard to broad overarching strategies for procurement.

Mr. Patrick Weiler: Thank you.

The Chair: Thank you, Mr. Weiler.

We'll go to Ms. Vignola for two and a half minutes.

[*Translation*]

Mrs. Julie Vignola: In 2017, there was a change to China's national intelligence law.

What was our situation before the law was passed in 2017, and what was it afterwards?

That's my first question because I only have two and a half minutes.

My second question is the following.

Should a company headquartered in Hong Kong be monitored as much as a company in Beijing?

[*English*]

The Chair: Ms. Vignola, who do you want that question directed to?

[*Translation*]

Mrs. Julie Vignola: My question can be for Dr. Burton or Prof. Carvin.

[*English*]

Dr. Charles Burton: I can say a couple of things about this.

I think that certainly before the 2017 intelligence law it was clear that Chinese citizens are always required to respond to the demands of the Chinese Communist Party. I think the intelligence law simply made explicit something that was already in effect.

With regard to Hong Kong, Hong Kong is now fully integrated into the mainland system. The companies that operate there would not be able to be independent of Chinese Communist Party control, and therefore I think should be regarded the same as companies from the rest of China.

I would say one other thing. These kinds of procurements are not reciprocal. The Chinese government would never put any foreign 5G into their telecommunications, allow any foreign company to install security equipment in their embassies or allow foreign acquisition of mines and other energy resources. I think that by itself, aside from the moral issues that Christian brought up, suggests this is not something that we should be doing.

[*Translation*]

Mrs. Julie Vignola: Thank you.

If I understand correctly, even though Hong Kong had another regime, today it is completely integrated. If a federally chartered company wants to do business with a Hong Kong-based company and lease a loading and unloading dock for 60 years along a very large Canadian river, is that also the kind of situation that should be viewed with suspicion and that Canada should put a stop to?

• (1645)

[*English*]

Dr. Charles Burton: I'm sorry but I don't understand the question. Is the question if a Hong Kong company has a lease on property in Canada?

[*Translation*]

Mrs. Julie Vignola: A company that wants—

[English]

The Chair: Ms. Vignola, unfortunately, we are running out of time.

Mr. Burton, maybe we can get a clarification from Ms. Vignola to you a little bit later and then you could answer that in writing.

Dr. Charles Burton: Okay.

The Chair: Thank you.

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

Mr. Matthew Green: Thank you, Mr. Chair.

I want to take this last section to do what was suggested earlier and get to the root of how we might be able, as a committee, to improve procurement.

Mr. Chair, through you, to Mr. Leuprecht, how can the federal government improve how security risks are assessed, in your opinion?

Dr. Christian Leuprecht: First, let's actually have a mechanism to assess those when it comes to procurement.

As I pointed out, we do have one when it comes to investment. It is under consideration for critical infrastructure, but it is not currently under consideration for broad swaths of what the federal government does or where the federal government invests, such as in research and development.

Maybe we could actually start even by having a discussion. I think the discussion that you are initiating is very prescient in that regard.

Mr. Matthew Green: In that regard, which federal organizations, if any, should play the key role in the security assessment process?

This came up in an earlier meeting, so I won't pre-empt what my answer is, but I'd love to hear yours.

Dr. Christian Leuprecht: We need to have a comprehensive strategy. I think Ambassador Mulroney alluded to this continuous working in silos with one agency, as Professor Carvin points out, reaching out while another entity does not. It also requires a complete rethink of how we actually work in government, with a much more horizontal approach instead of the vertical implementation we currently have. As I think Ambassador Mulroney rightly pointed out, there is no good mindset in Ottawa when it comes to policy implementation. The minister loses interest; many of the senior civil servants lose interest, and they just pass it off to someone.

I think it requires an entire process, from devising a policy to actually executing that policy. It's a several-step process that needs to have much more consistent attention at all points throughout it. That would already be a very good beginning in terms of getting a more equitable approach.

Mr. Matthew Green: In your opinion, based on your professional background, are there any bilateral or multilateral forums in which Canada should be engaging to improve its procurement security assessment?

Dr. Christian Leuprecht: The Five Eyes mechanism, which I think Professor Carver might have alluded to, already provides us a

very good opportunity for better operational integration. We do this quite well at the defence level, but it is much more recent at the level of intelligence and security, other than signals intelligence. We are leveraging mechanisms, but the learning curve is relatively steep, in particular with regard to what we can share and under what conditions with our partners.

Actually putting the frameworks in place so we can talk about things in an intelligent fashion with other people who hold other relevant information and put that together to see the whole picture beyond our borders would be a good start.

Mr. Matthew Green: It sounds like a course you could maybe put together and teach.

Dr. Christian Leuprecht: I'm teaching it at RMC right now. You're welcome to join and audit the course.

Thanks for your fantastic questions.

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

[Translation]

Mr. Pierre Paul-Hus: Thank you, Mr. Chair.

My question will be for Mr. Elcock.

I'm a member of the Special Committee on Canada-China Relations. Two weeks ago, the Minister of Foreign Affairs, the Hon. François-Philippe Champagne, appeared and mentioned right away in his speech that the China of 2020 was not the China of 2015.

We can see this very well today; Nucotech is just a drop in the bucket and really shows us the security issue that China can represent.

I'd like to know if you currently consider that Canada has already given up the fight against China.

[English]

Mr. Ward Elcock (As an Individual): Mr. Chairman, no, I don't. I think the reality—and on this I would agree with Mr. Mulroney—is that the absence of policy decisions at the top makes it more difficult for the government, more broadly writ, to respond to the threat from China. I think the importance of a policy, or the revision of a policy on China by the Government of Canada, is an enormously important thing. I'm more sanguine than Mr. Mulroney would be about how government would respond were such policy decisions to be taken, but I think the policy decisions, ultimately, need to be taken.

● (1650)

[Translation]

Mr. Pierre Paul-Hus: Thank you, Mr. Elcock.

I think it's pretty clear from the testimony we've heard today that the government urgently needs to do a national security review with respect to procurement. We're here primarily to talk about procurement. We know that two years ago, the government did a review of the legislation through Bill C-59 that touched on national security and tried to put some structure back in place. However, I think we have an urgent problem with respect to the procurement.

My next question is for Dr. Leuprecht.

Do you think we should do this very urgently?

Dr. Christian Leuprecht: We need a more nuanced approach. Our current approach is too one-size-fits-all. Indeed, not every investment from China is a threat, on the contrary. As an average country with an average economy, we need investment from abroad. We need some degree of technology from abroad because we don't have the capacity to research and manufacture everything in Canada.

So, we need to be able to identify where this investment could be a positive-sum game for China and Canada, and could be a positive-sum game in the private sector as private investment when the same interaction within the public sector and public procurement pose a threat to national security.

We currently lack the tool to take this much more nuanced approach to engagement with China. We need and lack leadership from ministers and politicians because, at the end of the day, they are the ones who give direction to public servants. So, public servants could just follow the mechanism, the frameworks, the law and regulations that are put in place by the policy branch of our democracy.

Mr. Pierre Paul-Hus: It's clear that the lack of political strength in this issue is serious.

I'd like to talk to you from a technical point of view. We remember Nortel. At the time, when it went bankrupt, the Canadian Armed Forces took possession of the building, and they found that the premises were bugged. The Chinese had bugged the entire place. The technology at the time was not as advanced as it is today.

In your presentation, you talked about critical infrastructure. Is there a concern that China right now, with all the technologies already in place everywhere, is in a position to take over the subway in Toronto or Montreal, for instance? That may seem exaggerated, but do you think, from a technological point of view, the Chinese can already do this?

Dr. Christian Leuprecht: The risk is bound to exist given the ubiquity of technological facilities. That said, you mentioned Nortel, but in the 1970s and 1980s, it was the largest private-sector employer of engineers in Canada and a world leader in this field. It went completely bankrupt as a result of its own mistakes, but also because its intellectual property had been stolen by hostile actors.

So, there's a great risk, not only to the public transportation you mentioned, but also to Canadian businesses. Who will invest in research and development in Canada knowing that intellectual property will be stolen by competitors?

Mr. Pierre Paul-Hus: Thank you.

[*English*]

The Chair: Thank you, Mr. Paul-Hus.

We will now go to Mr. Drouin for five minutes.

[*Translation*]

Mr. Francis Drouin (Glengarry—Prescott—Russell, Lib.): Thank you very much, Mr. Chair.

I'd like to thank the witnesses for being with us today. I greatly appreciate it.

Dr. Leuprecht, you spoke earlier about Nuctech in Canada and its relationship with its head office. You explained that it was a master-servant relationship. I assume what you meant by that was that the decision-making process was master-controlled and that this decision was made in China, even though there were subsidiaries in Canada. Decisions aren't made in Canada, and any decision relating to Nuctech is made in China.

Have you seen the same process used in other Chinese state-owned enterprises?

• (1655)

Dr. Christian Leuprecht: That's a good question.

[*English*]

Data is the most valuable commodity in the world.

[*Translation*]

It has more value than oil, gas or other natural resources.

China's geostrategic approach is to dominate in terms of networks and software, everything from data flow to data analysis. They want to have the capacity to receive and control this data. China knows that the country that will dominate this field in the 21st century will be able to dominate the geostrategy of the 21st century. It's an integrated strategy.

Because the relationship between the Chinese government and Chinese companies is very close, the Chinese government is able to execute this geostrategic approach in a way that is incomparable to democratic countries.

Mr. Francis Drouin: Thank you very much for your answer, Dr. Leuprecht.

[*English*]

Mr. Mulroney, through various testimonies at this committee, you've often alluded to how we should be cultivating a culture, I guess, of "let's be worried about China right now". You've often evoked that it should start at the leadership, but the fact that China has been stealing IP and the fact that China has been somewhat acting in bad faith in some of our obviously ally countries is not new news.

Then, bringing it back to Nuctech and procurement practices and thinking of recommendations that our committee needs to make, how would you share that China knowledge within all the bureaucracies knowing that—you've served in the federal government—we often act in silos and it's hard to break those silos? How do you cultivate that leadership inside our federal bureaucracy?

Mr. David Mulroney: It has to come clearly and unequivocally from the top, and that is the Prime Minister. It's not even just the foreign ministry, because the fact that we have this.... If you listen to the testimony about the procurement, you'll see that even Global Affairs doesn't have the voice and, for a variety of reasons, isn't always listened to. It has to start from the top.

People will say that we can't speak about China because of all the things they've done to us, including holding Michael Kovrig and Michael Spavor. There's a lot of truth to that, but it's also China's objective. By silencing the government, largely, and by keeping the government passive, China.... I've often said that the people who are affected by this aren't the Chinese. The Chinese are very skilled operators. The people who are affected by the silence of the government are Canadian public servants, who continue to pump missions and visits into China and continue to treat procurement as business as usual.

Let me, if I may, just add one observation as someone who has spent a lot of time in Canadian embassies. The reassurance you got that vendors are supervised inside the embassy is something that you should be very skeptical about. I've made it my business to travel around and to see what was happening when service was being done. This is seen as a very boring joe job and it's often given to—and I mean no offence—family members and to kids who are returning from university. When I went through, I saw people looking at their phones and reading magazines.

All China has to do in this relationship that it would establish through Nuctech is find a few weak links, and believe me, they'll find some.

Mr. Francis Drouin: Would you recommend that all—

The Chair: Thank you, Mr. Drouin.

Mr. Francis Drouin: I've run out of time. Thank you.

The Chair: Yes. Unfortunately, time is very tight today. We've just finished our first hour and we actually have about 12 minutes left before we have to go in camera.

What we will do is go to the Bloc for two minutes, the NDP for two minutes, the Conservatives for four minutes and the Liberals for four minutes.

Ms. Vignola, you have two minutes.

• (1700)

[*Translation*]

Mrs. Julie Vignola: I'll come back to my previous question, Dr. Burton.

Suppose a Canadian port does business with a Hong Kong company to ensure its development. This company will be responsible for automating the port and its operations. In return, for the investments, the company receives a 60-year lease.

Is this the kind of event that Canada should be very wary of, especially on its doorstep? How should Canada respond to this type of economic proposal?

[*English*]

Dr. Charles Burton: I'm not aware of the contract that you're talking about, but on the face of it, it strikes me as completely nuts to give a company subservient to the Chinese Communist Party control over critical infrastructure like port facilities. If we've agreed to such a thing, I think we should review it pronto and stop it.

[*Translation*]

Mrs. Julie Vignola: Thank you very much. We agree, especially since it's a port that leads to the heart of the continent.

X-rays seem very harmless. We've talked about what can be dangerous, such as having a machine made by the Chinese that is then installed and updated by the Chinese.

If the updates aren't done by a Chinese company, is the security risk less or the same?

[*English*]

Prof. Stephanie Carvin: I'm not saying that it's harmless. What we're dealing with is a spectrum of risks here, and how we manage those risks can have a huge impact on the overall security. Even if we aren't going through Chinese companies, there still are a lot of risks that are put in place. That's effectively what I'm saying.

The other thing is that I'm more worried about the janitor than I am about the X-ray machine because, frankly, the janitor is going to have a lot more access than the X-ray machine. That's what I'm trying to say.

Look, I think the issue here is not necessarily that this is harmless or that even if it's a non-Chinese company servicing the X-ray machine there isn't an insider threat there. There is, absolutely, an insider threat, and this is why this kind of overall layered security approach that's looking at these things in steps and trying to.... Sometimes in critical infrastructure protection we talk about the Swiss cheese model, which is where you're trying to layer security so that you can't shoot through all the holes all the way through and then eventually hit some kind of vulnerability.

The Chair: Thank you, Ms. Carvin.

Mr. Green, you have two minutes.

Mr. Matthew Green: Mr. Mulroney, in your view, should companies be excluded from open competitions based on their country of origin?

Mr. David Mulroney: Yes. In the security sector, we should not allow Chinese companies, for example, to compete, and I wouldn't let Russian companies compete. We need to think seriously about where the risk is coming from. I think Professor Burton said earlier that this country-agnostic view is unrealistic and detrimental to our national security.

Mr. Matthew Green: To what extent can the federal government assess these security risks associated with a company by virtue of its country of origin?

Mr. David Mulroney: It could do so by cross-referencing the technology related. Also, any technology coming from a country like China that could make us vulnerable and that could harvest information about Canadians or about our foreign guests would be off the list. That's certainly not impossible.

Mr. Matthew Green: Would this relate to our emergency exemptions, like our security exemptions?

Mr. David Mulroney: That's why I talked about creating new structures. We might have to look at this in a new way, but we've had two years of daily focus on the risks posed by China, and we haven't done it yet. I think we should get down to figuring out just what that would look like. The result would be that in many sectors we would not be procuring Chinese equipment or services for the Canadian government.

• (1705)

Mr. Matthew Green: In your mind, while obviously trying to honour our obligations under international trade, is this approach something that is manageable and something that we could do based on our current international trade agreements?

Mr. David Mulroney: That's why I said you have to weigh our obligations to the WTO against our obligations to the national security of Canada. That's the first point.

The second point is that you're going to find that a lot of other countries are in the same boat, and we could be spurring some creative thinking about how we do this collectively. I could tell you that others are already doing it and that we are laggards in thinking about this.

The Chair: Thank you, Mr. Mulroney and Mr. Green. Two minutes go by very quickly.

Mr. McCauley, you have four minutes.

Mr. Kelly McCauley: Professor Carvin, before we can set up an overall rejigging of our procurement process, who do you think should be doing a last-person review of any procurement? Would it be CSE or someone else like CSIS?

Prof. Stephanie Carvin: It depends on the issue. On the technical expertise it would certainly be CSE. I do believe they have that expertise now and have provided it in certain select cases but they have to be consulted first.

Then on the geo-economic aspects, I think you wouldn't want to involve an agency like CSIS, which could provide perhaps the broader context and would have knowledge of.... The other thing about these companies too is even when it looks like it's a private company, that just may be a shell company that's owned by layers and layers of different Chinese companies that ultimately end up at an SOE as well. CSIS does have that capability to understand that larger context.

It's not just one, unfortunately, as I think we've all agreed on this panel, but in the meantime, I would definitely, at a bare minimum, be talking to CSE and CSIS.

Mr. Kelly McCauley: That's something we could do immediately. Obviously we have a lot of changes we have to address. To me it would seem pretty straightforward. We could have saved a quarter of a million dollars. Of course, Deloitte would have been out of

pocket a quarter of a million dollars for a four-page report, but it could have bought someone from CSE a coffee and asked them over coffee if we should buy sensitive security equipment from China. Obviously, the answer is no.

Thanks very much.

Mr. Mulroney and Mr. Burton, I have to assume you're familiar with Anne-Marie Brady's paper, "Magic weapons". I'm wondering whether we are facing a similar threat in Canada.

Mr. David Mulroney: We most definitely are, and we've been slower to recognize it but we're facing the same techniques: elite capture, penetration of universities, diaspora communities, media that's happening in Australia.

Mr. Kelly McCauley: Should we be banning groups like the Confucius Institute outright?

What steps should we take to stop the magic weapons and all these other programs they are using against us?

Mr. David Mulroney: I've written that one thing we should copy is the Australian foreign influence measures that look at people who are acting on behalf of other states or state-controlled actors and make it an offence not to disclose who is paying you to say things, who is paying you to do things in this country. That would be a significant step, but that also involves giving the intelligence community investigative powers and adding criminal sanctions to punish those who are doing this.

Mr. Kelly McCauley: Is there anything you see in the Australian version that we wouldn't want to do here? I know the Americans have their foreign agents act that goes back to the 1930s. Is the Australian one a better one to copy? Should we take some from the U.S. one? Are there parts of the Australian one that go too far or not far enough?

Mr. David Mulroney: It's still early days with the Australian one but we're seeing that it has some bite and some effect and, as Professor Burton has mentioned, it certainly got the attention of the Chinese.

What I think is important is it makes explicit what should be explicit anyway, that if you've had a senior position in government, certainly if you've been a minister, you need to disclose if you're on the payroll of a foreign state and acting on that behalf, and failure to do that should result in criminal sanctions.

I think the Australians have taken tough measures but they are absolutely the right measures.

• (1710)

Mr. Kelly McCauley: That's wonderful.

Professor Burton, do you want to chime in?

Dr. Charles Burton: Yes, the argument that's made on Senator Yuen Pau Woo's website, that Canada does not need this comparable legislation because we don't have those sorts of issues going on and that our existing arrangements are already fully able to address problems of retired officials who receive benefits from a foreign state, particularly China, is utter nonsense. I think what's going on in Australia and New Zealand is almost certainly going on in Canada.

Other concerns have been raised that the Australian legislation might not be compatible with the Canadian Charter of Rights and Freedoms. I'd like to see a serious study done of it, to see if that is in fact the case. I don't see why anyone would object to such legislation because it simply allows transparency, and sunshine is the best disinfectant.

I think we do have a serious problem—

The Chair: Thank you, Professor Burton.

We now have Mr. Kusmierczyk as our final questioner.

Mr. Irek Kusmierczyk (Windsor—Tecumseh, Lib.): Mr. Chair, I'm going to delegate my time to my colleague, Mr. MacKinnon.

The Chair: Certainly.

Mr. MacKinnon.

Mr. Steven MacKinnon (Gatineau, Lib.): Thank you very much, Mr. Kusmierczyk and Mr. Chair.

I'm going to ask Mr. Elcock to respond just because it seems to me we haven't heard a lot from him today.

Should Canada not procure anything from China?

Mr. Ward Elcock: I think, Mr. Chair, that's probably unrealistic. China is still a trading partner of Canada and is likely to be so into the future. If you were to ask Canadian rapeseed farmers and pork farmers, I suspect they envisage trading with China.

Do we need to trade with China a lot more carefully? Yes, we do, but to do that, ultimately we really need to have a policy with respect to our relationship with China. I would agree—I think it was David Mulroney who also said this—that we ultimately need to find partners amongst other countries around the world in confronting China. To suggest that we would do it on our own is probably unrealistic—

Mr. Steven MacKinnon: I'm going to stop you there because we have very limited time, Mr. Elcock. My question was about procurement, specifically federal government procurement. Should we stop procuring from China?

Mr. Ward Elcock: I think that probably is unrealistic, but again, if you have a policy on what your relationship with China is and it's clearly stated, and you are more careful—

Mr. Steven MacKinnon: It's nuanced. I'm sorry to keep interrupting you, sir, but we don't have a lot of time. It is nuanced. There's a point at which you'd stop not procuring from China.

Mr. Ward Elcock: Yes. That's exactly right.

Mr. Steven MacKinnon: Presumably for broom handles and paper clips, that's all fine.

Mr. Ward Elcock: Yes.

Mr. Steven MacKinnon: If we were to stop procuring below that line for things we deemed sensitive, what would we expect China's reaction to that to be to, say, a Canadian technology supplier to China? What would we expect that to be?

Mr. Ward Elcock: They're probably already not going to buy much in the way of technology from Canada. Nortel tried to sell into China without any success, so the reality—

Mr. Steven MacKinnon: That's a 20-year-old example, but...

Mr. Ward Elcock: It's nonetheless true today.

Mr. Steven MacKinnon: As a 10-year-old example, BlackBerry never sold into China. Shopify doesn't sell into China.

Mr. Ward Elcock: I doubt very much whether they were able to sell very much into China.

Mr. Steven MacKinnon: The point I'm taking from you, though, is that it's probably case-by-case.

Mr. Ward Elcock: It's case-by-case, but also, as David Mulroney said earlier, we need a policy. We need to know what our policy is with respect to China. Once you know what the policy is, many of the other decisions will fall out from that, together with building a relationship with other countries that allows us to confront China much more clearly than we can now.

Mr. Steven MacKinnon: How do you devise a policy that is case-by-case?

Mr. Ward Elcock: I didn't say that the policy was case-by-case. We need to know what our intentions are vis-à-vis China and what we're prepared to accept and what we're not prepared to accept.

Mr. Steven MacKinnon: Okay. In terms of procurement, which is the focus of this committee specifically, for the minister who has the authority to execute or not execute on a purchase, what guidance should he or she take in the case of GAC here? From your accumulated wisdom and that of our witnesses, what should we take specifically as to your advice for her or for him?

• (1715)

Mr. Ward Elcock: If you're thinking about the present procurement of Nuctech, the reality is that it's a relatively minor thing. You could add to the security review that was done that they should have looked at the technology of the equipment that was being bought, as well as the two security issues that they did look at. Apart from that, it's a relatively minor issue. Perhaps that wouldn't in fact change, unless the question of whether the Chinese had so dominated the screening industry that it became a threat in and of itself. You might continue to want to buy from China if you've taken all of the security issues into review.

Again, in much of what your procurement policy will be, it doesn't fall out necessarily in detail from what your policy view is of China relationships. Once you know what your China policy relationships are, you can start to make clearer decisions about what your procurement rules are going to be, what kind of position you're going to take on Chinese SOEs selling into Canada and what kind of position you're going to take on the level with which you're prepared to see Chinese companies investing in Canada. All of the—

Mr. Steven MacKinnon: We're putting the cart before the horse in this meeting today. There are five hearings scheduled on this Nuctech issue at the behest of the opposition. Is your view that it would be four too many, Mr. Elcock, and that it's a minor issue?

The Chair: Thank you. Unfortunately, our four minutes are up.

I appreciate that it's a tight schedule today.

Perhaps, Mr. Elcock, you could answer Mr. MacKinnon in writing. That would be greatly appreciated.

Mr. Steven MacKinnon: Thank you very much.

Thanks to all of you.

The Chair: The challenge is that we have to get this on time.

Witnesses, I'd like to thank all of you for being here today and for your answers to our multiple questions. It's very tough to answer some of these questions in a short time frame, but we do appreciate your comments.

Again, thank you for being here. You are now welcome to leave.

Committee members, we are ending the public portion of our meeting and we are going in camera.

In order to do that Zoom will end. You will need to go out and come back in on the Zoom attachment that you were given, plus the new code that you were given.

With that I'll suspend the meeting until we are in camera.

[Proceedings continue in camera]

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

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

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

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

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

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