HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

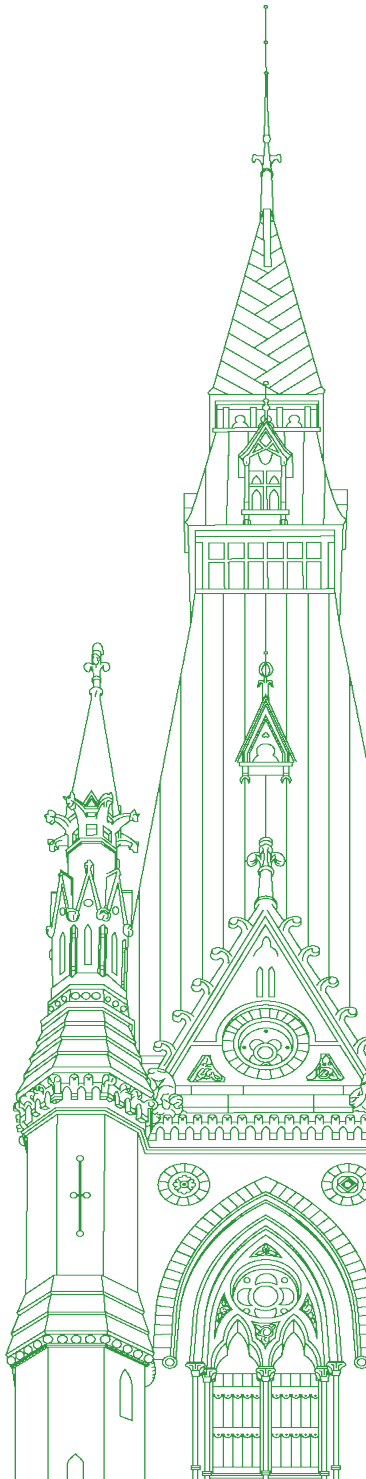
44th PARLIAMENT, 1st SESSION

Standing Committee on National Defence

EVIDENCE

NUMBER 013

Monday, March 28, 2022



Chair: The Honourable John McKay

Standing Committee on National Defence

Monday, March 28, 2022

● (1530)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Colleagues, we have quorum, so I will bring this meeting to order.

There are a couple of points just before we call on our witnesses.

First of all, our colleague Rob Oliphant has COVID. Of course, he was at the meeting on Wednesday with us, and some of us had pictures with him. Mr. Motz, wisely apparently, didn't. Just in terms of your own health, you should be aware of that.

You'll notice that our second panel now has two witnesses, whereas before, it had three witnesses. Our third witness, Mr. Tadej Nared, wrote to the clerk this morning and said that he, too, has COVID. He was hoping to be able to tough his way through it, but it's apparently a little bit more difficult for him, so we'll have to make sure to have the opportunity to invite him back.

Cheryl.

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): Will we invite him back?

The Chair: It's just a question of an opportunity to invite him back. That's the issue.

Having said that, I see that we have two witnesses who apparently don't have COVID. That's a good start.

We have Cherie Henderson, assistant director, requirements, for CSIS, and Mr. Sami Khoury is head of the Canadian Centre for Cyber Security at the Communications Security Establishment.

Mr. Khoury, I am intensely jealous of that tie. That is a beautiful tie. I'm sure there is a story behind it.

With that, I'll call on Ms. Henderson for her five-minute opening statement.

Ms. Cherie Henderson (Assistant Director, Requirements, Canadian Security Intelligence Service): Mr. Chair, members of the committee, good afternoon.

I'm Cherie Henderson, the assistant director of requirements at the Canadian Security Intelligence Service. Thank you for the opportunity to appear before you once again this year, this time to discuss cybersecurity, which of course is a very important topic.

As Canada's principal government agency responsible for investigating threats to the security of Canada, CSIS also investigates cyber-threats. As such, we employ all our investigative tools to collect intelligence on cyber-threat actors' exploitation of cyberspace to conduct espionage, sabotage and foreign-influenced activities against Canada and Canadians. CSIS also co-operates with a wide range of domestic and international partners.

Our unique value lies in our ability to collect intelligence on the nature and scope of hostile cyber-activities and the intentions of the actors behind them. This intelligence supports the mandates of our Government of Canada partners, enabling them to better formulate foreign and domestic policies, protect critical Canadian entities and strengthen our nation's overall cybersecurity posture.

Under the CSIS Act, the service also has the legal authority to use threat reduction measures in order to reduce cyber-threats to Canada. One of the most important challenges to address in protecting our national security is the sharing of timely and actionable intelligence. CSIS is addressing this particular challenge in a number of ways, including through regular outreach and partner engagement. We have delivered briefings to partners on the espionage and foreign influence threats posed by state cyber-actors, as well as the potential national security impacts of ransomware attacks carried out by criminal groups.

With today's rapidly evolving technology, we are witnessing an unprecedented level of change in the threat environment. It has become more complex, increasingly fluid, less predictable and consequently more challenging. Threat actors are conducting activities in the online space, simultaneously taking advantage of the technology that enables them to disguise their activities and their identities. Moreover, cyber actors have more opportunities than ever to conduct malicious activity as our world becomes increasingly interconnected.

We investigate the criminal elements as well as the hostile state cyber actors who conduct malicious activities to advance their countries' interests, whether they be political, economic, military, security or ideological. Hostile state actors seek to compromise computer systems by manipulating their users or exploiting security vulnerabilities to gain access to trade secrets or to achieve various objectives through the disruption of critical infrastructure and vital services. These types of activities are not going away, and in fact are currently on an upward trajectory.

CSIS has observed persistent and sophisticated state-sponsored threat activity for many years. We continue to see a rise in the frequency and levels of sophistication of this threat activity. Canadian companies in almost all sectors of our economy have been targeted and compromised.

Unauthorized, malicious access to Canada's critical infrastructure can have drastic consequences for the safety and security of Canadians. If you think about all the systems we rely on in our lives, including systems that support our telecommunications, energy, transportation, supply chain, health and financial activities, any interference with these systems can have unforeseen impacts on our personal safety, our well-being and our national security.

For example, the COVID-19 pandemic has given rise to an unprecedented number of individuals working from home offices, which are much less secure environments. This new standard of work increases the risk of exposure to malicious cyber-activities on networks and sensitive information. We have all heard accounts of cybercriminals conducting ransomware acts on companies and public institutions, including hospitals at the height of the pandemic.

The increasingly interconnected and global nature of security threats means that CSIS cannot fulfill its mandate in isolation. There is tremendous co-operation and ongoing work within the security and intelligence community to provide the Government of Canada with the best intelligence and advice possible concerning cyber-threat activity.

Today's global threat environment requires that each partner use their unique mandate and legal authorities to protect Canada and Canadians. That is exactly what CSIS has been doing and will continue to do.

● (1535)

Again, thank you for the opportunity to discuss this issue with you today. I am pleased to answer any questions.

The Chair: Thank you, Ms. Henderson.

We now have Mr. Khoury, for five minutes.

Go ahead, please.

Mr. Sami Khoury (Head, Canadian Centre for Cyber Security, Communications Security Establishment): Thank you, Mr. Chair, and members of the committee, for the invitation to appear today.

My name is Sami Khoury. I'm the head of the Canadian Centre for Cyber Security, often referred to as the Communications Security Establishment's cyber centre.

CSE, reporting to the Minister of National Defence, is one of Canada's key security and intelligence agencies, with the five-part cyber-centric mandate derived from the CSE Act introduced in 2019. We use our technical expertise across all five aspects of our mandate, and we do so to keep Canadians safe and secure.

[*Translation*]

I'd like to give you an overview of the current cyber threat landscape.

Clearly, the cyber threat environment is rapidly evolving. Cyber incidents, including those involving critical infrastructure, are increasingly numerous and sophisticated.

People rely on the Internet for a growing number of important daily activities, from banking, government services and health care to business and education, which puts them at risk. We saw that during the pandemic, when people had to become more reliant on digital infrastructure. Threat actors took advantage of the pandemic and stepped up efforts to exploit human and technological vulnerabilities.

[*English*]

In addition to this increase in cyber incidents, I'd like to highlight some of the specific trends we've observed.

We assessed that cybercrime remains the most likely threat to impact Canadians. Now and in the years ahead, Canadian individuals and organizations will continue to face online fraud and attempts to steal personal, financial and corporate information. We also assessed that ransomware directed against Canada will continue to target large enterprises and critical infrastructure providers. The protection of these organizations and networks is crucial to the productivity and competitiveness of Canadian companies and vital to Canada's national defence. While cybercrime is the most likely threat to impact Canadians and Canadian businesses, the state-sponsored cyber programs of China, Russia, North Korea and Iran pose the greatest strategic threat to Canada.

● (1540)

[*Translation*]

If you'd like to learn more about the cyber threats facing Canada, I encourage you to read CSE's “National Cyber Threat Assessment 2020”.

I am aware that Russia's invasion of Ukraine is a current cause of concern for the committee. I can't comment on our specific operations today, but I can confirm that we are keeping a close eye on cyber threat activity associated with those military manoeuvres.

[*English*]

Today, we're not aware of any specific threats to Canadian organizations in relation to events in and around Ukraine. But as the situation evolves, I can assure you we continue to monitor the cyber-threat environment in Canada and globally, including cyber-threat activity directed at critical infrastructure networks.

Although the trends I have outlined today seem quite worrisome, the cyber centre is working tirelessly with stakeholders and building strong partnerships across Canada to develop a shared awareness of the threat landscape and promote the necessary measures to protect and defend against them.

[*Translation*]

We continue to provide advice and guidance—largely informed by Russian cyber threats—to help Canadians and Canadian businesses become more cyber safe.

CSE is also sharing important cyber threat intelligence with Ukraine so that it can better defend its networks.

We are working with the Department of National Defence and the Canadian Armed Forces to support intelligence co-operation and cybersecurity.

[*English*]

As Canada's cyber-threat environment rapidly evolves, we must all play our position. Cybersecurity is a “whole of society” concern. It will take all of our expertise and collaboration to protect Canada and Canadians.

Thank you again for the opportunity to appear before you today. I'm pleased to answer any questions you may have.

The Chair: Thank you, Mr. Khoury.

Thank you, Ms. Henderson.

We now go to our six-minute round.

Ms. Findlay, go ahead, please.

Hon. Kerry-Lynne Findlay (South Surrey—White Rock, CPC): Thank you, Mr. Chair.

Thank you for being here with us today. We very much appreciate it.

Ms. Henderson, what type of cyber-threats does Canada face on a daily basis and what portion of those attacks are state sponsored?

Ms. Cherie Henderson: My understanding right now is that Canada regularly suffers thousands of cyber-threat attacks on a daily basis all across the country, and numerous organizations are under that attack. I wouldn't have for you actual stats on which particular countries those are coming from. I would leave that to my colleague Sami, but what I can say.... Or the quantity...let me correct that: I wouldn't know the quantity from each particular country. Sami may have better stats on that.

What I can say is that we certainly use all of the tools that we have in our tool box to investigate any of those threats—

Hon. Kerry-Lynne Findlay: I understand that, but when I was minister of national revenue—which was some years ago now, the Liberals are happy to hear—we suffered through thousands of cyber-attacks daily at the Canada Revenue Agency. I've been told that it has proliferated since then and it's much, much more. Would you agree that it's an ever-increasing issue?

Ms. Cherie Henderson: Yes, I would. It is an ever-increasing issue, and it's something that we all need to be alive to.

As we have moved forward in technology advancement, there has been much more cyber-activity in that area and many more cyber-actors. Historically, we focused on state-sponsored attacks, but with the proliferation of tools, many more actors have entered the arena.

Hon. Kerry-Lynne Findlay: For either of you to answer this question: What sectors of Canada's economy would you say are the most vulnerable to cyber-strikes?

Ms. Cherie Henderson: I can start with that one.

This is one of the things I worry very much about. The service investigates and tries to do a lot of outreach to inform our research industries and our companies that are involved in research and development. As you know, Canada is a top leader in research and development and has a lot of very valuable intellectual property.

There are numerous countries out there that would like to get their hands on that research without having to put the money and investment into it. For all those industries, we really work on outreach to try to increase that awareness so they can protect themselves.

We are also very focused on our critical infrastructure. Critical infrastructure is necessary to maintain our day-to-day lives, and that is another area that is very vulnerable and would need to ensure a very high level of protection and awareness.

Perhaps I can pass this to Mr. Khoury for some further comments.

● (1545)

Hon. Kerry-Lynne Findlay: Do you have some comments on that, Mr. Khoury, on the most vulnerable sectors of Canada's economy?

Mr. Sami Khoury: Thank you for the question.

From the cyber centre perspective, our priority is to defend Canada against all sorts of cyber incidents, regardless of the sector, but we are paying particular attention to the critical infrastructure sectors to make sure they have the necessary tools to protect themselves.

Hon. Kerry-Lynne Findlay: I'm not sure, but perhaps Mr. Khoury is better to answer this. In terms of cyber-threats, how would you rate these state actors in their cyber-attack capabilities: China, Russia, North Korea and Iran?

Mr. Sami Khoury: In our national cyber-threat assessment of 2020, we called out the capabilities of the four of them—Russia, China, North Korea and Iran—as being state-sponsored programs of the greatest strategic threat to Canada. It's difficult to compare one against the other, but I would suggest that in the current context we have to be mindful of the geopolitical tensions and the Russian cyber-threats.

Hon. Kerry-Lynne Findlay: How would you rate a cyber-threat posed by Anonymous?

Mr. Sami Khoury: Anonymous, like many other organizations, brings a certain level of threat to the cybersecurity of a country. We've seen some of them align with Russia and some of them align with the Ukrainian cause in the context of the current geopolitical tension.

Again, we learn as much as possible from all of the incidents, and that's why we encourage all victims to report to us so that we can learn and promote new cybersecurity practices. We take all of that information, digest it and put out new advice and guidance.

Hon. Kerry-Lynne Findlay: Are you aware that Huawei was involved in a hacking attempt of Australia's telecom, Australia of course being a member of our Five Eyes alliance?

Mr. Sami Khoury: I will defer to Australia to comment about the nature of the incident that—

Hon. Kerry-Lynne Findlay: I didn't ask you for the nature of it. I said, are you aware that it happened?

Mr. Sami Khoury: We track the activities of Huawei and other telecom operators around the world, and that helps inform the security of the Canadian telecom infrastructure.

Hon. Kerry-Lynne Findlay: Are you also aware that China Telecom Americas, China Unicom Americas and ComNet have also been accused of spying for the Government of China?

Mr. Sami Khoury: Again, we track all of these reportings. They help formulate the position of the cyber centre on how to protect the Canadian telecommunication infrastructure.

Hon. Kerry-Lynne Findlay: Ms. Henderson, are you aware of the Chinese national intelligence law that makes it mandatory for state and non-state enterprises to gather intelligence for the Chinese state on demand?

Ms. Cherie Henderson: Yes, I am aware of that law. It is a law that I believe was brought in in 2017, if I'm correct. That law does compel all Chinese companies to support any requirements of the Chinese government.

Hon. Kerry-Lynne Findlay: Thank you.

The Chair: Thank you, Ms. Findlay.

Madam Lambropoulos, you have six minutes, please.

Ms. Emmanuella Lambropoulos (Saint-Laurent, Lib.): Thank you, Mr. Chair.

I'd like to thank both of our witnesses for being here to answer our questions today.

Ms. Henderson, I'll begin with you. If you believe that Mr. Khoury can answer some of the questions a little more in depth, then I'm happy to have you pass them on as well.

You mentioned that there's been an increase in the sophistication of cyber-attacks over the years, that things are only likely to continue heading in that direction, and that there are more and more of them each time. Do you believe CSIS and its partners have the tools they need in order to meet these new and sophisticated threats? Considering that things are becoming more and more sophisticated as time goes on, do you think these organizations, including yours, will be able to continue to meet these threats and counter them?

Ms. Cherie Henderson: That's a very good question. Thank you for it.

It's very important, as I think both Mr. Khoury and I have said, that every agency that has national security responsibilities is able to investigate those attacks using the tools that each agency brings to the fight, in a sense. That's why it's extremely important that we all co-operate together in order to fulfill each of our mandates. Within that umbrella, then we can successfully combat the current threat environment that we're facing.

It's also important, I believe, that all Canadians and all businesses and industries also are very aware of the cyber-threat and can then take the necessary precautions and measures to protect themselves. I think it's also important, as we move forward in the future, to make sure that we are continually looking at whether or not we do need new tools and whether or not there are ways in which we can improve. That's why we do talk about looking at modernizing, for example, the CSIS side just to see if there are new tools that we would be able to bring to bear that would help protect Canada and Canadians as we move into the future.

I would reiterate that it's extremely important that each agency co-operate and we do communicate very well together to make sure that we're all using all the tools we have in our tool kit at the moment.

● (1550)

Ms. Emmanuella Lambropoulos: Thank you very much.

Mr. Khoury, do you have anything to add to that?

Mr. Sami Khoury: I would echo what Ms. Henderson said. This is a whole-of-society effort. We learn a lot from all of the cyber-incidents in the government. From that experience, we promulgate that information to the public sector and the private sector and Canadian citizens at large and we collectively make a dent in the cost of cybersecurity.

Ms. Emmanuella Lambropoulos: Thank you very much.

Going on what you just mentioned, which was modernizing the CSIS Act, I'm wondering if there's anything you'd like to mention here—without necessarily compromising Canadian cybersecurity—that we should be looking into, even in our report and our own recommendations here at the defence committee. As well, do any obstacles currently exist that prevent us from improving the current Canadian situation?

Ms. Cherie Henderson: There are no obstacles, per se, that would prevent us. What I think we need to do is make sure that, one, we have all the tools that are necessary and are fully aware of where technology is moving and how it's developing. Then, it's also extremely important that we balance the rights and privacy of Canadians as we're moving forward.

It's a very delicate way to move forward—to make sure we have the tools to catch the bad guys but also protect the rights of Canadians. It takes quite a bit of research and study to make sure we're getting to where we are and what we need in order to protect our national security.

Ms. Emmanuella Lambropoulos: Mr. Khoury, do you have any recommendations for this particular study that you'd like to share with us today?

Mr. Sami Khoury: From a cyber centre perspective, that teamwork across government and across Canada is extremely important. Reporting cyber-incidents will be very important, so that we learn from all of those incidents that are happening and then we can up the cybersecurity of the country.

Ms. Emmanuella Lambropoulos: Thank you very much.

Mr. Chair, how much time do I have left?

The Chair: You have a little over a minute.

Ms. Emmanuella Lambropoulos: My next question is in a completely different category and has to do a little more with Russia.

We know that a lot of the cyber-threats we face are coming from Russia. A lot of the cyber-attacks are coming from Russia. I want to know how they are able to deny that they are committing such acts. Who do they use to get to and to influence Canadians in any way to think a certain way?

Ms. Cherie Henderson: What I would say is that Russia is an extremely capable threat actor. We know that Russian intelligence services have previously engaged in disinformation campaigns to discredit and create divisions in the west, to promote Russia's influence abroad, and to push for an end to western sanctions. We also know that Russia covertly gathers political economic military information in Canada through targeted threat activities in support of its own interests.

While I can't go into any specific measures, I can say that CSIS uses the full suite of its tools at its disposal to counter those Russian activities.

● (1555)

The Chair: Thank you, Ms. Lambropoulos.

We now have Madame Normandin, for six minutes, please.

[*Translation*]

Ms. Christine Normandin (Saint-Jean, BQ): Thank you, Mr. Chair.

Thank you for being here, Ms. Henderson and Mr. Khoury.

My first question is for Ms. Henderson, but feel free to jump in, Mr. Khoury, if you'd like to answer.

I'd like to know whether Canada has the capacity to track crypto currency transactions in which the sender or receiver is an illegal or terrorist group.

Ms. Cherie Henderson: Thank you for your question, but I, personally, don't have that information.

[*English*]

I would direct you to FINTRAC, which would be the better department to answer that type of question.

[*Translation*]

Ms. Christine Normandin: Mr. Khoury, would you like to answer?

Mr. Sami Khoury: I, too, was going to say that the Financial Transactions and Reports Analysis Centre of Canada, FINTRAC, would be in a better position to answer that question.

Ms. Christine Normandin: Thank you.

That brings me to another question. Would you say too much of CSE's and CSIS's work happens in isolation? That question could also apply to the armed forces. Do you think the two organizations communicate enough?

Mr. Sami Khoury: Thank you for your question.

I would say that they absolutely do. We are constantly in contact with our neighbours at CSIS and our counterparts in the Canadian Armed Forces. In fact, we support two of their missions, operations Unifier and Reassurance, so we have good lines of communication when it comes to sharing information with both of those organizations. We also work with institutions government-wide to mitigate risks to the federal government, as well as with provincial and private sector partners.

Ms. Christine Normandin: I have a more specific question on that front.

Ms. Henderson, can you give me an overview of Task Force Osprey's role within CSE? No, actually, that question would be for you, Mr. Khoury. Could you tell me more about Task Force Osprey's role?

Mr. Sami Khoury: For an answer to that question, I would refer you to the Canadian Armed Forces. If the armed forces can't answer, I can provide the information.

Ms. Christine Normandin: My understanding is that it's a group from the armed forces working within CSE. Is that right?

Mr. Sami Khoury: I would prefer to get back to you in writing, if I may.

Ms. Christine Normandin: Thank you.

My next question is for both of the witnesses.

I want to know whether Canada was forced in any way to contract out services to the private sector to meet its requirements, say because of a lack of skills, personnel or equipment. Has Canada ever had to do that?

Mr. Sami Khoury: The Canadian Centre for Cyber Security plays an important role in the integrity of our supply chains. If we had to examine the privatization of a service—within the federal government, I mean—we would have a hand in evaluating the program.

If you're talking about a domestic threat, I would refer you to Ms. Henderson, who can provide more clarity on that.

Ms. Christine Normandin: Actually, my question was more about whether CSE or CSIS had ever turned to the private sector to fill gaps in internal capacity and thus meet operational requirements.

Mr. Sami Khoury: Of course, we work with private sector stakeholders on a number of issues. In some cases, they provide us with details related to cyber threats. I would say the relationship is more complementary, but when it comes to cyber incidents, there are things that CSE does not do.

For example, the private sector is responsible for helping a victim get back on track.

Ms. Christine Normandin: Very good. Thank you.

I have a follow-up question for Ms. Henderson, but Mr. Khoury, you may wish to answer as well.

For a few years now, the possibility of setting up a foreign intelligence service has been talked about. CSIS focuses a lot more on domestic assessments. In terms of human resources, CSIS doesn't have personnel on foreign soil.

In light of the war in Ukraine and new threats facing Canada, is that an idea Canada should entertain? I'm referring to a model along the lines of the CIA.

● (1600)

Ms. Cherie Henderson: Thank you for your question. I'm going to switch languages to answer.

[*English*]

This is another very interesting question. What I would say is that, under section 12 of the CSIS Act, we can do an investigation overseas if it is determined that there is a threat to our national security. What we cannot do overseas is any activity under section 16 of the CSIS Act, which is allowing us to collect political information or economic information in the support of national defence or foreign affairs.

Under section 12—threats to the security of Canada—it's not an issue. It's under section 16 that we must remain within Canada to collect any intelligence.

[*Translation*]

Ms. Christine Normandin: Thank you.

I'll have follow-up questions the next time around, Mr. Chair.

[*English*]

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

Madam Mathyssen, you have six minutes. Go ahead, please.

Ms. Lindsay Mathyssen (London—Fanshawe, NDP): Thank you so much to both witnesses.

Thank you, Mr. Chair.

We've, of course, seen the weaponizing of social media. Here in Canada online troll farms have been set up. There's been such a sowing of distrust and hate and online conspiracy theories. We've seen them potentially interfere in our elections, and certainly within general society.

The NDP have called on the government to convene a national working group to counter online hate and protect public safety. In what ways can we make social media platforms legally responsible for furthering that mistrust and that interference in elections and those online conspiracies, and for removing that extremism before it can cause real harm?

Mr. Sami Khoury: In the "National Cyber Threat Assessment 2020", we mentioned that the Internet was at a crossroads and that we are seeing more and more misinformation and disinformation that's not limited to political campaigns or election periods. We're seeing much broader use of misinformation and disinformation. We're definitely seeing it in the context of the Russia-Ukraine conflict.

From a cyber centre perspective, we are calling out those activities. We're not a regulatory agency, so we're not here to offer a comment on the social media platforms themselves. Rather, it's about how we can work with Canadians, at large, on identifying misinformation and disinformation, on being informed readers, on making sure that they get the news from reputable sources—in terms of both a news perspective and an IT perspective—and making sure that the domain that's hosting the information is reputable too.

We put out a bulletin very recently, two or three weeks ago, specifically on disinformation and misinformation and malinformation. We hope people will read it and draw from it some nuggets of information that will help them in their information gathering or in their social media presence.

Ms. Lindsay Mathyssen: So you're putting the onus upon individuals themselves. You don't see any role, per se, in terms of what role social media companies need to play in this. Is that what you're saying?

Mr. Sami Khoury: From the cyber-centre perspective, our role is to defend the country from cybersecurity incidents and give Canadians and Canadian businesses the necessary tools to raise the cybersecurity bar.

We are not an agency or a centre that is here to regulate social media. I will defer to other government agencies to maybe answer that element of the question.

Ms. Lindsay Mathyssen: Okay.

Ms. Henderson, do you say the same as Mr. Khoury, or something slightly different?

Ms. Cherie Henderson: I believe that Mr. Khoury has answered the question. Neither of our two agencies is here to regulate social media platforms. That is the responsibility of other departments and perhaps society as a whole, as to how we want to manage that situation.

● (1605)

Ms. Lindsay Mathyssen: Okay. Changing topics a little bit, in terms of recruitment and retention, we have certainly heard a great deal about the challenges that the Canadian Armed Forces has in that regard.

Can you comment on whether or not CSIS has faced similar challenges in terms of recruiting and ensuring that we have the necessary talent within the ranks to tackle those cyber-threats that we're discussing today.

Ms. Cherie Henderson: CSIS has a very active recruitment program to look for the right talent, and we are always exploring new ways to find the right talent and bring them into the service.

There are many Canadians out there who are extremely interested in working in national security in our department, and we are finding ways to encourage them to join and encourage them to stay. You mentioned retention. With the changing work environment, that sometimes gets a little challenging in a national security world, but we are looking at all avenues to recruit and retain our staff.

Ms. Lindsay Mathyssen: Earlier at our committee, several weeks ago now, we had an expert come before us, Christian Leuprecht, from RMC. He told the committee that there simply aren't enough resources to attract talent into the Canadian Armed Forces. He said that the CAF, for example and specifically, is competing against about 200,000 unfilled cyber-positions in North America.

Again, that challenge is getting the right people through the door and interested in the idea of national security. Does CSIS find the same problems and issues in terms of that huge competitive nature of the industry?

Ms. Cherie Henderson: CAF is a much larger organization than we are, so they would have much different types of recruitment challenges than we do. We certainly have witnessed a huge interest in working for this service just from the volume of applications that come to us on a regular basis.

The Chair: Thank you, Ms. Mathyssen. That completes the first round.

The second round starts with Mr. Doherty.

I see that we have 25 minutes' worth of questions and 20 minutes. I'm going to let it go at five minutes a pop and we will just start late.

Mr. Doherty, you have five minutes.

Mr. Todd Doherty (Cariboo—Prince George, CPC): Thank you, Mr. Chair, and thank you to our guests for being here.

I will pose this question to both Mr. Khoury and Ms. Henderson. It's very straightforward.

Does Huawei pose a threat to Canadian safety and security?

Mr. Sami Khoury: From a cyber-perspective, the security of the telecom infrastructure is something we take very seriously. The government is conducting an examination of these emerging technologies and notes that a decision will be announced in due time.

In the meantime, we are working with partners and other agencies to mitigate the risks stemming from the use of these designated technologies, including the Huawei entity.

Mr. Todd Doherty: Ms. Henderson.

Ms. Cherie Henderson: I'm not going to speak specifically to Huawei, but I would note, further to a response to a question I answered earlier, that the Chinese national security law compels any of these companies to engage in activities in support of the government's requirements.

Mr. Todd Doherty: That's why I asked that question. I get it.

Further to that question and that comment, Ms. Henderson, would you say that certain policy positions in recent years have hurt our standing within the Five Eyes? Are we being left out of important meetings because we still have Huawei at the table and are still partnered with Huawei?

Ms. Cherie Henderson: What I would say is that right now, the Government of Canada is engaged in an ongoing review that's being led by Public Safety and it's determining the Canadian approach for the implementation of 5G technology and telecommunications networks.

Mr. Todd Doherty: Do you believe our allies see this as a threat and have concerns over Huawei still being at the table with Canada?

Ms. Cherie Henderson: All of our allies have taken different approaches to 5G and to Huawei and to the implementation, and they're adopting various mitigation measures to protect their national security in response to the needs of their unique environments, and we all continue to talk and work very closely together.

● (1610)

Mr. Todd Doherty: Do you feel there are concerns among our allies with respect to Huawei and Canada's partnership with them?

Ms. Cherie Henderson: I couldn't speak to what the allies are thinking at this point, but what I can say is that we all work very closely together.

Mr. Todd Doherty: How would you define, for lack of a better term, a cyber-Pearl Harbour attack, and are we prepared for it?

Ms. Cherie Henderson: We work very closely with our partners around the world as well as with our domestic partners to really educate and inform the critical infrastructure, the various business enterprises, industry and our own government departments to shore up their resources and protect their cybersecurity, and we constantly work together to learn about new ways in which we may be attacked so that we can prepare and help support all of our departments to protect themselves against a massive cyber-attack.

Mr. Todd Doherty: What keeps you up at night?

Ms. Cherie Henderson: Lots of things keep me up at night.

Mr. Todd Doherty: What is the perfect storm and what keeps you up at night with respect to our national security and the cyber-attacks and cyber-threats?

Ms. Cherie Henderson: I would say at the moment that we are all working extremely hard and closely monitoring the current situation and environment, and monitoring the advances in technology so that we can make sure we have the defences to protect ourselves. We are only as strong as the weakest link, which means we really need to work together, educate, and learn from anybody's mistakes so we can shore up everything and protect ourselves today and into the future. It's a constantly evolving environment, and we can never let our guard down, because there is always a threat actor out there that would be willing to try to take advantage of our systems and our country and to have a hugely negative impact on our national security.

Mr. Todd Doherty: I won't put words into your mouth, but you've said that we're only as strong as our weakest link. Would you say that Canada is viewed as a weak link within our Five Eyes system because we are still considering Huawei and in negotiations with Huawei?

Ms. Cherie Henderson: No, I would not, because as I noted earlier, every country needs to find the mitigation measures that work in its specific instance, and we all work extremely closely to share information to make sure that we're all helping each other protect ourselves as we move into the future.

The Chair: Thank you, Mr. Doherty.

Mr. Todd Doherty: Thank you.

The Chair: Mr. Fisher, what keeps you up at night? You have five minutes to tell us.

Mr. Darren Fisher (Dartmouth—Cole Harbour, Lib.): Thank you very much, Mr. Chair. I won't get into what keeps me up at night, but I'm sure it's not at the same level as that of our amazing witnesses.

Thank you very much for being here and for your testimony.

I was trying to read an awful lot to prepare for today's meeting. There's an awful lot here dealing with cyber-threats and cybersecurity, and in fact I will throw a compliment out to Ms. Gallant across the way. When I was first on the National Defence committee, she was one of the members leading the charge on cyber-threats and cybersecurity, and I did learn quite a bit from her.

Some of the reading I've done talked about Canada being almost collateral damage when it comes to cyber-threats and cybersecurity, basically on the basis of our proximity to the United States and our connections to the U.S.

I will ask this of both of you, maybe starting with Ms. Henderson. Is that still true, now that we've just unleashed significant sanctions on Russia? None of us around this room is welcome in Russia anymore for our summer vacations. Are we more than collateral damage now that we have enacted those massive sanctions against Russia and its oligarchs?

Ms. Cherie Henderson: As I noted earlier, we work really closely with our partners because, as Mr. Doherty pointed out, I did say that we're only as strong as our weakest link, and because we all work so closely together to share each other's experiences, to learn and to develop, I would not say that we were collateral damage. I would say that we are a partner and we work closely with our allies to build those partnerships and our knowledge and awareness.

● (1615)

Mr. Darren Fisher: Okay.

I wasn't sure if Mr. Khoury was going to chime in on that, but that's fine. Thank you for that.

Mr. Sami Khoury: I was going to echo what Ms. Henderson said.

Mr. Darren Fisher: Okay. That's excellent.

Many state actors are now contracting out to criminal networks, for instance, as we hear about Russia on a regular basis. How are we to follow up on state actors when they're contracting out their cyber-threats around the world?

That's for whomever wants to answer.

Mr. Sami Khoury: I'm happy to maybe take a first crack at that.

We are aware of the connection between the Russian intelligence services and cybercriminal organizations. That is something we identified in our national cyber-threat assessment of 2020 and more recently in the context of the Ukraine and Russia conflict.

We have seen cybercriminal organizations take sides one way or another. From a cyber centre perspective, we have the task of defending the country, defending Canada and defending critical infrastructure against all sorts of threats, irrespective of whether they are by nations states or cybercriminals, and to promote cybersecurity across the board.

Obviously, calling out a country for cyber-activity is a whole-of-government...and GAC has the lead on the attribution framework. We would provide, from a cyber centre perspective, one piece of input to the dossier that will help the Department of Foreign Affairs, GAC, make the determination on naming a country more publicly.

Mr. Darren Fisher: In 45 to 60 seconds, can one of you help me better understand “ethical” hackers? What is an ethical hacker?

Mr. Sami Khoury: I would say that it's a hacker without ill intent. It's somebody who will hack into a system to discover a vulnerability and then report it to the system owner and say, “I found this vulnerability in your system and here's how you should fix it.” That's opposed to a hacker who goes in and steals information and then maybe holds it for ransom or damages the system.

Mr. Darren Fisher: That's really helpful. Thank you.

I think I know the answer to this, but where do most cyber-attacks or attempted cyber-attacks come from? More importantly, how do we defend against them as a country?

Mr. Sami Khoury: Cyber-attacks, from the perspective of the cyber centre, come from pretty much everywhere. We defend the government against cyber-attacks that come from everywhere, and also for different intents, be they state sponsored or criminal. To defend is to raise the bar and to put out, as much as possible, timely information. The measure of success here would be how quickly we detect it, how quickly we mitigate the incident and how quickly we turn it into a lesson learned so that we can help protect Canadians.

The Chair: Thank you, Mr. Khoury and Mr. Fisher.

Madame Normandin, you have two and half minutes to continue this shocking outbreak of collegiality.

[*Translation*]

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

I'm going to follow up on two of my earlier questions. The first relates to FINTRAC.

Should CSE and CSIS co-operate more closely with FINTRAC to follow the money when it comes to the use of cryptocurrency by terrorist groups?

Mr. Sami Khoury: Thank you for your question.

We work closely with our FINTRAC colleagues, but we don't have a mandate to investigate. Oftentimes, cyber currency is used in cases involving ransom or other criminal activity, so I would refer you to the RCMP. This is more their responsibility.

Ms. Christine Normandin: Very good. Thank you.

Ms. Henderson, you brought up section 12 of the CSIS Act, which provides for overseas activity. I realize that the act provides for the possibility, but what I want to know is whether it would be a good idea to establish a service on a permanent basis. In other words, should a permanent foreign intelligence service be created to give CSIS a broader reach internationally?

● (1620)

[*English*]

Ms. Cherie Henderson: CSIS is a domestic intelligence agency. As I said, we have the ability and the authority to investigate any threats overseas that are a threat against our national security. We do have representation overseas, as is publicly acknowledged—we have an officer in Paris, London and Washington—that supports any of the working relationships with our partners overseas.

We do have the ability to investigate to protect our national security.

[*Translation*]

Ms. Christine Normandin: My last question is for the both of you. It's a quick one.

As you know, some cyber-attacks are meant to extract payment of a ransom, and others are designed to destabilize a country.

How would you break down the cyber-attacks against Canada?

Mr. Sami Khoury: It's hard to put a figure on the number of incidents because they are under-reported. Not all cyber-attack victims report the incidents to us. I can talk about attacks against the government or its attack surface, but it's hard to draw a comparison with ransom-based attacks.

That said, the government is certainly an attractive target.

Ms. Christine Normandin: Thank you. I think that's all my time.

[*English*]

The Chair: Ms. Mathyssen, you have two and a half minutes.

Ms. Lindsay Mathyssen: Thank you.

Media reports have cited unnamed U.S. officials as saying that China has signalled a willingness to provide economic and military supports, potentially, to Russia's attack in Ukraine. What is the likelihood, in your estimation, that China would extend that support, perhaps or potentially in the form of co-operation on cyber-operations when it's targeting western nations—Ukraine and western allies?

That would be for both of you, I would say.

Mr. Sami Khoury: We know from, again, the cyber-threat assessments that China has a state-sponsored cyber program in the same way as Russia. We have to defend the government, and more broadly Canadian society, against both threats, be it a strategic threat against the government or international property theft or things like that.

On the nature of the relationship between Russia and China, I would defer to our intelligence colleague, who might be in a better position to speak about it.

Ms. Cherie Henderson: I wouldn't want to speak particularly about the relationship between China and Russia, but I would say that both of them are extremely capable threat actors who will operate in their interests and what works best for their requirements.

The Chair: Mr. Motz, you have five minutes.

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

Thank you to the witnesses for being here.

It's nice seeing you again, Ms. Henderson. Hopefully, my question doesn't put you on the spot.

First, I will deal with a question from NSICOP, the National Security and Intelligence Committee of Parliamentarians. In their report, which I won't get into, because it's a long one, they cited and described the 2017 cyber breach of the Department of National Defence network that resulted in a theft by a state actor of significant amounts of information. The network in question was not part of the Shared Services Canada enterprise internet service, and therefore lacked protection by CSE's network sensors.

I'll ask you first, but I'm sure Mr. Khoury will weigh in as well. Importantly, the compromised network contained legacy technology that could not be patched and was therefore vulnerable to cyber-threats. Are DND and the Canadian Armed Forces now using up-to-date and fully patched technologies in all of their systems and networks?

Ms. Cherie Henderson: I wouldn't be able to answer that question. I don't know if Mr. Khoury would have a response for you on that front.

Mr. Sami Khoury: I would defer to DND to answer that question on the specific state of their IT.

Mr. Glen Motz: I appreciate that from both of you. I know you have to be careful, but I mean, it was your organization that identified the problem. Are you still as alarmed that the problem exists that they still have some security vulnerabilities with unpatched technology?

Mr. Sami Khoury: We have worked tirelessly with DND but also with the rest of government to increase the coverage of the sensors that the cyber centre has made available to the government for defence. Definitely we are in a much better space today than we were in 2017.

As far as technology and legacy systems are concerned, I will defer to DND. They know their environment best to say whether or not certain technologies have been updated.

● (1625)

Mr. Glen Motz: Fair enough.

You mentioned just a second ago, Mr. Khoury, when I asked you how prevalent the issue is of unpatched legacy software in the federal systems and networks more generally, you said that you're getting better. Do we still have some vulnerabilities? I do not want you to identify them, but how are we doing as compared with even two or three years ago?

Mr. Sami Khoury: I would say we're much, much better, but patching a system is not without risk. Every department, including Shared Services and others, has to weigh in the impact of patching a system. Sometimes it breaks technology, or it breaks systems currently in use. I will defer to them to assess it.

We have put together quite a slew of security capabilities to protect the federal government that we're very proud of, at this point.

Mr. Glen Motz: Great.

As part of Canadian Armed Forces Operation Unifier, CSE is sharing threat intelligence with Ukraine and helping Ukraine defend itself against cyber-attacks. Are CSE and/or the Canadian Armed Forces engaging in active cyber operations as part of Operation Unifier?

Mr. Sami Khoury: When we have seen cyber-activities directed against Ukraine, we have shared those cyber indicators with Ukrainian officials so that they can better defend their networks. Beyond that, on the question of cyber operations, I am unfortunately unable to answer that.

Mr. Glen Motz: Okay. Fair enough.

On February 25 of this year, a day after Russia invaded Ukraine, Conti Group, a Russian-affiliated organized crime organization that specializes in ransomware attacks, pledged its support for the invasion, and threatened retaliation for any war activities directed at Russia. Other ransomware groups joined Conti Group in its pledge of support.

How have the threats of retaliation from Conti Group and other ransomware groups affected Canada's cyber-defence planning?

That question is for both of you.

Mr. Sami Khoury: We are familiar with the Conti Group. They were active in Canada pre-invasion, so we have a good body of knowledge on how to defend against them. We launched a major campaign on ransomware in December to call attention to the problem. As a follow-up to the Russian invasion of the Ukraine, we've twice issued threat bulletins to critical infrastructure operators, calling attention to the threat posed by Russia and Russian-affiliated groups, to better defend themselves.

We're constantly learning from what is going on out there, updating our advice and guidance, updating our threat feeds and our indicators of compromise, and defending—

The Chair: Thank you, Mr. Khoury and Mr. Motz.

Mr. May, go ahead for the final five minutes, please.

Mr. Bryan May (Cambridge, Lib.): Thank you very much, Mr. Chair.

Thank you to both of our witnesses this afternoon.

Mr. Khoury, can you comment and elaborate on the Canadian Centre for Cyber Security's work with various industry sectors?

Mr. Sami Khoury: Yes. While the cyber centre's primary mission is to protect the government and lead the response to cyber incidents, we work side by side with the public and private sectors. We have a number of engagement platforms with the sectors through sectoral tables, be it energy, electricity or health care. Some meet more regularly than others. With the health care round table, which includes the cross-Canada health care community, the hospitals and the clinics, we meet weekly if not every other week.

With the electricity sector, we have started a pilot called Lighthouse for them to appreciate the threats posed to their networks. Likewise, we have another pilot with the Canadian Gas Association where we work collaboratively for them to appreciate the threats to their landscape.

Beyond that, we also care about national-level outcomes. We have worked with the Canadian internet registry to make available, free of charge to Canadians, a protective DNS service so that when you browse online, if you point to the Canadian shield, you can be assured that there is no malicious website where you are going. We have a pretty broad engagement program with the private sector.

● (1630)

Mr. Bryan May: Thank you.

Which critical infrastructure sectors would you say are best equipped to defend against cyber-attacks?

Mr. Sami Khoury: It's difficult to compare one sector against another. The threats could be different. Our role at the cyber centre is to make sure we pass on all the information to all the critical sectors—be those finance, energy, transportation or health care—and to make sure they all have the necessary tools to protect themselves in the event of a cyber-attack. It's difficult to simply say which one is better prepared than the others.

Mr. Bryan May: I appreciate that, but maybe a better way to ask that is which sectors need to significantly improve, in your opinion? Which need more work, and how do we help them raise that bar?

Mr. Sami Khoury: There's a program under which we can work with the various entities to assess their cybersecurity maturity, and we're happy to work with all of them. Every sector needs something different, so the programs that we tailor to, for example, municipal engagement, are different from the programs we tailor to the banking sector. We have to cover the entire waterfront of Canadian sectors so we can make sure they're all protected.

Mr. Bryan May: To answer my last question, both of you can weigh in if you each takes about 30 to 35 seconds, which may not be fair. Would, in your opinion, reporting requirements such as those recently enacted in the United States improve the situation in Canada?

Mr. Khoury, you can start.

Mr. Sami Khoury: We know that ransomware incidents are under-reported, so we encourage everybody to reach out to us, whether an incident is big or small, to share with us the nature of the cyber-incident so we can learn from it and quickly turn around to mitigate the threat across Canada. The more reporting, the better it will be to raise the collective bar across Canada.

Ms. Cherie Henderson: I would second that. I fully believe that we really need to have open communication, to discuss and raise the issues and to encourage anybody to report an incident. Many companies are very uncomfortable and think it will reflect very negatively on them, but all of that can be managed in a secure manner so we are not giving out identities but are collecting as much information as possible to protect them and other companies.

Mr. Bryan May: Thank you both very much.

The Chair: On behalf of the committee, I want to thank both of our witnesses, Mr. Khoury and Madam Henderson, for their contribution to our threat analysis study. Cyber is unique in that it seems to be awfully difficult to wrap our heads around what's going on given its nature, which is both obscure and pervasive. Thank you for your insights and your work on behalf of our nation.

With that, we're going to suspend while we assemble the next panel. Thank you.

● (1630)

(Pause)

● (1635)

The Chair: In this next panel we have Benoît Dupont, professor and Canada research chair in cybersecurity at the Université de Montréal; and John Hewie, national security officer with Microsoft.

I'm going to call on each of you for your five-minute statements.

We're going with Professor Dupont first for five minutes.

Go ahead, please. Thank you.

[*Translation*]

Dr. Benoît Dupont (Professor and Canada Research Chair in Cybersecurity, Université de Montréal, As an Individual): Thank you, Mr. Chair and members of the committee, for inviting me to appear before you. I will be making my opening remarks in French, but I would be happy to answer questions in both official languages.

I am a professor at the Université de Montréal and Canada research chair in cybersecurity. I am also the scientific director of the Human-Centric Cybersecurity Partnership, a group of 30 or so cybersecurity researchers, and government and private sector partners, including Microsoft.

Like other witnesses who have appeared before the committee, I want to focus on the technological changes that are currently redefining the parameters of the military conflicts in which Canada is, or will be, involved. With the invasion of Ukraine, cyber-attacks and disinformation are, of course, top of mind. Looking further ahead into the future, I would point out that digital technologies such as artificial intelligence, 5G networks, the Internet of things, quantum computing and the advent of neural interfaces are also challenges that have the potential to radically alter armed conflicts.

With these predictable changes on the horizon, we must think about the strategies that need to be put in place now to prepare. It is essential to consider the medium- and long-term policy implications of these technologies and anticipate their role in future conflicts, for instance, in 2025 or 2030. We must start preparing now, by acquiring new technical capability and by recruiting and training the people who will be called on to leverage that capability. This foresight work is crucial if our armed forces are to adapt proactively to a constantly changing environment.

These technological changes must go hand in hand with fundamental changes in the recruitment and training of cybersecurity experts, whose role will become increasingly important. The general labour shortage in this field—which I believe my colleague Christian Leuprecht talked about—is affecting the private sector, so the armed forces will have to be creative if they are going to attract skilled workers. Some countries have already introduced specific recruitment strategies for their armed forces, while others have opted to build reserve forces with specialized skills to quickly mobilize skilled personnel in times of crisis. To my knowledge, Canada's examination of the issue is still in its infancy.

Beyond human resources, it is crucial that Canada develop digital sovereignty in defence, specifically over key areas such as artificial intelligence and quantum computing where Canada leads the way in research but lags behind in industry. That involves the deliberate development of industrial innovation ecosystems that can contribute to Canada's defence and that of its allies. I want to draw your attention to the AUKUS security pact between the U.S., the U.K. and Australia, a pact that Canada was not invited to join. Announced in September 2021, the arrangement focuses on more than providing nuclear-powered submarines to Australia; it calls for a very high level of integration across the three countries' R and D and commercialization efforts in the strategic areas of cybersecurity, artificial intelligence and quantum computing.

In conclusion, the cyber threat landscape is becoming increasingly complex and adversaries are stepping up their cyber-attacks. These challenges cannot be dealt with effectively using traditional solutions, whose limitations have become painfully clear. The innovative solutions we need cannot simply be carbon copies of those our neighbour and allies have devised and implemented. We must genuinely engage in a process to thoroughly examine our interests, resources and strategies if we are to implement the bold measures needed to make up for lost ground.

● (1640)

The Chair: Thank you, Mr. Dupont.

[*English*]

Next, we have Mr. Hewie from Microsoft.

Mr. John Hewie (National Security Officer, Microsoft Canada Inc.): Good afternoon, Mr. Chair, Mesdames Vice-Chairs.

Let me begin by thanking you for inviting me to appear today to inform this committee on the cyber-threats affecting Canada, and the Canadian Armed Forces' operational readiness to meet those threats.

My name is John Hewie. I'm national security officer with Microsoft in Canada.

One of our principal and global responsibilities as a company is to help defend governments and countries from cyber-attacks. Seldom has this role been more important than during the past weeks in Ukraine. All of us at Microsoft are following closely the tragic, unlawful and unjustified invasion.

This has become both a kinetic and digital war, with horrifying images as well as less visible cyber-attacks on computer networks, accompanied with Internet-based, state-sponsored disinformation campaigns.

Our single most impactful work in this area in Ukraine has been assisting with the protection of Ukraine's infrastructure against Russian cyber-attacks. These ongoing cyber-attacks have been precisely targeted, and we are especially concerned about those on Ukrainian civilian digital targets, including critical infrastructure, emergency response services and humanitarian aid efforts. We have deployed cybersecurity technical protections to dozens of targeted organizations in concert with the Ukrainian government. We are also assisting organizations in Ukraine to move services to the cloud so they may continue to potentially operate from outside of the country. Our disaster response teams have also been supporting numerous groups that are providing aid to the Ukrainian people.

Our efforts have involved constant and close coordination with the Ukrainian government, the European Union, the U.S. government, NATO and the United Nations. We are committed to supporting Ukraine and helping to protect its government, citizens and our employees.

While the events in Ukraine certainly have the world's attention, other cybercriminals continue targeting and attacking all sectors of critical infrastructure, including public health, information technology, financial services and the energy sectors. Ransomware attacks are increasingly sophisticated and successful at crippling governments and businesses. The profits from these attacks are soaring, which leads to fuelling criminal and state-sponsored financial interests. Global estimates indicate that the cost of data breaches worldwide will reach in excess of $5 trillion by 2024.

During the past year, 58% of all nation-state cyber-attacks observed by Microsoft have been attributed to Russia, followed by North Korea, Iran and China. Russian actors are increasingly targeting government agencies involved in foreign policy, national security and defence for intelligence gathering.

The SolarWinds compromise at the end of 2020 by a Russian actor is an example of the increasing and concerning attacks observed against the supply chain. These and other insights are further detailed in the second annual Microsoft digital defence report, which provides our view into the global cyber-threat environment.

Microsoft recently made an unprecedented global commitment to invest $20 billion in cybersecurity over the next five years. Our overall security strategy has a comprehensive approach across diplomacy, by promoting digital peace and advocating for norms of acceptable behaviour in cyberspace, disruption of cybercriminal infrastructure using innovative civil litigation and law enforcement partnerships and, of course, defensive cyber-attacks that target Microsoft and our customers globally using advanced cloud technology—a zero-trust approach to security that involves information-sharing partnerships and thousands of highly skilled people.

Good examples of partnerships are our 15-year relationships with Canada's Communications Security Establishment and now the Canadian Centre for Cyber Security, where we share information on emerging threats and cyber-defence techniques enabled through the Microsoft government security program.

As we look around us, it's apparent that digital technology plays a vital role in almost every aspect of our lives. Microsoft's mission is to empower every person and every organization on the planet to achieve more. We can only do so by protecting the digital world we all use. What has become very clear to the world is that cybercrime and state-sponsored attacks are critical threats to national security and Canada's economy. No single entity can combat these threats effectively on their own. Working together with industry, academia, civil society and government, in Canada and internationally, is paramount.

As a company at the forefront of cybersecurity, we are here to support, build knowledge and expertise, and play a key role in helping to enhance preparedness for Canada, the whole of government, including the Canadian Armed Forces.

Thank you, members of the committee, for your time and attention. I welcome your questions.

● (1645)

The Chair: Thank you to both of you.

This is the six-minute round.

Colleagues, I'm looking at the clock, and there's not a snowball's chance that if we put six minutes and the other five-minute round in, we'll be anywhere close to being finished, so I'm going to start with a five-minute round.

With that, Mr. Doherty, you have five minutes.

Mr. Todd Doherty: Thank you to our guests for being here today.

Mr. Hewie, I'm glad you brought up the 2021 SolarWinds cyber-espionage incident. In your opinion, what responsibility should software and information technology providers have in ensuring their products and service offerings are truly secure?

Mr. John Hewie: Thank you for that question.

Certainly, technology providers have a critical responsibility to ensure that their software and services are as secure as possible. Microsoft takes this responsibility extremely seriously.

While we have led the world and led technology organizations worldwide with the development of and education around things like the security development life cycle, which Microsoft pioneered over a decade ago, and of course with continued improvements around information-sharing and partnerships with organizations and governments around the world, and working with our competitors, including Amazon, Google and many others across the security community, in doing our absolute best to build reliable and trustworthy software, we're really, quite frankly, up against adversaries that are very determined, very patient and very well funded.

Software today is incredibly complex, and while we aim to minimize vulnerabilities in software, it is a task that we're continuously vigilant on and continue to work towards.

Mr. Todd Doherty: One of the things that is interesting is that we have had quite a bit of testimony that there's a drastic shortage in manpower, and also in that next generation of cybersecurity experts with those skills. As we move forward in the next eight years, we're seeing that there are going to be about 3.5 million jobs open globally.

What is Microsoft doing to help fill that gap not only within North America but worldwide?

Mr. John Hewie: Thank you.

It's a great and in fact very important question. We are also acutely aware of that resource and skilling shortage across the security community. We're taking a number of steps.

Here, specifically in Canada alone in the last year, Microsoft has invested millions of dollars in the security skilling, tools and programs to help bring new individuals and much more diversity into the security space here in Canada. We have partnerships in supporting various academia and academic institutions across the country with skilling programs and I think we're trying to build awareness across the broader community that this is not simply something that's going to be solved by technical nerds who know how to configure networks. There are legal issues, civil rights issues and just a diversity. We need a broad range of thinking brought in to fill this skills gap to, together, help combat this problem.

Mr. Todd Doherty: On the 28th of February, Microsoft president, Brad Smith, posted the following information:

> Several hours before the launch of missiles or movement of tanks on February 24, Microsoft's Threat Intelligence Center...detected a new round of offensive and destructive cyberattacks directed against Ukraine's digital infrastructure. We immediately advised the Ukrainian government about the situation, including our identification of the use of a new malware package (which we denominated FoxBlade), and provided technical advice on steps to prevent the malware's success.

When and under what circumstances did Microsoft's threat intelligence center begin working with the Ukrainian government?

● (1650)

Mr. John Hewie: Microsoft's threat intelligence center tracks a number of actors around the world on a constant basis. We've been doing that for a number of years, and that's really to help inform not just how we build cybersecurity protections into our products and services but to help inform and provide intelligence to our various customers around the globe.

Mr. Todd Doherty: Who is behind FoxBlade?

Mr. John Hewie: I don't believe I have details at hand on exactly whom we've attributed FoxBlade to, but that was certainly a malware wiper attack that was targeted at the Ukrainian infrastructure.

Mr. Todd Doherty: What was the objective and was it achieved?

The Chair: Please be very brief.

Mr. John Hewie: From what we're seeing, the FoxBlade wiper is a good example of what appears to be a ransomware-type attack on infrastructure, but is actually a destructive attack. While the intention is to encrypt data, there is no ability to restore that data or an intention on the part of the adversary to actually ransom the victim.

The Chair: Thank you, Mr. Doherty.

Mr. Spengemann, you have five minutes, please.

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

I thank both of our witnesses for being with us this afternoon.

This is an extremely complex area, as you and our previous witnesses have outlined. It's highly interdisciplinary. We're talking about the establishment of an ecosystem that, in many parts, has not been established yet, or has been insufficiently established. Then we have the Russia-Ukraine invasion, which has brought everything to a point and illustrates the urgency with which we need to look at this issue.

This goes into the private sector, into public civilian infrastructure, and into the military side. We saw, through the response of the European Union, Canada and many of our allies with respect to the application of sanctions, how quickly the private sector and the capital markets are implicated in a security question.

I'd like each of you to take a moment and give us a thumbnail sketch of the state of this ecosystem at the moment, looking at these complexities and interdisciplinarities. What needs to be done urgently, from the perspective of the federal government? What are some of the challenges, operationally, with respect to human resources, changing our mindset, and looking at digital security as an urgently needed and, ideally, rapidly growing area of investment?

If you could zoom back to your initial comments with a bit more depth for 45 seconds each.... I have limited time, and that would be helpful.

The Chair: Five hours, at least.

[*Translation*]

Mr. Sven Spengemann: Professor Dupont, you can go first, followed by Mr. Hewie.

[*English*]

Dr. Benoît Dupont: The Government of Canada just announced an $80-million investment in the cyber security innovation network through ISED. I think this is a great initiative, because it's going to bring together more than 120 academics and industry partners from the private sector and from the provincial, municipal and federal governments. I think this needs to be supported and probably accelerated, as well.

In terms of training, we need to bring in people from all kinds of disciplines, since you mentioned it's an interdisciplinary approach. When we reviewed all of the disciplines involved, we identified more than 40 disciplines, from public health and political science to psychology and computer science, of course. I think we need to foster a lot more engagement in cross-disciplinary work in Canada and to think about how this could be put to work to protect Canadian assets, vulnerable groups and critical infrastructures.

Mr. Sven Spengemann: Thank you very much.

Go ahead, Mr. Hewie.

Mr. John Hewie: I would build on what my colleague just said. Absolutely, no single entity can combat these threats on its own. We heard similar themes from the previous witnesses. We need strong collaboration across government, industry and academia, both domestically and internationally.

I think it's important to recognize that, when we're talking about cyberspace, the private sector—private industry, especially cloud service providers like Microsoft—operates much of that infrastructure. It's what the Canadian Forces would call the “cyber battlespace”. We certainly have a unique view, and it's probably a different view from what government organizations have. By working together, we can really complement each other's abilities to defend and protect customers, organizations, governments and all Canadians in that space.

● (1655)

Mr. Sven Spengemann: Thank you both very much.

I have about a minute and a half left.

Briefly, on a more defence-related issue, what are the views of each of you on offensive capacity, with respect to the cyber domain?

Mr. John Hewie: Maybe I'll go first.

There's a short answer from Microsoft. Microsoft does not condone or involve itself in offensive cyber-activities.

Mr. Sven Spengemann: Thank you very much.

[*Translation*]

Mr. Dupont, could you answer that?

[*English*]

Dr. Benoît Dupont: This is something I have very little information about. I work in academia, so this is something that is very remote from my work.

Mr. Sven Spengemann: Okay, that's helpful. That leaves me a bit more time.

When we look at interdisciplinary connection points with respect to cyber-attacks, how stovepiped is our system, and how separate are the various stovepipes that need to respond to this? How well are they coordinated at the moment?

Dr. Benoît Dupont: There is a real effort to try to coordinate with the Canadian Centre for Cyber Security and through other initiatives, but it's probably still lagging. This is such a complex issue, and we probably need to inject a lot more effort, energy and money into it.

I think a lot more work remains to be done. A lot of people are very much aware of the need to de-silo all of those isolated groups.

The Chair: Thank you.

Mr. Sven Spengemann: Thanks very much, Mr. Chair.

[*Translation*]

The Chair: Ms. Normandin, you may go ahead. You have five minutes.

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

Professor Dupont, you said that Canada's industry was lagging behind. The SolarWinds incident came up earlier. FireEye, a U.S. think tank, uncovered the breach.

Is that the sort of initiative we don't have in Canada, or are the deficiencies more on the government's end?

Alternatively, is it the balance and co-operation between the two where the deficiencies lie?

Dr. Benoît Dupont: FireEye is a private firm, not a think tank. It has more or less the same type of expertise as Microsoft.

I think Canada is behind because security and cybersecurity issues are not high on the political agenda. They are considered important, but not necessarily seen as priorities that need to be dealt with at the highest political levels, unlike in other countries, where the office of the president or prime minister plays a direct role. That's where we differ from our allies.

Ms. Christine Normandin: That brings me to my next question.

Can you list some countries whose leads we could follow in terms of developing cyber capacity in the military and other sectors?

Dr. Benoît Dupont: We could certainly look to Europe for some worthwhile initiatives. The U.K.'s armed forces, for instance, created a cyber reservists unit to attract people from the private sector to work on matters of national security on a temporary basis.

My colleague Christian Leuprecht mentioned something Germany is doing. The country established a specific recruitment pathway to attract people to careers in the military. They obtain the rank of lieutenant-colonel and gain very specialized skills to speed up their integration. France set up a cyber defence reserve as well.

Certain countries have introduced really positive measures, and some of those countries are comparable to Canada in size and don't necessarily have the unlimited resources the U.S. has. We can look to initiatives of those countries as models.

Ms. Christine Normandin: Are initiatives like those precisely why the countries in AUKUS are part of the pact, unlike Canada, which is not a member and is lagging behind?

Dr. Benoît Dupont: Yes. It does indeed depend on how much of a priority the country has made the issue and its level of investment in recent years.

Ms. Christine Normandin: I'm going to pave the way somewhat for our next study.

You mentioned recruitment. Should the Canadian Armed Forces reconsider its recruitment requirements when seeking out people with specialized skills?

Should the armed forces get rid of training components that focus more on technical skills or on-the-ground operations? Should it avoid sending people on postings, which are a deterrent for many?

Should the armed forces put more focus on skills than on general military training?

Dr. Benoît Dupont: When very specialized skills are needed, people want assurance that they are going to stay in their position for a number of years.

Remuneration is another important consideration. Even though those who consider a career in the armed forces are not motivated by money, it's still important to offer them competitive pay vis-à-vis the private sector, which has the ability to pay people in the field very well. It's important to think about the system for compensating people with these special skills.

● (1700)

Ms. Christine Normandin: In your opening statement, you brought up digital sovereignty. Can you clarify what you mean by that?

Do you mean that digital matters should be the domain of the government?

Does that open the door to co-operation with the private sector?

Dr. Benoît Dupont: When I talk about digital sovereignty, I'm talking about Canada developing its own businesses and capacity so that it can produce Canadian technologies and services in response to strategically important technological needs. This means helping to build Canadian companies and industries with the ability to not only sell their products outside the country, but also supply our armed forces with technologies we can have full confidence in.

Ms. Christine Normandin: You mean regardless of the public or private dimension.

Dr. Benoît Dupont: That's right.

Ms. Christine Normandin: I see. Thank you.

I'm almost out of time, but there may be enough for you to answer my next question.

When the experts analyze cyber-attacks that are ransom-based versus those that seek to destabilize a country, are they looking for the same things? Do they analyze the attacks in the same way? Do the cyber defence teams require the same skills in both cases?

Dr. Benoît Dupont: Yes, the same skills are required to carry out the same type of analysis in determining the appropriate response. The only exception is that, in cases involving ransom, negotiating skills can come into play, but more in the private sector.

Ms. Christine Normandin: Thank you.

I think I'm out of time.

[*English*]

The Chair: Thank you.

Ms. Mathyssen, you have five minutes, please.

Ms. Lindsay Mathyssen: Thank you so much.

Professor Dupont, I was really taken with your description of some of the technologies that are moving forward. I was feeling as old as our chair—

Some hon. members: Oh, oh!

Ms. Lindsay Mathyssen:—in terms of the neural interfaces. I would like to hear a lot more about that.

Can you expand on those technologies that you were describing?

Dr. Benoît Dupont: When I was talking about a neural interface, it's a new brand of technology trying to connect human brains to machines in order to communicate faster between those two components. For example, Elon Musk is investing a lot of money in a company called Neuralink, which is trying to implant electrodes into human brains in order to communicate much faster, and in a more effective way, with computers. The initial aim is to blend artificial intelligence with human intelligence.

This is not science fiction. This is what's happening right now in research and development.

Ms. Lindsay Mathyssen: I believe I've heard about that. It's the ability to bypass some of the misconnections sometimes. For instance, if someone has been in an accident and their spinal cord isn't working in the way it should, it is then bypassed through those neural links. Is that what you're talking about specifically? Is that one of the examples of what you are basically talking about?

Dr. Benoît Dupont: That is one of the examples. It is one of the early use cases, but the applications will be much broader than that.

Ms. Lindsay Mathyssen: Can you expand on that in terms of defence and weaponization? Are you talking about that in terms of the defence industry?

Dr. Benoît Dupont: Yes. We could be thinking about implanting neural interfaces in the brains of soldiers to make them much more effective combatants.

Ms. Lindsay Mathyssen: How far away are we from that in your estimation?

Dr. Benoît Dupont: It's hard to know, because it's all very sensitive and confidential. This is being developed at the moment. There are papers and documentaries. Investors are investing millions of dollars in these technologies. This is coming for sure.

Ms. Lindsay Mathyssen: Considering Tesla's inability to make self-driving technology as quickly as it had wanted, I imagine there are quite a number of bumps along the road, no pun intended.

Do governments around the world, internationally and in Canada, have legislation in place? Are they close to providing protections from this new kind of technology that you're talking about—not just the neural link but the other technologies you were talking about?

● (1705)

Dr. Benoît Dupont: I'm not aware of legislation being brought forward. I'm sure those technologies would be regulated by public health and pharmaceutical regulatory frameworks.

Ms. Lindsay Mathyssen: You referred to referred to Dr. Leuprecht's discussions—and here Madame Normandin always takes my questions—about recruitment, retention, and the competition that the Canadian Armed Forces and our security forces face from corporate institutions for the unfilled cyber positions within our institutions. A lot of that recruitment and retention is actually discussed in the documentation from DND entitled “Strong, Secure, Engaged”, but it was also written several years ago.

Is that still in line with what we need? Does that need to be updated? Where are we at in terms the direction the government is headed in terms of recruitment retention?

Dr. Benoît Dupont: I think the needs are still very acute. The types of profiles we need are pretty much the same. We need technically trained people. They are in very high demand, not only from the private sector in cybersecurity but from other sectors in AI development and video games. All the IT industries are hungry for all those people, and they're competing ferociously to attract those talented people.

The Chair: Thank you, Ms. Mathyssen, for that wonderful set of questions on neural links. We can hardly wait for Ms. Gallant's five minutes of questions.

Ms. Gallant, you have five minutes.

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

Mr. Hewie, you mentioned that SolarWinds attacks in the context of Canada's national defence.

Mr. John Hewie: I mentioned SolarWinds just in the context of the emerging trend we're seeing across nation-state adversaries, but especially Russia, in compromising the supply chain. What I mean by “compromising the supply chain” is that, instead of individually going after a specific entity individually, those actors will go after and try to compromise the software or technology systems that those companies use.

In the case of SolarWinds, Russia was attributed to the compromising of the SolarWinds company itself, whose software is used by many companies around the world, including governments, and the data that we have indicates that the single compromise of SolarWinds ended up impacting over 18,000 organizations worldwide.

Mrs. Cheryl Gallant: Is the scope of the SolarWinds attack still under investigation?

Mr. John Hewie: I don't have any detail to provide this committee on the current status of that investigation.

Mrs. Cheryl Gallant: No Canadian national defence software was impacted by it. Is that what you're saying?

Mr. John Hewie: I'm not aware either way.

Mrs. Cheryl Gallant: You mentioned FoxBlade earlier. Do you know whether or not it's being used against NATO members?

Mr. John Hewie: I don't have insight into that or have information on that either, but I can say that this is not the first time that this destructive malware has been used by a nation-state actor.

Mrs. Cheryl Gallant: Would FoxBlade have the potential to result in mass death?

Mr. John Hewie: I suppose, if it were targeted at critical infrastructure in a way that had some type of catastrophic chain of failure, then it could certainly impact human lives in a negative way.

Mrs. Cheryl Gallant: There's the term “threat emulation technology” as it applied to Cobalt Strike. What is meant by that, and how would it be applied or used against our national defence?

● (1710)

Mr. John Hewie: I'm sorry, I'm not aware of the term “threat emanation technology”.

Mrs. Cheryl Gallant: It's threat emulation technology.

Mr. John Hewie: Threat emulation technology.... No, I'm sorry, I'm not aware of that term either.

Mrs. Cheryl Gallant: Okay.

CSE judges that cyber-threat actors will very unlikely seek to intentionally seek to disrupt Canadian critical infrastructure and cause major damage or loss of life.

That being said, how vulnerable are we with the Internet of things, given that something as simple as your refrigerator is sending off pings? There seem to be so many vulnerabilities and it is the least protected throughway that is going to be attacked, so how can they be so confident, do you think, that it will be unlikely to be disrupted?

Mr. John Hewie: I think it's really difficult to predict a future in this space, and it's why we've seen a theme of needing to work together on sharing intelligence and looking at different ways to combat these threats, not just from the defensive perspective, but advocating for things such as what Microsoft is doing around our digital peace objectives and advocating for cyber-norms of acceptable behaviour in cyberspace so there are consequences to these actors.

Specific to your question about IoT, absolutely, that is a concern to Microsoft and many others across the industry, in that these devices are being plugged into the Internet at a prolific rate, and there isn't necessarily the structure or the organization among the vendors or even regulation around this to ensure that these devices are built and secured by design and securely operated, or even have the ability to be updated at a later point in time by the vendor. Those things are easy targets for actors to compromise and then use against either governments, critical infrastructure, Microsoft or any organization in a future cyber-attack.

Mrs. Cheryl Gallant: I didn't have a chance to ask this in the first round, but there was GiveSendGo, a U.S.-based platform that was hacked. Do you have any knowledge of who the expected or suspected perpetrator is of that?

Mr. John Hewie: I'm sorry. We do not have any information on that particular situation.

The Chair: Thank you, Ms. Gallant.

Mr. Kelloway, welcome to the committee.

Mr. Mike Kelloway (Cape Breton—Canso, Lib.): Thank you for having me, Mr. Chair.

Hello to my colleagues, to the staff who are here and to the witnesses.

Let me say, Mr. Chair, that I think you're getting better, not older.

The Chair: You have 10 minutes now.

Mr. Mike Kelloway: I have 10 minutes now?

Voices: Oh, oh!

Mr. Mike Kelloway: That's great.

I want to thank you for your opening remarks and your responses to a lot of the great questions that have been thrown your way.

I want to pick up on one particular item. I think, Mr. Hewie, you brought up the importance, when you're looking cybersecurity, of looking at it from an integrated approach. This includes the government, private sector and academia.

There are a couple of questions—and these are also for Mr. Dupont. Can you provide an example of where that integrated framework is working well?

The second piece concerns this. I'll paint a picture. You have an opportunity to speak to that collaboration of private sector, governments and academia. What are the first three things that you would recommend to that group to look at concretely and do a deep dive on?

We could start with Mr. Hewie and then go to Mr. Dupont.

Thank you.

Mr. John Hewie: I'd like to share a very timely and close-to-home example, and that's the work that Microsoft has done. I mentioned our long-standing collaboration with the Communications Security Establishment and the Canadian Centre for Cyber Security. Part of the threat intelligence that the Canadian Centre for Cyber Security develops and curates, as part of what they see through their various sensors and lens that is shared with critical infrastructure here in Canada, is also shared with Microsoft. That's been done over the past two years in an automated way.

Those indicators and signals that are contributed by the Canadian Centre for Cyber Security end up helping to improve the protections within all Microsoft products and services globally across the cloud. They help provide that additional level of protection to customers worldwide and in Canada, including the Canadian government and consumer organizations around the world.

That's very much a great example of that industry partnership and having real impact by sharing key information.

● (1715)

Mr. Mike Kelloway: Go ahead, Mr. Dupont.

Dr. Benoît Dupont: Another great example is the CCTX—the Canadian Cyber Threat Exchange—which brings together 150 Canadian companies. It provides them with threat intelligence from the Canadian Centre for Cyber Security, but the private sector also blends all of these [*Technical difficulty—Editor*] intelligence and shares that with Canadian companies, big and small.

One of the major issues is that we've talked a lot about critical infrastructure, but Canada is a country of small and medium-sized business and those businesses are being hit by ransomware and they cannot often afford the same kind of cybersecurity technology. We also need to be thinking about how can [*Technical difficulty—Editor*] we need to be thinking about more.

Mr. Mike Kelloway: We lost the last few moments.

The Chair: Could you repeat the last few sentences, please?

Mr. Mike Kelloway: Yes. Thank you, Mr. Dupont.

Dr. Benoît Dupont: Do you want me to repeat the last few sentences?

The Chair: Yes. We had a Russian hack here.

Dr. Benoît Dupont: It might have been Chinese.

I was just saying that the Canadian government needs to keep thinking a lot more about how to help SMBs—small and medium-sized businesses—because they employ 95% of the Canadian workforce and provide a lot of services and some of the critical functions to bigger companies. They are also involved in supply-chain attacks, and they have very limited resources to deal with cybersecurity issues.

Mr. Mike Kelloway: How much time do I have, Mr. Chair?

The Chair: You have 30 seconds.

Mr. Mike Kelloway: Very quickly, the second part of my question is for both of you.

If you had an opportunity to speak to that collaborative team—the best and the brightest, as it were—and you had one or two recommendations, what would they be? Let's go with one for the sake of time.

Mr. John Hewie: Number one is that cybersecurity basics matter more than ever now. When I say the “basics”, I mean keeping systems up to date, using modern technology and enabling things like multifactor authentication.

In our view of all of the attacks and customer compromises that we see, doing the basics and enabling MFA would prevent the vast majority of those. Unfortunately, as much as we work with things like Get Cyber Safe to build that education, there's still a lot of improvement we can make around the basics.

The Chair: Professor Dupont, you're going to have to work that answer into Madame Normandin's two and a half minutes.

Madame Normandin, you have two and a half minutes.

[*Translation*]

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

My question is for both witnesses. With the crisis in Ukraine, we are hearing a lot about the role of hacktivists, so hackers who have answered President Zelenskyy's call for help by hacking into Russian networks.

Mr. Hewie, how welcome are these hackers?

Professor Dupont, do they pose a long-term risk, especially if they are given free rein and encouragement?

Is there a risk of them going rogue because they couldn't be controlled, especially if they were encouraged to do what they were doing?

I'd like to hear how both witness see the role of these hacktivists and whether we should be worried at all.

Dr. Benoît Dupont: I'll go first. Their role makes the work of government agencies even more complex. It becomes very hard to know who is doing what in this new environment where anyone can call themselves a hacker to answer the call for help, with very good intentions, I don't deny that.

The risk is that some of the hackers may not necessarily know all the ins and outs of the systems they are attacking. As a result, they may launch attacks against critical infrastructure in Russia to the detriment of Russian civilians, who don't necessarily have anything to do with the attack on Ukraine. Those cyber-attacks have the potential to spill over into other countries, beyond Russia's borders, and be hard to control.

I think the situation needs to be approached with a great deal of care. It's important to not get excited and to think about all the uncontrolled and unforeseen implications of cyber-attacks mounted by isolated groups.

● (1720)

Ms. Christine Normandin: Thank you.

Would you like to answer as well, Mr. Hewie?

[*English*]

The Chair: You have about 30 seconds.

Mr. John Hewie: I would reinforce Microsoft's position that we certainly do not support cyber-offensive activities, primarily for a number of reasons.

We have seen that cyber-weapons are typically very difficult to target, and the potential for collateral damage to spill beyond the intended targets, much like the NotPetya attack in Ukraine a few years ago, which ended up impacting organizations around the world and costing hundreds of millions of dollars to recover from. That is example of where there's a potential for that collateral damage that could be extreme.

The Chair: Thank you.

Ms. Mathyssen, in spite of my better judgment, you have two and a half minutes.

Ms. Lindsay Mathyssen: Thank you, Mr. Chair.

One major issue we've seen with that cybersecurity threat is the issue of espionage and the stealing of Canadian intellectual property. What recommendations do you have for the committee to tackle this form of digital theft?

I would add that a lot of our data is differently managed from province to province. What challenge does that provide for the protections that are provided through cybersecurity and corporations like Microsoft?

That's for both witnesses.

Mr. John Hewie: I could maybe start with that one and Mr. Dupont could follow.

Certainly in our digital defence report we outlined some of the activity we have seen and detected, which includes espionage by some of the nation-state adversaries that I mentioned previously. These actors, quite frankly, whether they are cybercriminals or nation-state actors, are looking for gaps in our protection, gaps in our processes, and are looking to exploit those.

The general guidance that Microsoft would have, whether protecting against espionage or other types of ransomware attacks, quite frankly, would be similar. We would certainly encourage organizations with sensitive IP, or what we might call the “high-value assets”, to invest additional protections in those high-value assets, versus trying to just protect everything in the organization equally.

Dr. Benoît Dupont: The Canadian government has launched a new research security program to try to help, or to force or compel, universities to better protect their intellectual property and raise their awareness. I think that's an excellent initiative to try to counter the leakage of Canadian IP.

The government needs to think about helping universities to fund these new efforts they are required to undertake. That would maybe be a piece of advice.

The Chair: Thank you, Ms. Mathyssen.

We have Mr. Motz for five minutes, please.

Mr. Glen Motz: Thank you very much, Chair.

Thank you to our witnesses for being here.

For the sake of our chair, and to take you back to the very beginning, we all think we know what the definitions mean, but can both of you very quickly define what “cybersecurity” means and what the differences are between “vulnerability”, “threat” and “risk”?

Mr. John Hewie: Maybe I can take a crack at that.

Mr. Glen Motz: Yes, please, a quick crack at that.

Mr. John Hewie: “Cybersecurity” is really about protecting your computer infrastructure or your identity in the digital context, on the Internet or connected to a network. It's those security protections extended to the cyber domain.

A “vulnerability” is a problem within a piece of software code that could be exploited for unintended purposes by a particular adversary.

“Threats” can be considered across a spectrum of criminal organizations or nation-state adversaries.

We've also done work at Microsoft with the Citizen Lab at the Munk School at the University of Toronto to try to shine a light on what we call “private sector offensive actors” who are building spyware for sale to governments and other organizations.

Really, risk and risk management are what all organizations at the core are looking to focus their business efforts on. There's always a trade-off between risks and benefits, and there's only a limited amount of money and people—

● (1725)

Mr. Glen Motz: I'm going to cut you off there, Mr. Microsoft.

Mr. Dupont, do you have anything to add to that or do you have something substantially different from that?

Dr. Benoît Dupont: Well, just on top of that, I would say that cybersecurity is not only about protecting systems but also about protecting the information that resides on those systems and helping the people using those systems adopt the behaviours that will actually strengthen the whole architecture of the people, machines and information working together.

Mr. Glen Motz: All right. Good. Thank you very much for that.

I have one last question for both of you. A number of Canadian organizations have responsible disclosure policies that offer financial incentives to what we call “ethical hackers” to refrain from publicly disclosing software security and vulnerabilities they discover in that organization's products or services until a patch is available.

However, a frequent complaint of those who disclose security vulnerabilities under a responsible disclosure scheme is that the organization they disclose to fails to respect the rules of that game. Sometimes, an organization that has been alerted to a security vulnerability in their product or services plays down the significance of that vulnerability, so as to pay a smaller bounty, fails to give due credit to the ethical hackers or demands an unreasonable delay in public disclosure because they're unwilling to put resources into patching the vulnerability.

We all know that puts Canadians at risk. What do you think government should be doing to encourage organizations to implement responsible disclosure policies to prevent this sort of activity from occurring?

Dr. Benoît Dupont: Maybe the government could be offering tax deductions to cover those bounties. Maybe that would help those organizations take these bounties more seriously. Or, as well, it could regulate this area of activity.

Mr. Glen Motz: Go ahead, Mr. Hewie.

Mr. John Hewie: I would say that Microsoft has quite extensive experience in this particular topic. We'd certainly be happy to consult and to inform some views on that particular topic following this committee meeting.

We certainly encourage confidential vulnerability disclosure. We work with a community and have fostered a community with security researchers around the world. We have extensive bug bounty programs to try to direct that research into areas of our products and services that we feel are the most sensitive or where we'd like to see more inspection. Quite frankly, we've found that works generally very well.

There are certainly situations where.... Technically, these patches are updates to address these vulnerabilities, and they take time. We don't want to roll out a patch before it's ready and end up disrupting or negatively impacting existing infrastructure out there.

The Chair: Thank you, Mr. Motz.

The final five minutes will go to Mr. May and Mr. Fisher.

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

Mr. Hewie, I'm somebody who's really new to this, so I'm hoping you can really dumb this down and walk me through it. You talked about how much work from Microsoft's perspective goes into detecting these breaches and obviously stopping them.

Could you elaborate a little bit on the breach itself? Is it typically Microsoft that discovers this as opposed to the organization or a government?

Mr. John Hewie: Yes, absolutely. I would say that the techniques being used most predominantly are twofold. One, attackers are using vulnerabilities or exploiting vulnerabilities in software that for the most part have been patched by the vendor, but the customer or organization or agency just hasn't yet had a chance to deploy that patch.

Mr. Bryan May: But you see that first, right? Is it you guys who are detecting these breaches maybe before a government, or even before the company in question?

● (1730)

Mr. John Hewie: In the shared responsibility model in which we operate for cloud services, there's a security responsibility for both the cloud provider and for the actual end-user or the customer. In a case where we see attacks against identities, meaning that people are trying to access someone's username—their login and password, so to speak—certainly we've seen Russian actors use password spray and other types of techniques, including phishing, to gain access to those accounts.

We work with those customers to be able to notify them of suspicious activity when we see attempts to compromise those particular accounts or if we do have intelligence to detect that they have been compromised.

Mr. Bryan May: What does that decision tree look like? I'm wondering at what point you reach out to the government and say, "We've detected this. It's something we should be sharing with the wider community."

Mr. John Hewie: In the vast majority of cases, because these systems are massive and at scale, the tooling has been empowered so that there are alerts generated. It's the responsibility of the end-user, the end customer, to monitor those alerts and that suspicious activity themselves.

Mr. Bryan May: Thank you.

I'll give the rest of my time to Mr. Fisher, please.

Mr. Darren Fisher: Thank you very much, Mr. May, for sharing your time with me.

I have to say that both witnesses are amazing. The information we're getting here is absolutely astonishing. I thank you both for being here.

I'm short on time, so I guess this will be sort of a short snapper here. Presuming that the good guys and the bad guys are seeking the cyber-skilled young people of today and tomorrow, who has the edge on that skill set? Is it a bidding war to get the smartest and brightest people out there to be on the side of good versus the side of evil?

I just randomly looked at you, Cheryl....

Mrs. Cheryl Gallant: Evil.

Voices: Oh, oh!

Dr. Benoît Dupont: I think the side of good pays better than the side of evil, so I would say there is an edge for white-hat hackers.

Mr. John Hewie: I would like to agree with Mr. Dupont in that regard.

I think the area where there is an ethical line is in the security research community. The security researchers who are looking for vulnerabilities can do basically one of two things. They can provide that back to the vendor, which is part of the confidential responsible vulnerability disclosure program, and have it fixed, or they can sell that vulnerability to the cybercrime industry or others.

We try to provide "bug bounty" programs and other incentive structures to encourage and align those security researchers with the good guys.

Mr. Darren Fisher: Thank you.

That sort of leads me to my last question, which I have about 45 seconds for.

Mr. Hewie, you talked about the cost of data breaches. How do groups, these state actors or these criminal networks, profit other than by selling the data?

Mr. John Hewie: Unfortunately, they are very creative in finding ways to monetize data that's been stolen from organizations.

In the case of ransomware—I'm sure it's a term most people are familiar with—there's the traditional encryption of your files and holding them for ransom with the intent that you'll be given a key to decrypt those files. Then there's the second stage where they steal that data and leak it to the public.

In the last several years, I think we've seen a professionalization of that crime industry where it's not just one actor or two actors doing things; it's a whole economy of actors.

Another example is compromised accounts, where a username and password for a particular Canadian organization is compromised. It gets put into a market on the dark web and sold to the highest bidder as a way to gain access to this particular organization. They may have more experience dealing with critical infrastructure or the mining industry and know how to further monetize attacks against those organizations.

The Chair: Thank you, Mr. Fisher.

That will bring our questioning to an end. I want to thank Professor Dupont and Mr. Hewie for this very enlightening and somewhat scary peek into the new world. I'll be sure not to talk to my wife in front of our refrigerator any longer.

Voices: Oh, oh!

The Chair: With that, colleagues, assuming I live long enough, we will have another meeting next Wednesday. We will conclude our final hour. In the second hour, our esteemed analysts will outline to us at least some chapters in a report. If we could think about what we want to see in a report, that would be very helpful.

We will adjourn the meeting.