HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

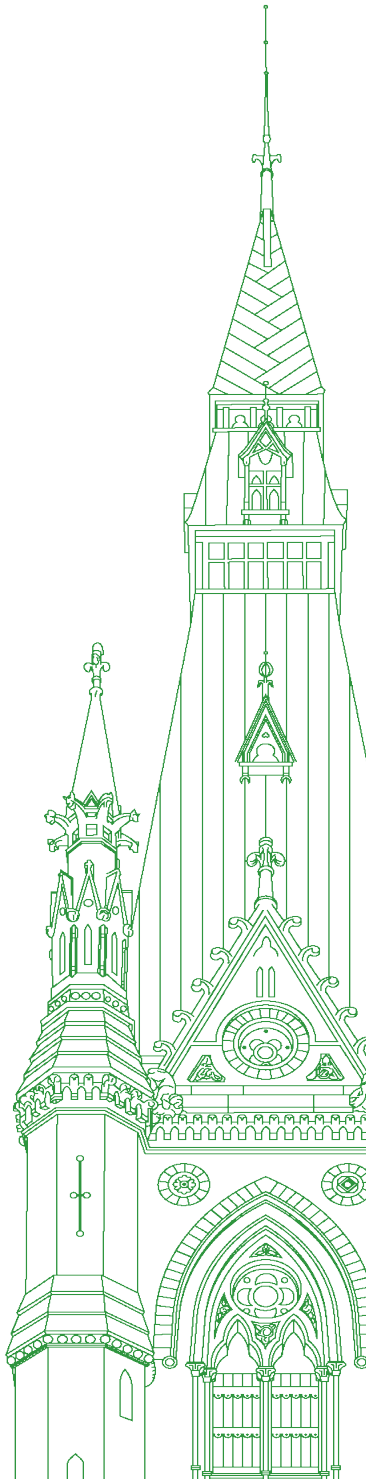
Standing Committee on National Defence

EVIDENCE

NUMBER 055

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Friday, March 31, 2023



Chair: The Honourable John McKay

Standing Committee on National Defence

Friday, March 31, 2023

● (0845)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): I call the meeting to order. I see a quorum and it's 8:45. We'll commence with our first three witnesses on our ongoing cyber study.

Present in the room are BlackBerry representative John de Boer and, from the International Civil Liberties Monitoring Group, Tim McSorley. Online we have Mr. Nared, chairman of the board, Slovenian Certified Ethical Hackers.

Welcome, everyone.

I will call on Mr. Nared first, for five minutes, and then we'll move to the other two witnesses. As I indicated to the witnesses who are here, we are expecting guests around 10:15. I don't know whether we'll have an hour or more than an hour. We'll get started and see how this plays through.

With that, Mr. Nared, you have five minutes. Go ahead, please.

Mr. Tadej Nared (Chairman of the Board, Slovenian Certified Ethical Hackers Foundation, As an Individual): Thank you, Mr. Chair and members of the committee.

Good morning. Let me add that I am honoured to be able to speak before you.

I serve my second term as chair of the board of Slovenian Ethical Hackers Foundation occasionally. I also collaborate with various parliamentarians and committees of NATO countries on diverse topics, from the safety of electronic elections to critical infrastructure and so forth. I also serve as virtual chief information security officer for a Swiss fintech company and as chief information officer to a U.S.-based, women-owned, Ukrainian-owned defence and cyber-defence company, where I try my utmost to empower these remarkable ladies who are heavily engaged in defending their country via cyber means and otherwise. Pertaining to that, if Mr. Chair would permit, I would take a few minute for introductory remarks.

Let me start by saying that usually I'm very diligent before each such engagement as today's hearing, preparing meticulously the topics I would like to present, but ever since I got acquainted with the truly brave and relentless women who are, in the most part, responsible for setting up one of the most formidable cyber armies in the world without outside help or funding and while under rocket attacks, I have kind of changed my perspective on what's important, and I fully embrace the new reality.

I believe it's one thing to discuss cyberwarfare from the comfort of your home or office while playing virtual cyber-games such as NATO's Locked Shields, and quite another when, as we had an example of, one of our core team members couldn't get online because a rocket landed in his apartment, cutting Internet cables, but luckily not exploding.

It's one thing to have a good night's rest and quite another to sleep two to three hours a day, being awakened by air raid sirens and still continuing highly demanding intellectual work and repeating that day after day for over a year because time is of the essence and your countrymen are dying.

I believe it is of the utmost importance to point that out, because I'm quite familiar with various cyberwarfare scenarios, but none of them take into account the aforementioned reality of working under such stressful conditions, where the only time you get to rest is when there is no electricity or Internet connectivity.

Having said that, we were recently present at a closed conference in D.C. on the topic of emerging technologies. The audience was mostly composed of military and intelligence agencies from Five Eyes. They asked us how we are able to accomplish all that we have showcased, and my answer was quite simple: These ladies don't sleep. That's how you accomplish what they have done, and, truth be told, it's them empowering me and not vice versa.

Also let me say that I regret that this hearing cannot be conducted in camera, as I believe is the term, because I wanted to share some of the accomplishments of the conducted cyber-efforts that surprised both the military and intelligence agencies that were present. I also have critical information pertaining to the security of all NATO countries that was acquired by cyber means, and I am quite certain that western agencies don't have that information available, so I would appreciate it if we could afterwards establish some secure communication channel with your present committee, which my colleagues and I trust, not only because Canada was doing and helping Ukraine while others were just talking, but also because we know from other experiences that members of the committee are trustworthy.

Now, as far as real-world experience goes, I would like to suggest to you starting points for discussions that we see as an example of the most important Ukrainian cyberwarfare efforts. Crowdsourced intelligence is being utilized very efficiently, both in terms of ISR—intelligence, surveillance, reconnaissance—especially with the Delta system, which I'm sure the members of the committee are familiar with.

● (0850)

Next is crowdsourced operations. Ukraine has effectively engaged the so-called “IT Army” of over 100,000 IT specialists in conducting mostly information war campaigns. Additionally, it has a core team of 1,400 highly sophisticated hackers who are not connected to any military or intel branch, but are still coordinating operations with both. It has proven itself to be a remarkable asset.

Lastly, I would like to draw attention to the recent public exposure of the Vulkan files, which are already known to western intelligence agencies. This incident, in essence, reinforces the warnings I've been expressing for years, including during my previous engagement with the committee on the subject of threat analysis for the Canadian Armed Forces—

The Chair: Mr. Nared, unfortunately, I have to interrupt you, because the five minutes have passed. You bring a level of reality to this conversation that has maybe been missing up until now.

I thank you. Certainly, there will be an opportunity to respond directly to other members.

Mr. Tadej Nared: Thank you very much.

The Chair: Thank you.

With that, I'm going to call on Mr. de Boer, and then Mr. McSorley.

You have five minutes, sir.

Dr. John de Boer (Senior Director, Government Affairs and Public Policy, Canada, BlackBerry): Thank you, Mr. Chair.

On behalf of BlackBerry, I'm delighted to speak with committee members today.

For over 35 years, BlackBerry has invented and built trusted security solutions to help keep people, governments and communities safe and secure. Today, we are a global leader in cybersecurity software and services. We protect more than 500 million systems worldwide. Our customers include all G7 governments, NATO, 45 of the Fortune 100 companies and nine of the top 10 banks, just to name a few.

Given that every aspect of our lives is intertwined with the cyberspace, we must act proactively to decrease our cyber-risks in Canada. This can be done by adopting technologies and approaches that have proven to prevent cyber-attacks.

Required, however, is a fundamental shift in our approach from the current reactive model to a proactive stance, and from a focus on incident response to a prevention-first approach to cybersecurity. At an operational level, that means, first, ensuring that we are equipped with the most advanced AI-driven cybersecurity solutions that can prevent malware before it executes. Second, that means clarity in roles when it comes to cyber-preparedness and response. Third, it means enhancing public-private collaboration to boost our collective cyber-defence.

When it comes to technology, the majority of today's cybersecurity solutions operate on the model of knowns. These are known malware, known attack techniques and known attackers. These knowns are based on a collection of malware samples and indicators of compromise. Once these knowns are gathered, they are triaged, examined and published into cloud repositories, and only after that are systems updated, tested and tuned to defend against these known threats.

This reactive model forces us to deal with the after-effects of a cyber-attack. We need to shift our focus from this incident response to incident prevention.

At BlackBerry, we know this can be done, because in the last 90 days, we stopped more than 1.5 million malware-based cyber-attacks, including more than 200,000 new malware samples, before they had a chance to execute. We did this by leveraging advanced AI and machine learning to continuously uncover and prevent attacks, including ones that had never been seen before. Without prevention-first, advanced AI-driven cyber-solutions like these, Canada is constantly in reactive mode.

Proactive defence also requires clear role definition and a unity of effort. Today, cyber-responsibilities in the federal government are distributed across at least 12 departments and agencies. Multiple ministers have cyber-responsibilities, yet it is unclear who leads and who is responsible for ensuring coherence and a unity of effort.

When cybersecurity doesn't have a dedicated person pushing and fighting for the issue, it sits in the middle of everyone's priority list.

Australia and the U.S. tackled this issue head-on by appointing a cyber minister. In the case of the U.S., it was a presidentially nominated and congressionally confirmed national cyber director. Canada should consider establishing a cabinet or other senior position responsible for ensuring government-wide coherence and action on cybersecurity.

Finally, improving public-private collaboration on cybersecurity should be a priority. Companies like BlackBerry have unique insights and expertise to defend against adversaries, while federal agencies have the means and authorities to act. We should foster proactive collaboration between government and the private sector at the operational level. This would help close gaps in our situation awareness, foster incident response playbooks that are aligned and help create a culture of proactive collaboration at scale.

BlackBerry stands ready to work with the committee to strengthen Canada's cyber-resilience. I thank you for this opportunity today.

● (0855)

The Chair: Thank you, Mr. de Boer.

Mr. McSorley, you have five minutes, please.

Mr. Tim McSorley (National Coordinator, International Civil Liberties Monitoring Group): Thank you very much, Chair, for the opportunity to speak to the committee today.

The International Civil Liberties Monitoring Group is a Canadian coalition that serves as a watchdog around national security, anti-terrorism and civil liberties in Canada. We have long-standing experience examining Canadian work regarding surveillance and cyber-activities, including the work of the Communications Security Establishment.

We agree that it is vital that Canada take steps to modernize cybersecurity laws to protect the private information of Canadians and the information infrastructure on which we rely. It is also clear that as cyber-attacks increase in activity and sophistication, Canada must take steps to defend itself; however, these actions must not come at the cost of accountability and transparency of government activities, including those of the CSE.

In our work, we have seen how overly broad powers and extensive secrecy result in the violation of the rights of Canadians and people in Canada. This can have real-world impacts, including when the information of Canadians and people in Canada is shared internationally with the Five Eyes as well as with other foreign agencies. When this information is in the hands of foreign jurisdictions, Canada loses control over how the information may be used, including in ways that can result in rights violations, abuse and even torture.

We also disagree with the premise that the private information of non-Canadians outside of Canada is simply fair game for mass collection and retention. This approach reinforces ongoing global systems of mass surveillance and associated rights violations.

This was revealed in detail by Edward Snowden, and while it did lead to promises of reform within Canada, it is unclear to what degree the CSE's activities have truly changed. While many of these concerns are related to the CSE's signals intelligence work, they also apply to CSE's cybersecurity and cyberwarfare activities. For example, while the CSE may have two distinct areas within its mandate, signals intelligence and cybersecurity and information assurance, they do not exist in a silo.

Recently, the BC Civil Liberties Association published material obtained from disclosure in their lawsuit against the federal government regarding the CSE's operations. These documents revealed, for example, that under an agreement with the former department of foreign affairs, information that CSE collected during its provision of cybersecurity support to the department, including the private communications of Canadians, could be shared with its Five Eyes counterparts. While this agreement dates to 2012, this concern persists under the CSE Act adopted in 2019.

Specifically, the National Security and Intelligence Review Agency, or NSIRA, noted in its 2021 annual report that the CSE Act explicitly allows for this kind of information sharing between the CSE's various mandates, including cybersecurity and foreign intelligence. NSIRA raised concerns that this sharing must be narrow and case by case and that the CSE should obtain legal advice on compliance with the Privacy Act. The CSE disagreed.

Why is this important? Bill C-26, currently being studied by Parliament, would formalize the CSE's role in ensuring the protection of cyber-infrastructure and would see the CSE obtain information about the security of critical infrastructure.

This means that a lot more information will flow to the CSE, including potentially private information relating to Canadians. Without adequate safeguards in place, both in the CSE Act and Bill C-26, information collected by the CSE, including information relating to Canadians, could be used in unexpected ways and shared with unaccountable foreign partners.

For more on this, I'd like to direct the committee to an open letter that we co-signed with several other civil society groups regarding a recent report from Citizen Lab entitled “Cyber Security Will Not Thrive in Darkness”. I can send those along to the committee afterwards.

The CSE also has a troubling history of obfuscating the nature of its work and violating its mandate. For example, the CSE tracked the Wi-Fi connections of Canadians at major airports, despite not being allowed to conduct surveillance within Canada. It collected massive amounts of Internet traffic through 200 Internet backbone sites worldwide. Despite prohibition, it regularly collects Canadians' information. It received it from foreign partners, and it violated Canadian law for five years by failing to minimize Canadian information shared with Five Eyes partners.

The CSE also resists fully complying with review and oversight. For example, the CSE refuses to grant NSIRA full access to records that the agency needs to carry out its review function. Instead, the CSE requires NSIRA to submit a request, and CSE staff provide what they say are relevant documents. This approach, NSIRA wrote in its latest annual report, "undercuts NSIRA's authority to decide whether information relates to its reviews and contributes to significant delays in the provision of information to NSIRA."

● (0900)

The intelligence commissioner has also raised concerns that CSE authorizations for both foreign intelligence and cybersecurity have not included information crucial to the approval process, particularly regarding the outcomes of previous authorized activities or explanations of specific activities based on facts.

Finally, NSIRA has also raised concerns that the CSE is not providing adequate information on the impact of active or defensive cyber-operations nor appropriately delineating between the two kinds of activities, despite each requiring a different approval process.

I do have some recommendations, very short ones, but I will save those for the question period.

Thank you very much.

The Chair: If, in fact, you don't get them in during the question period, you can certainly submit them through the clerk.

With that, we'll go to our six-minute rounds, and we'll start with Mr. Kelly.

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

I'm going to start with Mr. de Boer, but I might ask all three witnesses to comment on my question.

I want to talk about the threat that I would think of as corporate espionage or the vulnerabilities within the private sector to cybersecurity. There was an article recently that talked about how hackers can manipulate the temperature of a barn and wipe out livestock populations, or that the food supply chain in Canada was particularly vulnerable to cyber-attack. That goes well beyond damage to a private corporation; it goes right to food security and things like that.

I will start with you and have each witness comment on the vulnerabilities within the private sector that affect national security.

Dr. John de Boer: Thank you, Mr. Chair. It's an excellent organization.

The focus of cybersecurity up until now has been largely on what we call enterprise IT systems. One of the largest gaps that has emerged is in operational technology. These are typically systems that control, for instance, an electricity grid, gas-powered turbines, industrial control systems in pipelines, etc. A lot of these systems are now coming online. What we witnessed in the U.S., for instance, related to the Colonial Pipeline attack, or even in Florida's Oldsmar water system, is that these systems were not designed to be connected to the Internet, including farm equipment etc., and people are now trying to enable optimization through connection to the Internet.

We noted, for instance, in the manufacturing sector over the past year that the number of attacks has risen by 2,000%. The three sectors most targeted over the past year by cyber-criminals have been health care, financing and manufacturing, but manufacturing is rising the most quickly. Why? Our assessment is that because of the supply chain vulnerabilities that we're seeing and because of the intrinsic link between economic security and national security and the fact, as I mentioned earlier, that everything is intertwined, those are becoming increasing attack vectors.

● (0905)

Mr. Pat Kelly: If you don't mind, I'll ask the other witnesses to comment as well. Maybe I'll have time for other questions.

Go ahead.

The Chair: Mr. Nared, would you comment?

Mr. Tadej Nared: Cybercrime, which is the term we usually use to describe both industrial espionage and ordinary crime activities, is in fact the third-largest economy in the world. By 2025, the damage resulting from cybercrime is going to amount to $15 trillion. It grows by an amount of $1,500 billion a year. It is a huge problem. Efforts conducted in this matter are not on par with the damage that is occurring and growing.

Taking into account what the previous witness was talking about, attacks on critical infrastructure especially, which are forbidden by the Geneva Conventions because they attack civilian infrastructure, are growing daily. We have to take nation-state actors into account, especially Russia.

This was what I was trying to bring into force before the Vulkan files. Before, we were just speculating on their capabilities, but now we are certain, and we have confirmation that they are collecting data all over the world. They are compromising systems, power plants, hydroelectric power plants, electricity grids and civilian infrastructure from hospitals to everything else. They are collecting that, scanning systematically and collecting vulnerabilities in one huge, giant database and preparing, in a way, for a black swan scenario.

What I'm really concerned about is that western countries, NATO countries, are not protecting their infrastructure in the manner that they should be. It is a huge problem, and it should be addressed promptly.

Mr. Tim McSorley: Just very briefly, it's clear that there's a role for the federal government in supporting private companies in increasing their cybersecurity and protecting national security. We think that one thing that's key to this is that there's trust and transparency around that process so that private companies can trust what the government is going to be doing when they provide that support. The public needs that trust and understanding around what those services are. We think that needs to be a central component of legislation like Bill C-26.

Mr. Pat Kelly: Okay, thank you.

If I can just have a quick moment, I want to ask something quite specific resulting from Mr. Nared's testimony.

The Chair: So do I, but you're bang on six minutes. If I do, the trouble is that the whole thing just goes south on me if I let one run away. I'm sorry, Pat,

Mr. Pat Kelly: Well, maybe in somebody else's time, you can quantify that multi-trillion-dollar number.

The Chair: It is a shocking number. I picked up on it as well.

Mr. May, you have six minutes.

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

Mr. de Boer, you noted in a 2021 post for the Canadian Chamber of Commerce that:

> The OECD reports that Canada is one of the few countries where technology R & D investment, is "stagnant," investing only 1.5 percent of GDP and declining—while Canada's competitors are investing billions to improve their cybersecurity capabilities.

In your opinion, sir, what are some of the factors that contribute to that under-investment in R and D by the Canadian private sector?

● (0910)

Dr. John de Boer: That was in 2021, but the data remains the same today. We are laggers when it comes to R and D investment. While we welcome, for instance, the renewal and revision of the SR & ED announced very recently, enterprises benefit much more from developing R and D outside of Canada, particularly multinational corporations, because there are much more collaborative support systems in place, whether with university-based research or elsewhere.

BlackBerry has made a commitment to invest in Canada. We invest about 24% of our annual revenue in R and D, working very closely with Canadian universities, etc., but not all companies are incentivized to do so.

There really needs to be a concerted partnership between government and the private sector, not all across the board, but betting in particular niche areas where Canada has a comparative advantage. Our post here was that cybersecurity is one of the areas where Canada has a comparative advantage. We rank fourth in the world in the number of cybersecurity companies, but we're not keeping up the pace with Israel, the U.K. or the U.S., which is far ahead of us.

Mr. Bryan May: Can you elaborate a little bit more and provide some recommendations on how we can take steps to ensure that IP grown in Canada, often with the help of direct or indirect public funding, stays in Canada?

Dr. John de Boer: I think one of the key things here is commercialization.

There's a lot of what we call lower TRL—technology readiness level—or very initial-stage R & D that takes place in Canada, but then, after it passes this initial stage, it goes through something called the valley of death, which means that it's very difficult to productize this R & D here in Canada.

There are very few programs, for instance, that support Canadian companies to help launch initial products to test them and get them to market, while in the United States, for example—of course, U.S. government procurement budgets are much larger—their procurement process is much more agile. They have systems in place to help companies get through that valley of death to help commercialize their products.

One of the suggestions that we put forward with the Canadian Chamber of Commerce was to establish a Canadian commercialization fund that would help Canadian companies move towards that productization.

The Canada innovation corporation, which was announced in the 2022 budget, may be a start, but we have yet to have very much detail about that. We're hopeful that the whole commercialization question there, which will help commercialized products here in Canada keep IP in Canada, would be a key aspect to that question.

Mr. Bryan May: We've heard a number of times that there are concerns that electronic components manufactured by state-affiliated corporations in countries like China pose a cybersecurity risk in Canada. Should we be concerned about the cybersecurity risk posed by offshore manufacturing of IT equipment?

Dr. John de Boer: BlackBerry, because it created devices, was very focused on ensuring that all of the components in those devices, including software, were what they said they were. We even developed software that helped us identify the provenance of each component.

This is a huge concern in the U.S. You have executive order 14028, which is about the nation's cybersecurity. It mandates what they call a software bill of materials that would basically produce an ingredients list of all software contained in every device. Right now, if you ask people what software is in their system or in their device, very few people know about it.

Part of the problem is also open-source software. This is free software available on the Internet that is used widely, but there are high security vulnerabilities there.

I think one thing that Canada should consider that many other countries in the EU and the U.S. are considering is making sure that there's a commitment to secure-by-design principles. You can't bolt on security afterwards.

● (0915)

Mr. Bryan May: Thank you.

In my last 10 seconds, sir, I'm wondering if it's the will of the committee that Mr. Nared talk about information that he can't share in this forum. I'm wondering if I could request that he work with the clerk to find a potential solution for that.

The Chair: I don't see why that's not a good idea, so we'll leave it as an instruction. Thank you for that.

With that, Madam Normandin, you have six minutes.

[*Translation*]

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

Mr. de Boer, my line of questioning will be similar to Mr. May's.

You said that one of your three priorities was being equipped to prevent incidents rather than focusing solely on incident response. Canada always seems to be in reactive mode.

Where do we need to prioritize equipment investments in order to be proactive? Do we focus on AI or post-quantum cryptography, for example?

Dr. John de Boer: Thank you for your question.

[*English*]

What we can do immediately is ensure that the Department of National Defence, our government and our critical infrastructure are equipped with what we call the latest technologies, AI-driven technologies. That is not the case right now.

Right now there are two large problems. One is that there are not enough cyber professionals in the world. There are more than three million vacant jobs globally, and in Canada there are probably around 200,000. The Department of National Defence and critical infrastructures agencies suffer with that as well.

You have to complement that with machines, with AI, because there are more than 400,000 new malware samples a day. This is proven technology. BlackBerry's, for instance, was developed in 2012. We're in our seventh generation.

That can be implemented. Ensure in the procurement specifications, etc., that we do not include specs that tie us to previous generations of technologies, signature-based technologies. That's number one.

Number two, we have to continually invest in R & D, as was mentioned previously, to ensure that we outpace our rivals. We're already seeing cybercriminals use ChatGPT and others for phishing attacks. We need to ensure that our AI is better than their AI when it comes to defending.

That's something that we can do immediately. Quantum cryptography technologies exist, but some of those issues we need to continually work on. That is an endeavour that's ongoing. I would suggest using the technology that we have now.

[*Translation*]

Thank you.

Ms. Christine Normandin: Thank you.

You also talked about the public and private sectors working together. I'd like to hear your comments on that and a potential three-way partnership with cyber hackers. Mr. Nared can jump in as well.

Is it possible to make progress that way? Are there risks to working with cyber hacker communities?

Mr. de Boer can go first, followed by Mr. Nared.

Dr. John de Boer: That's a great question.

[*English*]

The reality right now is that a lot of the public-private partnership or collaboration in Canada is, again, reactive. It's in the wake of an incident or an indicator of vulnerability, and it's largely one-way. We provide information to the government; it disappears into a black hole.

BlackBerry maintains good relationships with the Canadian Centre for Cyber Security, etc., but that could be much more robust.

What I would suggest, again, is moving to a prevention-first approach. Let's plan before an incident. Let's develop operational plans, contingency plans and mitigation plans in turn that clarify roles and responsibilities when a critical infrastructure system is hacked.

In terms of working with hackers, absolutely, we work with white hackers, ethical hackers, to test vulnerabilities in systems, whether that be in automobiles or in other connected devices. They're a key part of our community.

I'm not so sure about the situation in Canada, but in some contexts, their ability to work in cohort in collaboration with businesses and government is limited because the legal framework to enable that is not allowed. In the U.K., for instance, they're currently considering changing that legal framework so that there can be much more robust collaboration between the white hackers, the good hackers, and government, etc.

It's a fantastic question.

[*Translation*]

Thank you.

● (0920)

Ms. Christine Normandin: Thank you, Mr. de Boer.

Do you have anything to add, Mr. Nared?

[*English*]

Mr. Tadej Nared: I think that the collaboration with ethical hackers is crucial if we want to secure western nations.

I would use the Pentagon's pilot bug bounty program as an example. They opened up their systems on the bug bounty platform, where ethical hackers could test the systems and report their vulnerabilities. The result was that the systems got compromised. The first report came in, I believe, in the first seven minutes and, in the first six hours, there were 200 to 300 reports. That means 300 security vulnerabilities, 300 security holes that an adversary could exploit to gain access to their systems.

Because of this collaboration, the Pentagon was more secure. I believe that it was Mr. Ash Carter who complimented the initiative and in a way concluded that they didn't realize how many good ethical hackers and how many good IT professionals there are who would like to help but don't have the opportunity to do so.

As the experience in Ukraine has shown, using crowdsourced intelligence, using crowdsourced efforts, is the key in such environments, especially in the cyber environment, to achieve desired results. Without it, I don't think it's even possible.

The Chair: Thank you, Madame Normandin.

Ms. Mathyssen, you have six minutes, please.

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

Thank you to all the witnesses for appearing today.

Mr. McSorley, I want to ask you something. In this committee, at the beginning of the study, we heard from Canadian intelligence agencies, CSE specifically, and they said repeatedly that Canadian intelligence agencies don't target Canadians or collect data on Canadian activity, but the BC Civil Liberties Association had a lawsuit, and one of their concluding arguments was, "What was truly shocking is how hard CSE pushes up against the edge of legality, and pushes back against even the most reasonable regulation and oversight."

Could you comment on that in terms of how those intelligence agencies are constantly pushing against the legal boundaries that are Canadian law?

Mr. Tim McSorley: I think a lot is riding on that word "target" and what you were speaking about in terms of what the CSE presented to the committee.

It's true that the CSE, through its mandate and through the CSE Act, cannot target Canadians, but in collecting signals intelligence and in carrying out their work, including on cybersecurity and protecting cyber-infrastructure, as I mentioned, they collect all kinds of information, and then they sift through it. There's information that's known as unselected information, which is information that is not specifically targeted, but they may accumulate it in carrying out their collections, and then that information is retained, and some of that information may relate to Canadians. That's where they came into problems, as I mentioned earlier, in terms of sharing Canadian information with the Five Eyes and with other countries.

It isn't that they are targeting Canadians—there's that word "targeting"—but rather that they are incidentally collecting that information and retain it, and it is still used in other ways, so that's what we see. When they're pushing up against the boundaries, that's what they do.

There's another category of information, metadata. Metadata isn't the communications themselves; it's all the information around the communication, like who sent the information, who received it, at what time, from where, what kind of software was used and what kind of equipment. There's a debate of long standing around whether or not metadata should be considered private information. It's been clear that metadata taken together can paint a very clear picture of what individuals do and can lead to being able to identify certain individuals, yet the CSE has consistently argued that that doesn't amount to private information. Again, it's not targeting Canadians but collecting that kind of information.

The final thing I'll mention is around publicly available information. Despite every other restriction around the CSE's collection of information, they are allowed to collect publicly available information. Again, they're not allowed to collect information that has privacy impacts on Canadians, but there's still debate around what's considered private information or what maintains a reasonable expectation of privacy. For example, regarding information that we post on social media, there's an argument that it's publicly available information, but at the same time, are we expecting that to be collected, retained and possibly shared by our national security agencies?

That was at the heart of the debate around Clearview AI. They argued that facial images of Canadians online were considered publicly available information and that they could collect it. The Privacy Commissioner ruled that it was mass surveillance and was illegal. When they brought that to the RCMP, the RCMP said that they had no obligation to ensure that if they were working with Clearview AI, they were following Canadian law.

We don't know about the CSE's work on facial recognition technology, but if we can see that with the RCMP and that approach, that definition and the lack of clarity around publicly available information, we have to be worried that the CSE would be interpreting it the same way.

● (0925)

Ms. Lindsay Mathyssen: Thank you for that.

Yes, it was mentioned within that same lawsuit, in the documents that the BC Civil Liberties Association came out with, the glossary of terms of unselected data and publicly available data and how they are used. Do laws like Bill C-59...? That lawsuit was before Bill C-59. It addressed more the old Bill C-51 problems. Specifically as we look at Bill C-26, do those laws adequately address the threats that civil libertarians are worried about in terms of taking advantage of publicly available data?

The Chair: Thank you.

That's a good question. You have about 30 seconds to answer it, though.

Mr. Tim McSorley: I'll just quickly say no. Several of the problems I raised were actually enshrined in Bill C-59, the creation of the CSE act. One of the things we think needs to be done is to bolster the powers of both NSIRA and the intelligence commissioner to be able to review these kinds of activities and be able to discuss their findings publicly.

The Chair: Thank you.

He actually was very efficient in the response, so you'll get another 15 seconds, Ms. Mathyssen.

We're on the five-minute round and Ms. Gallant.

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): Thank you, Mr. Chair.

My questions will be for Mr. Nared. I'm going to ask three quick questions and then he can budget his time in answering them.

We just finished a study on the Arctic in this committee. One of the recommendations is that instead of getting submarines, we should be using drones under the ice in our Arctic. We know that adversaries are currently traversing in submarines, and they have the data in real time.

Is there a vulnerability for an underwater ice drone in the Arctic in transmitting the data back to whomever, as opposed to just being there in real time and seeing for yourself? That's one question: threats for underwater ice drones.

Second, how is artificial intelligence impacting the cyber-threat environment?

Third, how can security agencies or national defence distinguish between a series of attacks, or simultaneous attacks, on communications technology or industrial control systems and tell if those are precursors of a kinetic attack?

Mr. Tadej Nared: Thank you, Ms. Gallant, for the questions. They're excellent ones.

Regarding the drones, it's actually about the pinnacle of the cybersecurity industry. That means it's about electronic warfare. I've recently had discussions with people who are really tightly involved with the field, and it's an ongoing game of cat and mouse. It is not a question that is easily answered, but there are technologies available in drones that are built more in the private sector that make them quite electronic warfare resistant. We had an opportunity to see some of them flying over Russian territory recently, and they continue to fly, so....

It is more of an electronic warfare question. The main point here is that all those electronic warfare units are able to pass the signal, but the most crucial problem is how to transform that signal to zeros and ones, to put it plainly. That's one of the biggest challenges that electronic warfare units of Five Eyes countries or NATO countries are currently experiencing, but they are working on that.

Regarding how AI is affecting the cyber-threat environment, I would say that it is a double-edged sword. It can be used for both defensive and offensive means, as our co-witness has previously stated. ChatGPT, as an example, has become one of the largest producers of malware. It was hacked in less than a few days. Like Head Hackers, they use it efficiently not just to produce phishing emails and content related to that, but you can effectively use it to produce very sophisticated malware. It's very easy to bypass the restrictions put in place by OpenAI and basically make it write whatever code someone would think of, including to attack SCADA systems or to duplicate the STUXNET worm or whatever. It all depends on the creativity of the person talking with it.

As to how to distinguish precursory attacks as something that would lead to kinetic attacks, I would say that every precursory attack is something that will lead to a kinetic attack, especially in terms of Russia and their capabilities. I would again like to point out that just yesterday information was released regarding the Vulkan files, which are very descriptive in terms of Russian cyber-capabilities. They actually proved that they have been systematically attacking western infrastructure for years—attacking our infrastructure and our industrial control systems, such as hospitals—and whatever information they can gather, they do gather within the database, and they simply wait for the right moment to strike. It is, as I've said, a black swan in the making, and we should start taking it very seriously.

● (0930)

The Chair: Thank you, Mr. Nared and Ms. Gallant.

Mr. Sousa, you have five minutes, please.

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

I'd like to thank the witnesses for their presentations. We have a concern—all of us do—with regard to security measures in this country, as well as privacy and our sovereignty as a nation.

My first question is for Mr. de Boer. When we look at the notion of IP and the commercialization of IP, and the ownership of the technologies, we see that Canada seems to do well at advancing.... In fact, Canada is a pretty good supplier of infrastructure and IT to other countries, and they themselves have noted we're lagging behind just by what they see happening in other jurisdictions. I believe the science and research committee is also looking at the commercialization of IP and how to get through that valley of death you mentioned.

The questions then become these: Who adjudicates some of these deals? How do we coordinate the private sector to facilitate that engagement with the academic sector? What role does this government have to play in this? You mentioned a couple of funds that were being proposed.

I'm still struggling, though, because the mindset we have, while it may seem reactive, is that it's also a means of necessity by which to come forward with new technology and new innovation and then protect it with ownership of the IP and the patent so that others can't use it. How do you make others accountable—and other countries accountable, for that matter—for escalating some of this? Is there a real sense of...? I mean, we have Five Eyes out there, but there are misbehaviours. How do you make them accountable?

● (0935)

Dr. John de Boer: It's a complex question, obviously, and a lot of it is outside my scope of expertise, but when it comes to protecting against, for instance, espionage or malicious behaviour that tries to either siphon off or sabotage IP and the entire R and D process, there are a couple of vulnerabilities, I think, that need to be filled immediately.

One, companies like BlackBerry, but not just BlackBerry, work very closely with the universities, research institutes and small and medium-sized businesses in Canada to create new products, new IP, across that supply chain. The security assurances required are not always in place. We need to ensure that security, guarding of the IP as we develop it, is as important as developing it itself. In essence, it should be considered a national asset. When it comes to universities, I do know that CSIS is starting to push forward programs to raise awareness about security within university research labs themselves to safeguard IP. We need to act similarly with SMEs that work on IP, so if there's one recommendation I can make....

The Insurance Bureau of Canada did a survey last year asking SMEs about whether they had invested in cybersecurity. Last year 47% of them had invested zero dollars in cybersecurity. We know that SMEs are critical to IP creation. We need to do something to incentivize these SMEs to protect their IP. They're not investing in it largely, apparently, because of the cost. It's a trade-off. I think as a government and as a society we need to shift the lens to start incentivizing security to be part of that.

The last thing I'll mention is that two years ago, ISED rolled out a fantastic program, in theory, called the Canadian digital adoption plan. The idea there was to increase the use of digital technologies by small and medium-sized businesses. Cybersecurity was not included in that initially. We worked with ISED later to include that in the assessment, but these kinds of programs need to embed cyber as a fundamental core of their operations.

The Chair: Thank you, Mr. Sousa. You have eight seconds left and you're not going to get them.

Voices: Oh, oh!

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

The Chair: Madame Normandin, you have two and a half minutes.

[*Translation*]

Ms. Christine Normandin: Thank you.

Now I'm going to turn to Mr. McSorley.

You mentioned a number of situations that pose privacy risks as far as CSE is concerned.

I know very little about all this, so could you tell me how you obtain information on what CSE is doing? One of the things you said CSE did was track people's Wi-Fi connections at airports.

Does CSE put out that information, or do you collect information on CSE's activities in another way?

Mr. Tim McSorley: Thank you very much for your question.

● (0940)

[*English*]

There are multiple ways in which we collect that kind of information.

For some of it, before the creation of the intelligence commissioner, there was the CSE commissioner, who initiated review, and it's the independent review and oversight bodies that often have access to this information and will share that information, although still redacted in a way that protects national security when there are concerns. Sometimes those are still difficult to interpret because of redactions and euphemisms and language. Often, it relies on access to information requests. Researchers will have academic researchers and our own research requesting documents and digging in and trying to find information.

In terms of the issue around Wi-Fi at the airports, that was based both on the commissioner and on the journalists who discovered the information and publicized it, and then, one of the things that I think might—

The Chair: Sir, excuse me.

Charles, can you turn off your microphone, please?

Okay, please continue.

Mr. Tim McSorley: One of the reasons I have the access to information that I have today is the BC Civil Liberties Association lawsuit that resulted in disclosure. They then had to fight to publicly share the information they obtained, and only recently were they able to publish it publicly.

I guess what ties all of that together is that the information isn't coming from the CSE itself. It's coming from external bodies—from researchers, review committees and lawsuits—and it shouldn't have to be that way.

[*Translation*]

Ms. Christine Normandin: I'd like to hear more about that. You mentioned the importance of transparency and accountability.

Do you have any recommendations on how to achieve greater transparency and accountability?

[*English*]

Mr. Tim McSorley: Yes, definitely.

One of the things we've seen in terms of both the intelligence commissioner and NSIRA is that they're not receiving the information they require in order to do their review work and, in the case of the intelligence commissioner, their oversight work. We think there need to be amendments made to the CSE Act that make authorizations for their various activities contingent on providing adequate and appropriate information to the intelligence commissioner, as well as examining the idea of providing the intelligence commissioner with a power to make binding amendments to the authorizations that the CSE is seeking—

The Chair: Unfortunately, we're going to have to leave it there. It seems like every time we get into your recommendations, I have to cut you off. I'm sure we'll get them out in the course of the hour.

Ms. Mathyssen, you have two minutes and 45 seconds.

Ms. Lindsay Mathyssen: With that extra 15 seconds, I'll just say thanks to Mr. McSorley for all of those recommendations. I hope that you do submit them to the clerk, please, so that we can have that as part of our record and part of our study.

Within this committee, a lot of witnesses have talked about intelligence silos and Canadian intelligence agencies needing to integrate more for better intelligence sharing, but when you get into, for example, CRA sharing with CSIS or sharing with CSE, there are concerns that we have seen discrimination play a role in investigations of Muslim charitable organizations, for example.

Mr. McSorley, could you speak to the dangers that are posed by that further integration and to what we can do to avoid taking it too far in terms of that discrimination and victimization of some organizations that are quite legitimate?

Mr. Tim McSorley: Thank you very much for that question.

First, it's clear, as you said, that there is need for collaboration among national security agencies. Some of that does require the sharing of information.

However, as you pointed out, what we have seen is that there are deep concerns about how some of that information is shared and the impact it can have.

For example, again the BC Civil Liberties Association found in their research that CSE was sharing intelligence with the CRA in order to bolster their efforts to counter terrorist financing. However, what we have found in our research is that the CRA, through its efforts to counter terrorist financing, has taken a prejudiced approach to Muslim charities in Canada. It has been operating from an idea that because there are terrorist threats from Muslim-linked organizations, the Muslim community must be placed under greater suspicion. That results in greater surveillance, greater information gathering and sharing and greater repercussions as compared to other communities in Canada.

How this ties back to the study at hand is that the intelligence that is shared isn't known publicly to the organization that it's being used against, so they don't have the opportunity to challenge it. We see that also reflected in, for example, Bill C-26, where there's, we believe, an undue amount of secrecy and the ability to use information and to hide information from critical infrastructure companies that are providing telecommunication services to Canadians if they were, for example, to attempt to appeal or challenge an order made by the minister.

● (0945)

The Chair: Unfortunately, we're going to have to leave it there, Mr. McSorley, again.

Madam Kramp-Neuman, go ahead for five minutes, please.

Mrs. Shelby Kramp-Neuman (Hastings—Lennox and Addington, CPC): Thank you and good morning.

I would like to pose my questions to Mr. Nared this morning.

A briefing document your organization provided to a previous House committee indicated that concerns raised by other observers were still valid. In fact, the organization specifically pointed to an article written by Alexander Rudolf, who appeared before this committee earlier this year. In that he said,

> Canada needs both a whole-of-government cyber-security response and a very targeted cyber-defence response.

In addition to that, in a document provided to the committee last year, it's quoted that the author wishes to reiterate that,

> CAF is not ready to meet even moderate cyber threats (such as hacktivists). And taking into account publicly available information and emerging threats, it won't be ready to meet modern cyber challenges for the foreseeable time.

Could you possibly expand on that? Do you still share this view?

Mr. Tadej Nared: Thank you for your question.

Yes, I still share that view, because I think it's been a year since that document. I believe I wrote that the basic problem is that the threat environment was specified solely to where the Canadian Armed Forces are stationed at home in Canada and abroad. That is a failure in understanding the cybersecurity environment in general. There is no defence perimeter anymore. Not just Canadian Armed Forces and their members but also their family members are targets for a moderate attacker, a black hat hacker or especially some sort of group such as the Russian group Sandworm. They will attack not specifically hard and secure targets but rather so-called low-hanging fruit first. That means even attacking family members, for example, compromising their home networks and expanding from that point onwards. We had a similar case in Slovenia, in which our emergency response was taken down in the very same manner. It was a failure in strategic thinking.

I'm not familiar with whether that agenda has changed in the past year. If it hasn't, it should be updated and improved.

I hope that answers your question.

Mrs. Shelby Kramp-Neuman: It does, certainly. That leads me into my next question.

You've also been quoted as saying that the genie is out of the bottle in terms of cyberwarfare and that the cyber World War III is already in full swing.

Many observers have pointed out that there's a significant cyber-skills gap in our civilian sector.

Could you expand and share with the committee what it means for the Canadian Armed Forces, which is currently facing a recruitment and retention crisis in its very nascent cyber-operations division?

Mr. Tadej Nared: Thank you for the question.

To give you an example, as the Ukrainian experience has shown, a war cannot be won without the support of the native population. I think that is a term that quite sticks. It is the same in the cybersecurity sphere. Especially the western countries, the Americas, kind of rely on their ocean for defence, and on overspending for defence also, but that is not a concept that you can rely on in terms of cyberwarfare. Relying on crowdsource intelligence, utilizing everyone who can help and organizing initiatives is the way to go, in my opinion. A closed loop won't solve any problems.

● (0950)

Mrs. Shelby Kramp-Neuman: Thank you.

Can I leave you with the rest of your time to...?

Go ahead.

Mr. Tadej Nared: If I may, I would like to take a minute to explain the cyber-damages I was talking about before, because it kind of relates to the subject.

For example, the F-35 program, which cost $1.7 trillion to develop in terms of R and D, got hacked by the Chinese, and all the plans were stolen. That's just one hack. If we combine everything together, we get a clearer picture of where the damages are coming from. That relates to the army, to the air force and to basically every part of modern society.

The Chair: Unfortunately, we're going to have to leave it there. That's a rather unfortunate point at which to leave it.

Ms. O'Connell, you have five minutes.

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

Thank you to all our witnesses for being here today.

Mr. de Boer, you've spoken about mandatory reporting and things like that, but I also want to dive into some of the challenges we've heard in other testimony about the private sector not necessarily wanting to share if they've been hacked or if their systems are vulnerable. I could certainly see that if BlackBerry, for example, which has a reputation for security, ever had a breach: The board or the governance of the company may not necessarily want to promote that a breach happened or that an attack was successful.

How does government partner in order to understand the real-world picture in the private sector, keeping in mind that the private sector might not be interested in sharing this information?

Dr. John de Boer: Thank you for that question.

Trust that the information that any company will give over to the government will be treated in a confidential way is really important there. Liability protections and all these things need to be taken into consideration. Currently, that trust has yet to be built fully.

One way to get there is through, for instance, what the U.K. or the U.S. is doing, which is to build a joint collaborative environment or a joint cyber-defence collaborative. Before an incident happens, channels of communication for information exchange and threat information exchange are shared on a voluntary basis, oftentimes, where the private sector gets a better understanding of how the information they give is actually used and flows. It becomes a true partnership between the private and public sector. Right now I think the situation is that there is some hesitancy for regulators, etc., to engage, but I think we all recognize that a closer public-private partnership is essential.

Ms. Jennifer O'Connell: Thank you.

That clarification is important, because when I hear “mandatory reporting”, I don't necessarily think that's confidential. We've had other testimony that it would be public mandatory reporting so that Canadians have a broader sense, but I think that distinction, at least from that perspective, is interesting.

There is also, I think, a significant onus on individuals or individual corporations to safeguard their security. You mentioned in your testimony that your organization has a policy of knowing where every component of the product comes from, but when companies have boards of directors and shareholders and cost-effectiveness is important, that might not be the case. What would your recommendation be to ensure the public is more aware of what they're purchasing—the onus on them—and then what can government do to encourage the private sector to not always look at just the bottom line but also at the cybersecurity piece?

Dr. John de Boer: A huge driver of security, particularly in the automotive sector, has been an emphasis on safety, right? When consumers start demanding safety or security, it changes. I spoke earlier about a software bill of materials or an ingredients list. When we buy things at the grocery store, we know exactly.... There is an ingredients list there. It's listed, right?

There could be and there is discussion in multiple jurisdictions about, for instance, a cyber safety rating for IoT devices, whether that be for your fridge or elsewhere. That could be considered. More awareness about whether one product is safer than the other for public consumption could be something that's considered. I think these are important steps, not just to raise awareness, but to also entice producers to build in security up front, because that's not happening.

● (0955)

Ms. Jennifer O'Connell: Do I have any more time?

The Chair: No. Thank you, Ms. O'Connell. I'm going to cut you off. You had three seconds.

Colleagues, I need some guidance here. We've run over our hour.

First of all, I'll turn to the clerk to find out if we know the arrival time of our friends.

We don't? Okay.

I have some committee business that I'd like to do in camera. We had anticipated that our friends would arrive at 10:15. That gives us 20 minutes. It's going to take a few minutes to go in camera. My thought, because this is such an excellent panel, is that we have a two-minute lightning round with each party. There's stuff that could get out. Is that an acceptable idea, two minutes?

Some hon. members: Agreed.

The Chair: Going now—

Mrs. Cheryl Gallant: Are we going in camera first?

Voices: No.

The Chair: It will be the Conservatives, the Liberals, the Bloc and the NDP, and then we'll call it regardless. The rounds are two minutes.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Mr. Chair, before you start my clock, I want to give notice of the following motion.

> That the committee undertake a study of no less than eight (8) meetings to review how the readiness of the Canadian Armed Forces is impacted by Canada's procurement processes and the capabilities of our defence industry to ensure that the Canadian military's needs are being met. And that the Department of National Defence, Canadian Armed Forces, Public Service and Procurement Canada, Office of the Auditor General, Parliamentary Budget Officer, Treasury Board, defence industry, military procurement experts and academics be invited to testify before committee on this matter; and that the committee report its findings and recommendations to the House.

We have that in both official languages, and we'll circulate it.

I will start my lightning round of questions.

First of all, I want to thank all the witnesses for being here.

The government has proposed Bill C-26 as a way to encourage industry to have a stronger cybersecurity defence. There have been a lot of concerns raised that the fines and penalties are overly prescriptive and brutal for individuals and companies, but yet these same types of fines and penalties aren't applied to the government itself.

I'd like to get feedback from Mr. de Boer in particular, as he represents a Canadian industry here. I do miss my BlackBerry phone from back in the day.

Who's responsible for protecting critical infrastructure, including in the private sector? Is it the Canadian Armed Forces, the Department of National Defence, CSE or the Government of Canada as a whole, or is it best that it come from the individual companies? You can also touch on the issue around available people, because the Business Council of Canada says that currently we have 25,000 unfilled positions in the cybersecurity world.

The Chair: You have a little less than a minute of time.

Dr. John de Boer: Who is responsible? It's unclear. That was part of my testimony. We need to clarify roles and responsibilities, and that clarity doesn't exist right now. We don't have a unity of effort.

When it comes to Bill C-26, it's an important start. We are late to the game when it comes to mandatory reporting on cyber-incidents in critical infrastructure, so we welcome that initiative. However, it's limited to four sectors.

The reality is that there's a lot of policy action happening right now. The critical infrastructure strategy is being renewed. It was drafted in 2009. Cyber isn't even mentioned. Then we have the national cyber security strategy and Bill C-26. All of these need to be united.

● (1000)

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

Who's speaking for the Liberals?

Mr. Fisher, you have two minutes.

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

Thanks, folks, for being here. I appreciate your testimony today.

I've asked this question previously. I'm interested in your thoughts on this: How can Canada better partner with the private sector to raise the cybersecurity bar across the country?

Yesterday I read a story in the CBC about Halifax Water. There was a test of their cybersecurity. Emails were sent to 55 people, and 45 of them responded. They clicked the link and sent all of their information.

We talk about mandatory reporting. We talk about the importance of critical infrastructure. When we think about infrastructure like Halifax Water and public utilities across our country in terms of mandatory reporting and sharpening their cybersecurity pencils, I'm interested in your thoughts.

We'll start with you, Mr. de Boer, and then maybe move to Mr. McSorley in the short time we have.

Dr. John de Boer: Very quickly, if AI-driven cybersecurity tools had been used on the Colonial Pipeline, our 2015 model would have stopped it. Use advanced technology. It can help with the personnel issue and also protect critical infrastructure.

Mr. Darren Fisher: Go ahead, Mr. McSorley.

Mr. Tim McSorley: Thank you.

I'll mention another bill here.

Currently the government is looking at the artificial intelligence and data act. I agree with Mr. de Boer that we need to be looking at innovative solutions, including AI, but we also need to make sure we have regulations in place. There are wide concerns in both the private sector and civil society. There are problems with what's contained in the AI and data act right now.

Mr. Darren Fisher: Thank you.

The Chair: Thank you.

Ms. Normandin, you have two minutes.

[*Translation*]

Ms. Christine Normandin: Thank you.

My questions tie in with what Mr. Bezan raised.

Mr. de Boer, you said that roles needed clarifying. You also said that the U.S. and Australia had their own versions of a cybersecurity minister. I recall one witness, Christian Leuprecht, telling us that Denmark had a cybersecurity ambassador.

You talked about uniting all the efforts under one position. What might such a position look like in our context? Do you have any recommendations for us? What features should such a role have?

[*English*]

Dr. John de Boer: The primary role of such an individual—it could be a parliamentary secretary—would, first of all, be to signal to all Canadians that cybersecurity is important. Second, it would be one individual empowered with ensuring policy coherence and program coherence across Canada. Currently, that does not exist.

I mentioned the Australian case, but the U.K. also has a parliamentary secretary responsible for cybersecurity. We used to have a parliamentary secretary for digital. That is no longer the case.

The role would be to look across the Government of Canada to ensure coherence and unity of effort and to unify our approach to defending the country.

[*Translation*]

Ms. Christine Normandin: Mr. McSorley, do you have anything to add?

[*English*]

Mr. Tim McSorley: Yes.

I would just share that I think we need a centralized office to engage with cybersecurity. One of the questions we have around Bill C-26 is that it's not clear whether this would fall under existing national security review bodies. Having an agency tasked with not only ensuring cybersecurity is handled properly but also that it's reviewed and accountable, and that there's transparency around it, would be important as well.

The Chair: Thank you, Ms. Normandin.

Ms. Mathyssen, you have the final two minutes.

Ms. Lindsay Mathyssen: In this committee, we've heard a lot about the overclassification of information, and that 90% of what Canadians classify doesn't need to be.

Mr. McSorley, how does that overclassification of intelligence create a barrier or problems for civil rights organizations in holding the community of those intelligence agencies truly accountable? What is your solution to that?

Mr. Tim McSorley: Thank you very much for the question.

It isn't just a concern among civil liberties and civil society groups but across many sectors in Canada that there needs to be a trust developed. There needs to be openness and transparency to the degree that we understand what Canadian agencies, including the CSE, are engaging in when they are engaging in protecting Canada's cybersecurity, engaging in active and defensive cyber-operations and engaging in signals intelligence.

The way to ensure this is happening is to have greater mandatory reporting around the activities that they're carrying out. For example, there's a lack of mandatory reporting in Bill C-26 right now, so it would be very difficult to track not only the ways that it's used but also whether there are any failings so we can improve the system. Oversight and review are simply not only about putting organizations on the defensive and calling them out but also seeing where we can learn from our errors and improve the operations.

Right now, there are the intelligence commissioner and NSIRA, and, as I mentioned, it's not clear that they have a role in reviewing Canada's cybersecurity operations, because they touch on national security but not necessarily in the way that those bodies always review it. Therefore, we think that either there needs to be a new position or there need to be amendments made to their mandate to clarify that they do have that mandate.

● (1005)

The Chair: Thank you, Ms. Mathyssen.

Mr. Nared, I saw that you had your hand up there. It's disadvantageous to be virtual when everyone else is physically present, so let me give you a minute or two to comment.

Mr. Tadej Nared: Thank you very much, Mr. Chair. I'll be very quick.

An idea on how to quickly improve cybersecurity is to make the whole IT industry accountable, and that means software and hardware vendors, because right now they have quite a unique status among all other industries.

For example, if you have a car and the brakes malfunction or something like that, they would be held accountable. However, in terms of the IT industry, such scenarios just don't come into account, ever—they do not, and they should. They should not just put products that are non-market-ready and that are insecure onto the market and endanger all of us from that.

Thank you very much.

The Chair: Thank you, Mr. Nared.

I want to thank all the witnesses. It seems to me, sitting here, that we could have carried this conversation on for the rest of the day quite easily. Personally and on behalf of the committee, I want to thank you for your presence. This is an extraordinarily difficult subject to grasp, particularly for those of us who are not in it on a daily basis and don't necessarily understand the nuances.

With that, thank you.

We'll suspend, go in camera and continue with committee business.

Mr. McSorley, if you didn't get all of your recommendations in, please coordinate with the clerk.

Mr. Nared, I think the clerk will reach out to you at a further date.

Thank you again.

The meeting is suspended.

[*Proceedings continue in camera*]