HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

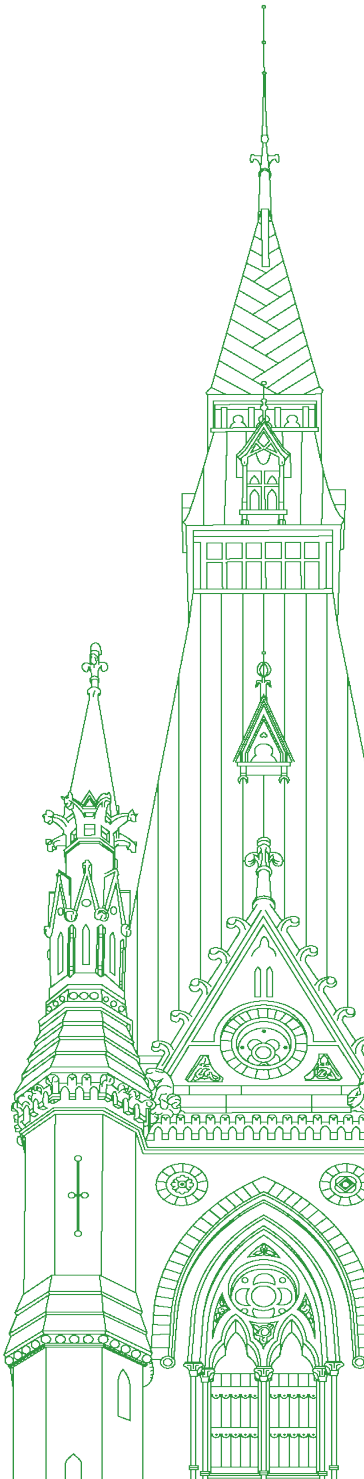
44th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 061

Tuesday, April 18, 2023



Chair: Mr. Ron McKinnon

Standing Committee on Public Safety and National Security

Tuesday, April 18, 2023

● (1635)

[*English*]

The Chair (Mr. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.)): I call this meeting to order.

Welcome to meeting number 61 of the House of Commons Standing Committee on Public Safety and National Security.

We will start by acknowledging that we are meeting on the traditional unceded territory of the Algonquin people.

Today's meeting is taking place in a hybrid format, pursuant to the House order of November 25, 2021. Members are attending in person in the room and remotely using the Zoom application.

Pursuant to the order of reference of Wednesday, September 28, 2022, the committee has commenced consideration of the annual report 2021 of the National Security and Intelligence Committee of Parliamentarians.

We welcome today, in person, four representatives of the National Security and Intelligence Committee of Parliamentarians, which I shall henceforth call NSICOP, as everybody else does. We have the Honourable David J. McGuinty, chair; Senator Frances Lankin, member; Lisa-Marie Inman, executive director; and Sean Jorgensen, director of operations.

Welcome to you all. Thank you for being here.

As agreed to prior to the meeting, up to 10 minutes will be given for opening remarks, after which we will proceed with rounds of questions.

Mr. McGuinty, go ahead, if you please. You have 10 minutes.

Hon. David McGuinty: Thank you very much.

[*Translation*]

Mr. Chair, committee members, thank you for your invitation to appear today.

In addition to Senator Frances Lankin, I am joined by two representatives of the NSICOP Secretariat: Ms. Lisa-Marie Inman, executive director, and Mr. Sean Jorgensen, director of operations.

[*English*]

It is my pleasure to be here to discuss the committee's 2021 annual report. The report accomplishes two objectives. First, it fulfills the committee's legislated annual reporting requirements. Second, it summarizes the special report we completed in 2021, which was our cyber-defence review.

I'll begin with the committee's four annual reporting requirements.

First, our annual reports must include the number of times a minister determined that a review we propose cannot proceed because it would be injurious to national security. To date this has not occurred.

Second, our annual report must disclose the number of times a minister refused to provide information to the committee because the information constituted special operational information and would be injurious to national security. To date this has not occurred.

Third, we are required to report the number of issues the minister referred to us for potential review. In 2021 there was one such referral. On June 4 the Minister of Health sent a referral to the committee regarding possible security incidents at the National Microbiology Laboratory in Winnipeg.

Fourth, we are required to include our findings and recommendations. In 2021 the committee came to four findings and made two recommendations, all as part of the cyber-defence review. I will discuss that report later in my remarks.

In addition, Mr. Chair, pursuant to the Avoiding Complicity in Mistreatment by Foreign Entities Act, 12 departments are required to provide their minister with an annual mistreatment report and then to provide it to NSICOP as soon as is feasible. All 12 departments have provided us with their annual mistreatment reports.

Next, I'd like to highlight that last year, the committee marked its fifth anniversary. Since its creation in October 2017, the committee has completed nine reviews, with 29 recommendations for the government.

In 2018 the committee completed reviews related to the Prime Minister's trip to India that year, the military's intelligence activities and how the cabinet sets the government's intelligence priorities.

In 2019 the committee completed reviews related to diversity and inclusion, foreign interference, the Canada Border Services Agency and the collection and use of information on Canadians by military intelligence.

In 2020 the committee completed an overview of the threats to Canada.

In 2021 the committee completed the cyber-defence review.

In 2022 the committee completed a review of the national security and intelligence activities of Global Affairs Canada.

Presently, the committee is completing its review of the federal policing mandate of the RCMP.

In the interest of pursuing our second foreign interference review, the committee has temporarily paused its work on the review of the lawful interception of communications for security and intelligence activities.

Members might recall that NSICOP is dissolved during writ periods and is then reconstituted within 30 sitting days after the return of Parliament. Therefore, over the past five years approximately there was one year in total not available to the committee to pursue its work. It was not operating because of two elections, in 2019 and 2021.

[*Translation*]

Now I would like to turn to the "Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack", published in 2021.

We conducted the review because of the importance of federal systems and networks, which form part of Canada's critical infrastructure. These networks store large amounts of personal information and are used to deliver essentially every government service.

Government networks are under relentless cyber-attack by a number of states, most notably China and Russia, and may be vulnerable to malware and other forms of cybercrime. Today, the federal government is a world leader in defending its networks, but this was not always the case.

In the early 2010s, China carried out damaging cyber-attacks against 31 federal departments. This was a wake-up call in terms of the scale of the government's cyber-vulnerability and its poor defences.

Since then, the government has incrementally developed a strong cyber defence system, in terms of both governance and technical capability.

● (1640)

[*English*]

This brings me to two of our findings.

First, our report found that over time the government's approach to cyber-defence evolved towards one that considers all government systems as a single enterprise. This horizontal approach, colleagues, has considerably improved cyber-defence, although we found it is challenged by the vertical nature of accountability in the government.

Second, our report found that not all federal organizations receive the same cybersecurity protection. There are two related reasons for this. First, the Treasury Board's cybersecurity policies do not apply to the entire government, and when they do apply, they do not always apply evenly. Second, departments are not obligated to adopt the cyber-defence services offered by Shared Services Canada and the Communications Security Establishment. This means that many federal organizations are entirely outside the government's cyber-defence perimeter, while others pick and choose services and do not subscribe to them all. These gaps and inconsistencies undermine the enterprise approach to cyber-defence. A system is only as strong as its weakest link.

With all this in mind, the committee made two recommendations. First, the committee recommended that the government continue to strengthen the enterprise approach to cyber-defence. Second, the committee recommended that the government fully bring all federal organizations into the cyber-defence perimeter, and that the cybersecurity policy suite should apply to all federal organizations, including Crown corporations.

The government agreed with both recommendations. Indeed, we are pleased that, for the first time, the government provided an official response to our recommendations in this cyber-review. However, the government has still not provided any updates with respect to 20 other recommendations contained in six of our previous reviews.

The last point we would like to raise is that this year we expect Parliament to begin a comprehensive review of the NSICOP Act. We're aware that your committee has sought to be designated as the House committee for this review. Once a committee is designated to conduct the review, our committee would be happy to make a specific series of recommendations about potential reforms of the act.

Today, I will only emphasize the importance of the committee's access to government information. Indeed, the committee faces several challenges to obtaining the information we are entitled to under the law and that we need to fulfill our mandate. For example, the committee is concerned that departments are applying an overly broad interpretation of what constitutes a cabinet confidence.

In closing, I wish to say that all of our reports are the result of the incredible and dedicated work of my colleagues on the committee. The cyber-defence report is yet another example of a unanimous, non-partisan review of a crucial government activity by a committee of security-cleared senators and members of Parliament from all major parties and groups.

Thank you very much, colleagues.

The Chair: Thank you, Mr. McGuinty, and thank you all for all your work over these many years to work to keep us safe.

We'll start now with our first round of questions. We'll start with Mr. Shipley for six minutes, please.

Mr. Doug Shipley (Barrie—Springwater—Oro-Medonte, CPC): Thank you, Chair, and thank you to the members for being here today and for sharing your time.

I'd like to start off by directing my first question to Mr. McGuinty, and if he has to pass it along, that's fine.

Mr. McGuinty, at the beginning of March, the Prime Minister's Office asked the Clerk of the Privy Council and the Minister of Intergovernmental Affairs to bring forward a plan to implement the five years of outstanding recommendations from your committee.

Given that it is now mid April, are you aware of any outstanding recommendations having been implemented since that announcement?

● (1645)

Hon. David McGuinty: The committee received, I believe maybe a week ago or less, a document that is an attempt to update Canadians on recommendations to counter foreign interference in Canada's democratic institutions. I believe the assignment given to the clerk and to Minister LeBlanc by the Prime Minister was to speak directly to recommendations not only from NSICOP but also from other authors who had evaluated the protocol process. I think the assignment was to let Canadians know how far the government has come in implementing our recommendations and its recommendations.

We're encouraged with what we've seen, but we would encourage this committee to call the government again to perhaps provide more detail on how it is moving forward.

Mr. Doug Shipley: Thank you for that. It's a nice segue to my next question.

I was a little shocked to find out that the government has only responded to one report in the five years of NSICOP's existence. Do you think a set time period in which the government must respond to your report should be implemented?

Hon. David McGuinty: It's an issue that's live among the committee members. Trying to ensure that the work that's done...it's very difficult, to be candid with colleagues. It's difficult and it takes a long time to arrive at these recommendations. We don't arrive at them lightly. The deliberations are long and extensive. There are some folks at this table who, I think, sat on our committee and understand what we speak about here.

We are hopeful that the government will now pay close attention, perhaps closer attention, to some of the recommendations, like what we put forward here today on cyber.

Again, I would encourage this committee to ask the government to come forward and to explain to what extent it has implemented the recommendations to bring more federal organizations inside the cybersecurity perimeter.

Mr. Doug Shipley: Thank you for that. Maybe I'll delve into that a little further.

We are all, obviously, sitting on committees, and it's great work that your committee is doing. We all work hard in these committees. Sometimes I wonder about these reports and what happens to them. Do they just go and sit on a shelf somewhere?

From what I mentioned in my last question, is your committee sometimes feeling that perhaps it's just not being acted on enough?

Hon. David McGuinty: There may be some times when we're looking for more immediate take-up. Sometimes it's difficult to point to the effects of the work. For example, the new architecture of review in Canada has compelled many organizations that are now subject to review to actually buttress and create new units inside their departments, such as the Department of National Defence. Prior to the existence of NSICOP and NSIRA, the Department of National Defence didn't really have a formal mechanism to respond to external review and now it does. That's encouraging.

The new architecture of review is pulling the government forward as a whole. There are some things we can point to directly. For example, the government did announce in the budget the creation of a foreign interference coordinator role at Public Safety—which is also in its recent report that I pointed to a minute ago entitled “Countering an Evolving Threat”. We've seen that some of the recommendations from NSICOP ended up directly in mandate letters for ministers, like DND and Public Safety. We've seen the public safety minister act directly on a CBSA review recommendation and implement direct change.

We're always looking for more take-up and more traction, because the purpose of the committee, why we're here, is to improve the situation for Canadians.

Mr. Doug Shipley: Thank you for that.

Mr. McGuinty, you touched on something in your opening remarks, namely, that we will soon be implementing or starting a five-year review of NSICOP.

I know this might be a little premature, but just to get our minds centred around some things, are there any major themes you would see for changes that we should be looking towards and implementing from that review?

Hon. Frances Lankin (Member, National Security and Intelligence Committee of Parliamentarians): Thank you.

I appreciate the question and can tell you that the committee has begun its work of thinking through this but we won't be putting forward specific recommendations until we have a committee to refer it to.

The chair has already indicated to you that one of the things that's very important to us is the issue of access to information.

I want to stress generally that the departments have been very good, and we've developed a very respectful relationship with organizations that at the beginning were really, you know, “these politicians, these parliamentarians, are going to have access to this information”.... There was some hesitancy there. By and large, it has been very good, but we have had specific incidents, as I think the chair referred to, where we think certain departments have perhaps given too broad an interpretation to what is a cabinet confidence.

The other question is, should cabinet confidences all be protected or in what circumstances? They don't have to be. They can be provided to us.

Those are the kinds of issues that we will be deliberating on. As of today, the only ones that we're prepared to say—because we've raised it in our own reports and our own comments about our reports when we've released them—are the two things about action or reporting back on recommendations being followed through on and the issue with respect to access to information in a timely and fulsome way.

● (1650)

The Chair: Thank you, Mr. Shipley.

Mr. Doug Shipley: I'm out of time, so thank you, all of you, for the work you do and for being here today.

The Chair: We will go now to Mr. Noormohamed.

Go ahead, please, sir. You have six minutes.

Mr. Taleeb Noormohamed (Vancouver Granville, Lib.): Thank you, Mr. Chair.

Thanks to all of you for your appearance here and being with us today.

I'd like to dig a bit into the importance of this committee.

Mr. McGuinty, you, your team and your colleagues have done a remarkable job of making sure that the work your committee does has been in the main non-partisan, with a tremendous amount of collaboration, and with what I hope are recommendations that all of us take seriously.

One of the concerns I've had over the course of the last few weeks particularly has been the attempt to politicize the nature of the work you do. I want to quote a specific comment that was made by the Leader of the Opposition in which he says, “NSICOP has been used in the past...and is being used here...to avoid accountability. It takes place in secret and is controlled by Justin Trudeau.”

I think it's important for Canadians to hear first-hand from you, as the chair, (a) whether or not that is true, (b) how you believe the role of NSICOP should be seen and, most importantly, how Canadians should view the committee and the important work your committee does.

Perhaps, Senator Lankin, you might also like to weigh in on this.

Hon. David McGuinty: The committee scrupulously avoids partisanship. I think the highest compliment that's been paid to the committee since we began is that a number of folks who have appeared before us have often said that if you were to close your eyes and listen to the conversation at the table, you actually wouldn't know from which political persuasion the commentary is coming.

We built what I think we like to refer to as “a nobility of purpose” around the work. We think there are some issues that transcend partisanship, that transcend any one government, and national security and intelligence is one of those issues.

It was a unique opportunity for Senator Lankin and me, in particular, who have been there since the beginning, to stand up the organization. It was like flying a fighter jet as we were building one. But the purpose of the committee really should transcend my chairmanship, our membership, the senior secretariat staff. It's an important mechanism for the future to allow for a full airing of classified information among colleagues from both Houses to treat these very important issues.

We all respect and understand that what goes on in the other arena, called the House of Commons or the Senate, is natural and is going to occur. The push and pull, the cut and thrust of that, is democracy, but when it comes to access to classified information and the treatment and the handling of that information, and the quiet, non-partisan opportunity to deliberate as colleagues, on behalf of 39 million Canadians, we think this is a really important structure for Canada, going forward, no matter who is in government, no matter who holds the seat as prime minister or minister, no matter what configuration the committee has.

There are comments sometimes about the role of the Prime Minister or of the government in the work of the committee that are, I would say, considerably off the mark. In the nine, 10 and soon 11 reviews that we have conducted, the Prime Minister of Canada has never instructed this committee to do anything. In fact, the only time we consult with the Prime Minister of Canada on our work is when we're presenting our reviews when the product is finished. The Prime Minister has an obligation to instruct the committee to redact, but on very, very transparent grounds.

The team that is here with us today—not just the members, but our senior secretariat folks—is extremely agile when it comes to entering into a discussion with officials in the government to say, let's talk more about that proposed redaction. We always tend towards being more transparent rather than less. We think that's important for Canadians to understand.

The debate that's going on now in the House, the Senate and in society is an important one; it's a really important one, but it's also a teachable moment for a lot of Canadians. For example, what is classified information? Why is classified information classified, and when can it be shared and when can it not be shared, and why isn't it being shared? Canadians get that. They can fully understand that.

We're trying to do our part in helping them understand that, and I'm sure Senator Lankin has much to add to that.

● (1655)

Hon. Frances Lankin: I think the chair said earlier, about the work of the committee, that all of our reports have been unanimous. They are, as indicated, in some ways multipartisan, but in other ways non-partisan.

One thing that I believe is such a strength of the committee is the fact that we do have cognitive diversity around the table. We have discussions that push and pull and think about it from this or that perspective. It's not just on the basis of political ideology; it's on the basis of backgrounds and the experience we bring. We've had people from the RCMP, from military and from provincial government. We have a range of individuals whose experience comes to bear in our consideration of items. I think that's very important.

The chair indicated that there has never been a time when the Prime Minister, the PMO or anyone weighed in on our work. I will echo that. I'll go further with him and say suggestions of that sort are patently false. There is no basis for that kind of a suggestion to be made because we protect ourselves and the nature of our work. As well, we've developed a competency that people respect and they respect our work. It's been very much a good exchange.

Before I was appointed to the Senate a number of years ago, I was a member of the Security Intelligence Review Committee, which was the predecessor to NSIRA. At that point in time, we were only reviewing CSIS. I do remember that we made recommendations about the need for a more broad review, which led to NSIRA. It was active discussion between members of our committee and people in the PMO and PCO of the day about establishing a committee of parliamentarians or parliamentary committee. We weren't precise on that at that point in time.

What is interesting is that we all had some hesitancy about whether a group of multipartisan or non-partisan parliamentarians would come together and be able to work in a way that respected all the secrecy requirements, understanding the nature of national security and the damage that can be done. Having lived through those debates and up to this point in time, I personally have an incredible confidence in the work that's being done there and a great respect for the individuals who put on their hat when they go into the House of Commons or into the Senate and take off that hat when they come into our committee for discussion. I think it serves Canadians well.

I think it serves parliamentarians well when they look at the result of it because it isn't one-sided. It is a product of good, deliberative discussion and collaboration in coming up with our recommendations.

The Chair: Thank you, Senator.

Thank you, Mr. Noormohamed.

[*Translation*]

I will now give the floor to Ms. Michaud for six minutes.

Ms. Kristina Michaud (Avignon—La Mitis—Matane—Matapédia, BQ): Thank you, Mr. Chair.

Mr. McGuinty, thank you very much to you and your team for coming here today. Thank you as well for the work that you do.

Before diving deeper into the annual report and the reviews you have carried out, I have a question. You mentioned that starting now, instead of publishing the summaries of your reviews in the annual report, you will publish them in special reports. I could not tell whether there was a reason for that decision. If there was, could you please explain it?

Hon. David McGuinty: We have to submit a report to Parliament every year. At first, we combined all reviews, like this one on cyber-attacks. As you can see, it's quite lengthy. We decided that, instead of presenting everything together in the annual report, we should conduct the reviews one at a time and submit them individually. That way, we have more time to work together. It is also easier for Parliament, the Prime Minister, and senior officials to receive the reviews and follow up on them.

That is the reason why we chose to separate the reviews. Before, in a single annual report, there might have been three reviews all at once. We made this decision to better manage our work. It was easier for us to operate this way.

● (1700)

Ms. Kristina Michaud: Thank you. This approach might also enable people to look into each detail of the reviews. Otherwise, when everything is lumped together, it's time-consuming to read and difficult to keep track of all the information.

As you probably know, our committee has studied Canada's posture in relation to Russia. In particular, we looked into the issue of cybersecurity, to determine if Canada was prepared to respond to threats of this kind. I take it that your committee has also looked at this matter in depth.

You say the government adopted a horizontal framework to protect itself against cyber-attacks. When we questioned witnesses who appeared before the committee, what we gathered was that non-government organizations are not always required to rely on the government or the various government services that are there to help them deal with threats or cyber-attacks. While it's understandable, I was nevertheless surprised to see that some government organizations did not possess exactly the same resources and tools, or if they do have them, they don't necessarily want to use them.

Can you tell us more about that and come back to the recommendations you made to the government?

Hon. David McGuinty: It is an architecture problem. The Financial Administration Act of Canada gives deputy ministers and the CEOs of Crown corporations the authority to decide if whether or not they will be part of the cyber-defence program provided by the federal government. We believe that this is a significant weakness.

[*English*]

We're only as strong as our weakest link.

[*Translation*]

Our cyber-defence system is well regarded nationally and internationally; it's a very solid system. However, if a cyber-attack is launched on a department, agency or Crown corporation that is not protected by our defence system, that could be used as a gateway into the entire governmental system.

That's the reason we are recommending that the federal government amend The Financial Administration Act in order to require that all organizations and Crown corporations be protected by the system provided by Shared Services Canada and the Communications Security Establisment.

Ms. Kristina Michaud: Has the government answered in the affirmative? Actually, has it answered at all? I don't remember if there was an answer.

Hon. David McGuinty: We are still awaiting a definitive answer, but we do encourage your committee to go ahead and communicate with the government, in this case that would be Treasury Board, to ask how things stand.

Ms. Kristina Michaud: As you explained, departments and agencies that have chosen the cyber-defence system could be indirectly infiltrated through others that haven't made that choice and have become the targets of a cyber-attack. That's why it's so important to use the system.

Do you have any other recommendations that you would like to make today or is there anything else you'd like to highlight from your cybersecurity review?

We know that cyber-attacks are a sign of the times. There are more and more of them. Just last week, there were all sorts of reports in the media. The websites of the Prime Minister, Hydro-Québec and many other organizations were hit by cyber-attacks. I am guessing that recommendations will be made and that the system is unfortunately not quite 100% bulletproof right now.

Hon. David McGuinty: I believe that our committee would state without any hesitation whatsoever that this is just the beginning. The attacks will go on, there will be more and more of them and they will become increasingly complex.

We laid out the situation in the report using six case studies. Two of those case studies hadn't been made public before. We did this in order to present the risks that are involved when not all agencies and departments are protected by the federal defence system.

I think that the members of your committee, as well as other MPs, would find these six extremely concrete case studies most interesting. For example, the National Research Council Canada lost 40,000 documents and spent $100 million to repair its system. The Department of National Defence, another case study, was targeted at least once. Yet another case involves a Crown corporation. All these case studies show the inherent risks when information about Canadians is held by the government.

● (1705)

Ms. Kristina Michaud: Thank you very much.

The Chair: Thank you, Ms. Michaud.

[*English*]

We'll go now to Mr. Julian.

Please go ahead, sir, for six minutes.

[*Translation*]

Mr. Peter Julian (New Westminster—Burnaby, NDP): Thank you very much, Mr. Chair.

I would also like to thank the witnesses, Ms. Lankin and Mr. McGuinty.

I'm going to pursue Ms. Michaud's line of questioning.

Mr. McGuinty, you mentioned the fact that 31 federal departments were targeted by China. Most of these cyber-attacks were not successful. Last week, the Internet sites of Hydro-Québec, the Port of Quebec and the Laurentian Bank were hit. In all those cases, Russia was responsible.

I would firstly like to know how we can determine if these cyber-attacks were successful or not, or if their defence systems were up to the task or not.

Secondly, as you so eloquently said, Mr. McGuinty, these attacks are going to become increasingly complex and more and more frequent. I am looking at the recommendations, and it seems to me that the federal government has not followed up on all of them. Are we too slow to respond to the growing threat to our infrastructure?

Hon. David McGuinty: As to knowing if Russia was successful or not or if we did indeed counter an attack, I think those questions should be addressed to the Communications Security Establishment. They would be able to answer you. Our committee has not really looked at the attacks carried out over the last two or three weeks.

[*English*]

The case studies that we have put forward illustrate how sophisticated foreign state actors and other actors can be. In some cases, the attacks have taken place on a federal organization. They were completely unaware of it, and were only informed of it by CSE after the fact. In some cases, under new powers the government has given some companies in our essential systems, a private sector company can now come to the Minister of National Defence and ask for authorization to deploy CSE capacity to help stop a problem with a critical infrastructure company.

The Chair: We seem to have a translation issue here. Can we check that please?

The floor audio works, but English doesn't. Can we try a little bit of French?

[*Translation*]

Hon. David McGuinty: As you wish, I will say a few words in French. Is it working?

[*English*]

The Chair: Please proceed.

Hon. David McGuinty: As I was saying, the six case studies, Mr. Julian, illustrate.... They were chosen deliberately by the members to allow parliamentarians, Canadians and readers to understand the practical implications of not taking steps to protect. As I say, the private company...the first time using CSE powers. That's the first time this case study has been made public.

The attack on the CRA called the Heartbleed attack is case study number 3. In case study number 4, the National Research Council was attacked by China. We talked about the loss of 40,000 files. China used its access to the NRC to infiltrate other government organizations. It was very expensive to clean that up—$100 million at least. In case study number 5, huge amounts of data were stolen from DND by a foreign actor. In case study number 6, in 2020, a state compromised the network of a Crown corporation.

Are we slow off the mark to respond to this? I don't know if the committee really examined that. I don't know if we examined it comparatively. We do know that CSE's abilities are now increasingly called upon internationally. We know for example that the government of the United Kingdom has called upon Canada's CSE to help with their cyber-defence systems.

I hope I've answered some of your questions.

● (1710)

Mr. Peter Julian: Let's come back to NSICOP. You did talk about the five-year review. I hope I quoted this accurately. I put quotation marks around it. One of the concerns that you had was the overly broad interpretation of cabinet confidence. First, does that make it more difficult for NSICOP to do its work? Second, what are the other tools that you need to do your work better at a time when there are more threats around foreign interference, more threats around cyber-attacks, more threats than we've experienced perhaps previously in our history as a country?

Hon. David McGuinty: I'm going to ask Lisa-Marie Inman to address the question of cabinet confidence, because she's on the front line often dealing with this.

One of the things that might help the committee is positive reinforcement by all parliamentarians. All parties and the Senate are represented on the committee, so respect the fact the committee has to work in closed quarters, has to proceed with enormous discipline and can't go out and comment gratuitously on subjects that are part of media reports or the cut and thrust of debate.

We really do try to focus on the evidence, focus on the classified information, and we like to think that the quality of the reviews speak for themselves, but on this question, if I could, on cabinet confidence, I think Ms. Inman is best placed to speak to it.

Ms. Lisa-Marie Inman (Executive Director, National Security and Intelligence Committee of Parliamentarians): Thank you for the question.

As Senator Lankin pointed out, the committee's not entitled to receive cabinet confidences, but it's also not prohibited from receiving them. The particular issue the committee pointed out in some of its previous work is not so much that the committee believes its work has been compromised or hindered by not being able to receive cabinet confidences; it's really two pronged.

First, departments aren't obliged to identify that they're not providing documents or relevant documents that are subject to cabinet confidence, so the committee doesn't know what it doesn't know. If there's a document or information subject to cabinet confidence, the committee doesn't necessarily know the document exists, because it doesn't need to be provided.

The act doesn't say you have to identify when you're not providing something; the committee is simply not entitled to receive that information. It's not necessarily that the committee has looked at things and identified that this is an obvious thing we're missing and that we need to go back to get that. It's more that it's useful to know what exists so that the committee can gauge the extent of information it may not be receiving or information it should be receiving.

Also what we have noticed, largely as a result of inadvertently getting information subject to cabinet confidence that is later identified as being cabinet confidence information, is that in those instances, we have been able to discern that the application of the definition was sometimes very broad. As I'm sure you all know, the legislative definition in the Canada Evidence Act is quite broad and can be taken to quite an extreme.

The question is, which cabinet confidences are in need of protection from the committee? Are they all? Is there a category of cabinet confidence the committee should be receiving? To be able to really dig into that question, it would be useful to know what the committee is currently not getting and to perhaps issue some sort of guidance or clarify the definition in terms of the government documents that need to be provided.

The Chair: Thank you, Mr. Julian.

That wraps up our first round. We'll start our second round. It seems probable that we won't be able to do a full second round, but we'll start with Mr. Motz.

Mr. Motz, go ahead for five minutes.

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

Thank you to the committee, Chairman McGuinty, Senator Lankin and the secretariat officials. Thanks for being here.

When I look back over my years so far in this responsibility, they pale in comparison to my experience on NSICOP. It was probably the best and most enjoyable time I've had, because it felt like I was making a difference. Why? It was non-partisan, and it was legitimately non-partisan. I can say that unequivocally. Kudos to you guys for setting that up. It was well done, and I enjoyed my time there.

There's so much I'd like to say and ask, but I'll try to focus my comments.

I appreciate your comments on the same battle we had back then on the broad interpretations of cabinet confidences and the realization that people on that committee, not only those on the secretariat but also the members of the committee, Senators and MPs, have the same or higher security clearance than most cabinet ministers do. That's important to remember—and we're bound by legislation. There is frustration, and I think this committee needs to have full access to cabinet confidences, because that broad an interpretation doesn't allow full transparency. I appreciate that.

The other thing I really appreciated about NSICOP is the fact that its chair has pushed for broader transparency on the redaction process. I think that is key for public confidence in what we do and what we do as whole of government. I want to applaud those efforts. We're not there yet, but we're headed in the right direction, so thank you for that.

I want to get to a question on cyber-defence and cybersecurity, but we talked a couple of years ago—

● (1715)

The Chair: Pardon me, Mr. Motz.

The bells are ringing. We need unanimous consent to carry on. I propose we carry on to 5:30.

Do we have unanimous consent?

Some hon. members: Agreed.

The Chair: Very well. Thank you all.

Carry on, Mr. Motz.

Mr. Glen Motz: Thank you, Chair.

We talk about a legislative requirement to have the NSICOP review within five years. It has been nearly seven years. What steps do you think we need to take to push that a little harder to make sure it happens? I believe, as others around this table, that this is probably the best committee to do that review. When we do it, there should be some urgency to it, I believe. We can get into lots of things, but what would you suggest, as NSICOP, we focus on?

Hon. David McGuinty: There are some practical challenges we do face from time to time. We're making, I think, great progress. Maybe Sean Jorgensen, our director of operations, can speak a little bit about the progress we've made on the redaction process.

Let me step back and publicly thank you, Mr. Motz, for your service at NSICOP. You were a superb member and represented not only your constituents, but also your party and the House very well. We miss you.

There are some practical challenges. For example, one of the challenges Lisa-Marie Inman faces is that we often can't get top-secret interpreters. We can't rely on interpreters, for example, who interpret for cabinet, because they're not sufficiently cleared, so we need a different category of interpreters. That's sometimes a bit of a challenge. During the pandemic we managed to hold ourselves together by having people on very secure satellite systems and meeting virtually across the country and so on. Sometimes the pace—

Mr. Glen Motz: Sorry, Mr. McGuinty, I don't mean to cut you off, but I want to get into cybersecurity.

Hon. David McGuinty: Oh, I'm sorry. Okay.

Mr. Glen Motz: I have a follow-up question to Ms. Michaud and Mr. Julian's.

Now, the report on cyber-defence and preparedness states that many governing organizations, such as Crown corporations, do not fall under Treasury Board policies on cybersecurity issues. We dealt with this a number of years ago. You recommend that this needs to be fixed. That hasn't happened—as of a month ago, that has yet to occur. Can you reinforce the urgency that those agencies fall under Treasury Board policy, because cyber-attacks and cybersecurity affect them as well?

Hon. David McGuinty: I would implore this committee to call forward here to this committee a number of federal government representatives, including the Treasury Board, and perhaps CSE, Shared Services Canada representatives, to put those questions directly to them. They know what we've called for. They've seen the recommendations.

But on the urgency, I think Mr. Jorgensen is best-placed to give you 30 seconds on why this is so important to do now.

● (1720)

Mr. Sean Jorgensen (Director of Operations, Secretariat of the National Security and Intelligence Committee of Parliamentarians, National Security and Intelligence Committee of Parliamentarians): Thank you, Mr. Motz.

In 30 seconds, I think in case study 6, the committee was very clear that there wasn't just one Crown corporation that was hit. CSE came out and said, in fact—and it's in the report—that there were indications that a number of them had been hit. This committee, Canadians, those Crown corporations, will never know they were hit by an advanced actor in this space. That is the very reason why Treasury Board needs to be pushing harder in that space.

Mr. Glen Motz: Thank you very much. I appreciate your service.

The Chair: Thank you, Mr. Motz.

Now we go to Ms. Damoff for five minutes, please.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you, Chair.

Thank you, Mr. McGuinty, Senator Lankin and others for being here today. I especially thank you for the work you do on NSICOP.

It's been in the news a lot lately. I'm so privileged and proud that I was on this committee when we created NSICOP, as well as NSIRA. At the time, Canada was late to the game in creating this committee. I think at the time the U.K. had had a committee similar to ours for about 20 years. That's why we said we'd review it in five years, because we wanted to see how it was working and how it evolved. I think my friend's math was a little off—it's not been seven years, but about five and a half. I'm disappointed to hear about the cabinet confidences, because that is something we discussed at the time of the creation of the committee.

You were talking about top-secret interpreters. I think one of the things that have been missed in the conversation generally about NSICOP is that it's not "top secret" because you're not wanting to be transparent with Canadians. Can you maybe explain why you have a top-secret clearance, and why you're meeting in a different location? Why is that critical to the work you do?

Hon. David McGuinty: Thanks for the question.

It speaks directly to the access the committee has to highly classified information. That information is shared after a process of screening members for top-secret security clearance, swearing an oath and, effectively, as parliamentarians, signing away our parliamentary privilege.

It's also important for members and Canadians to understand that the government doesn't have a majority of members on this committee. It was actually designed so that no government would have a majority of members on the committee. In fact, with the Senate and House combined, the government is always in a minority situation. However, I think it's important for members and Canadians to know that, in the last five and a half years, we've never had to hold a vote. Everything has been unanimous. If we don't have a unanimous outcome, we go back at it again and deliberate.

It's important for us to remind Canadians that we deal with classified information and material. We have to be careful in how we use and share it, because it speaks to, for example, the sources and methods behind it. Where did this information come from? How did our information collectors obtain it? If it's shared publicly, that can put at risk those systems. It can put at risk the Canadians who are good women and men working in security and intelligence in this country. They are working to help keep us safe and deal with national security and intelligence threats. We have to be very careful, and behind closed doors, because some of the information we get is from our Five Eyes partners. Perhaps it's shared with us in great confidence that it won't be shared again or passed on anywhere else, in any other shape or form.

There are privacy considerations we have to work around. The committee is not choosing to hide itself in a secure facility somewhere because it doesn't want to see the light of day. On the contrary, Senator Lankin and other members—and Mr. Motz, during his time at NSICOP—were very forceful in helping the committee come to the conclusion that we want to be as transparent as we can. We want to share as much information as we can. We want to push out on the redaction process as hard as we can for Canadians' benefits.

However, the decision to do things in a secure facility when handling highly classified information is not something we invented just because we want to be secret people. It's because we have to handle this information.

● (1725)

Ms. Pam Damoff: Also, you're required to keep it secret for life. It's not just during your time as a parliamentarian. Is that correct?

Hon. David McGuinty: That's correct. Under the Security of Information Act and the oath we swear, no information of this nature can ever be wittingly or unwittingly shared.

Ms. Pam Damoff: Would you agree that our democracy in Canada is one of the strongest and most stable in the world?

Hon. David McGuinty: I'm not sure I can answer that question completely. It's not something the committee has applied its mind to.

I will say that, with respect to the cybersecurity review we've done, we have progress to make. It's a work in progress. However, I would want Canadians to understand that the system we've evolved in Canada, on the cybersecurity front at the federal level, is very good and world-renowned, frankly. We should be confident we have a system in place that's keeping our information safe, as well, but there is work to be done.

Ms. Pam Damoff: I know my time is up, but I want to say I'm very proud of the work you and the committee are doing, and I thank you sincerely for it.

Hon. David McGuinty: Thank you very much. I'll pass it on to the other members.

[*Translation*]

The Chair: Thank you.

Ms. Michaud, you have the floor for two and a half minutes.

Ms. Kristina Michaud: Thank you, Mr. Chair.

I have a question about the allegations of foreign interference.

As we know, on March 6 of this year, the Prime Minister announced that the NSICOP would be undertaking a review of foreign interference in the 43rd and 44th federal elections. Some authorities or organizations have already started their reviews of these alleged cases of foreign interference. The Prime Minister also appointed a special rapporteur who will be charged with the work. You probably know that the Bloc Québécois has asked for an independent and public inquiry on this issue. If the votes of some Canadians were not what they initially intended, we think that those Canadians should be made aware of what happened.

Given that the members of your committee are bound by confidentiality and secrecy constraints, do you believe that your committee is best placed to conduct such a review?

Hon. David McGuinty: The committee members have not discussed this. We received a request from the Prime Minister to continue our work in the field of foreign interference. You should know that we have already submitted to the House of Commons a report on a review that covered three years worth of activities and over 40,000 documents. It was the most extensive review done in Canada on the subject. We submitted our report to the Prime Minister and to Parliament three years ago. We are picking up where we left off and concentrating on what happened during the last two elections.

As to the work of Mr. Johnston and the National Security and Intelligence Review Agency, that remains to be seen. We do not know what Mr. Johnston will recommend if he recommends anything at all.

As for our committee, we will carry on with our work. We have made our work agenda public. Honestly, we don't have any other comment to make on all the debates that are going on outside of our committee. We are concentrating on the work at hand.

[*English*]

The Chair: Thank you.

Mr. Julian, please go ahead, for two and a half minutes.

Mr. Peter Julian: Thanks very much, Mr. Chair.

On the issue of foreign interference, the NDP brought forward, and Parliament passed, a motion calling for a public inquiry.

There is no doubt that NSICOP has an important role to play. We also firmly believe that a public inquiry is warranted and needed in this regard. When we look at the excellent recommendations you put forward, again there is a sense, as the allegations have come out in the last few months, of possible support by the Chinese government of certain candidates from a couple of political parties. Concerns were already raised last year around Russian interference in Canada. We saw this with the so-called “freedom convoy”, which caused such misery in downtown Ottawa, depriving people of groceries, medication, and sleep. These are major concerns.

I see the recommendations, but I also note that to adequately respond to the threat of foreign interference requires Elections Canada to be bolstered and the disinformation campaigns to be stopped. I see the recommendations, but do you feel that a broader degree of coordination is warranted to push back against this to ensure that, after you've done your review of previous elections, we can get the answers for Canadians and ensure that in future elections we can stop any possibility of those attempts to influence our electorate increasing or deepening in any way?

You offer these recommendations. What about the coordination to actually get them implemented?

● (1730)

Hon. Frances Lankin: You asked a question that perhaps asks us to predict what our recommendations will be on this review, and we haven't done the review yet, so please excuse me if I don't go so far as to adequately answer that.

First of all, the recommendations that came out in the first part of our foreign interference review were based on the period of study we looked at. Whether it's that or whether it's cybersecurity, we see the world speeding up on these issues, so that will be something that will be part of this as we look at this and understand it.

It also calls upon us to understand a bit of the history of how this has come along. It's not as if it's just now that we're finding out about these cases of interference. There have been alarm bells over the years. I'm one who firmly believes that governments of all political stripes have responded by putting in place measures and have continued to build on those. If anything, what we will look at is whether they have kept pace with the need, but we are not at that point to be able to answer that. I'm sorry.

The Chair: Thank you. I'm afraid we have to draw the line there.

Thank you to NSICOP for all the work you do on an ongoing basis. It's very important. We appreciate your time with us today. It's very helpful.

Thank you all.

With that, we are adjourned.