HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 089 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, December 5, 2017

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Tuesday, December 5, 2017

● (0845)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): I'm going to call this meeting to order. This is the 89th meeting of the public safety committee.

We have with us two witnesses, one of whom, at least, is very familiar with this process, Mr. Neve and MS. Carvin, professor at Carleton University.

I understand that, between the two of you, you cut a deal and Professor Carvin is going to go first.

We look forward to what you have to say.

Professor Stephanie Carvin (Assistant Professor, Norman Paterson School of International Affairs, Carleton University, As an Individual): I'd like to thank the committee for inviting me to speak on Bill C-59, the most comprehensive and far-reaching reform to national security in Canada since 1984. I would like emphasize that I am not a lawyer. However, I do have experience working in national security and intelligence, and I study this area for a living. Indeed, in the interest of transparency, I would like to state that from 2012 to 2015, I worked at the Canadian Security Intelligence Service as a strategic analyst.

My comments are, of course, my own, but they're informed by my research and experience as the national security landscape in Canada has evolved in a relatively short period of time. All of this is to say that today my comments will be focused on the scope of this bill and will address some of the areas that I believe this committee needs to, at the very least, consider as it makes recommendations.

First and foremost, I wish to express my support for this bill. I believe it contains four important steps that are essential for Canadian national security and the functions of our national security agencies.

First, it provides clarity as to the powers of our national security agencies. There's no better example of this than part 3, the CSE act, which gives our national signals intelligence agency statutory standing and spells out its mandate and procedures to a reasonable extent. Given that the first mention of this agency in law was the 2001 Anti-terrorism Act, this bill takes us a long way towards transparency.

Second, Bill C-59 outlines the limits on the power of our national security agencies in a way that will provide certainty to the public and also to our national security agencies. In particular, the bill clarifies one of the most controversial parts of the current legislation formerly known as Bill C-51, that is, CSIS' disruption powers.

While it might be argued that this is taking away CSIS' ability to fight threats to Canada's national security, I disagree. Having found themselves embroiled in scandals in recent years, it is little appreciated how conservative our national security agencies actually are. While they do not want political interference in their activities, they no doubt welcome the clarity that Bill C-59 provides as to these measures.

Let there be no doubt that the ability to disrupt is an important one, particularly given the increasingly fast pace of terror investigations, especially those related to the threat of foreign fighters. In this sense, I believe that Bill C-59 hits the right balance, grounding these measures squarely within the Charter of Rights and Freedoms.

Third, Bill C-59 addresses long-standing problems related to review, and in some cases oversight, in Canadian national security. I will not go over the problems of our current system, which has been described as “stove-piped” by experts and commissions of inquiries. I will, however, state that the proposed national security and intelligence review agency, NSIRA, and intelligence commissioner —in combination with the new National Security and Intelligence Committee of Parliamentarians, NSICOP—create a review architecture that is robust and that I believe Canadians can have confidence in.

Fourth, in its totality, Bill C-59 is a forward-looking bill in at least three respects. First, the issue of datasets is not narrowly defined in law. While this has been a cause of concern for some, I believe this is the right approach to take. It allows flexibility of the term, but at the same time it subjects any interpretation to the oversight of the intelligence commissioner and the minister. It subjects the use of datasets to the internal procedures of the national security agencies themselves—and limits who may have access—and the review of the NSIRA and NSICOP.

Second, it takes steps to enhance Canada's ability to protect and defend its critical infrastructure. Increasingly, we are seeing the abilities of states and state-sponsored actors to create chaos through the attacks on electrical grids, oil and gas facilities, dams, and hospital and health care facilities. Much of this critical infrastructure is in the hands of the private sector. This bill takes steps to ensure that there is a process in place to address these threats in the future.

Third, Bill C-59 puts us on the same footing as our allies by mandating an active cyber-role for our national signals intelligence agency. I appreciate the legal and ethical challenges this raises, especially should CSE be asked to support a DND operation. However, the idea that Canada would not have this capability is, I think, unacceptable to most Canadians, and would be seen as unfortunate in the eyes of our allies, many of whom have been quietly encouraging Canada to enhance its cyber-presence in the wake of cyber-threats from North Korea, China, and Russia.

To reiterate, I believe this is a good bill, but there's room for improvement. I'm aware that some of my legal colleagues, especially Craig Forcese, Kent Roach, and Alex, of course, will be speaking to certain specific legal issues that should be addressed to make the law more operationalizable and compliant with our Constitution.

I encourage the committee to seriously consider their suggestions. However, I'm going to focus on four areas that may be problematic in a broader sense, which I believe the committee should at least be aware of or consider when it makes recommendations.

● (0850)

First, I think it's important to consider the role of the Minister of Public Safety. To be clear, I believe our current minister does a good job in his current position. However, the mandate of the Minister of Public Safety is already very large, and this bill would give him or her more responsibilities in terms of review and, in some cases, oversight. At some future date, the scope of this ministry may be worth considering.

Having said this, I acknowledge a paradox. Requiring the intelligence commissioner's approval for certain operations, as is clear in proposed subsections 28(1) and 28(2) of the proposed CSE Act, and potentially denying the approval of a minister is, in my view, at odds with the principle of ministerial responsibility in our Westminster system of government.

To be sure, I understand why this authority of the intelligence commissioner is there. Section 8 of the charter insists on the right to be protected from unreasonable search and seizure. The intelligence commissioner's role ensures that this standard is met.

Why is this a problem? Canada has an unfortunate history of ministers and prime ministers trying to shirk responsibility for the actions of our security services, which dates back decades. Prime Minister Pierre Trudeau used the principle of police independence to state that his government could not possibly engage in review or oversight of the activities of the RCMP even though the national security roles of the RCMP are a ministerial responsibility. There is simply a tension here with our constitutional requirements and with what has been the practice of our system for decades. If this bill is to pass through, it will be up to members of Parliament to hold the minister to account, even if he or she tries to blame the intelligence commissioner for actions not taken.

Second, despite the creation of no less than three major review agencies, there's still no formal mechanism for efficacy review of our security services. We will receive many reports as to whether or not our security services are compliant with the law, but we still will not have any idea of how well they are doing it. I'm not suggesting we need to number-crunch how many terrorism plots are disrupted. Such a crude measure would be counterproductive. However, inquiring as to whether the analysis produced supports government decisions in a timely manner is a worthwhile question to ask. Efficacy review is still a gap in our national security review architecture.

Third, while I praise the transparency of Bill C-59, I'm also concerned about what I'm calling “report fatigue”. I note that between last year's Bill C-22 and now Bill C-59, there will have been at least 10 new reports generated, not including special reports as required. It is my understanding that some of these reports are very technical and can be automatically generated when certain tasks such as, hypothetically, the search of a dataset is done. However, others are going to be more complex. More briefings will also be required. Having spent considerable time working on reports for the government in my former work, I know how difficult and time-consuming this can be.

Finally, and related to this last point, it is my understanding that the security services will not be receiving any extra resources to comply with the reporting and briefing requirements of either Bill C-22 or Bill C-59. This concerns me, because I believe that enhanced communication between our national security services with the government and review bodies is important. As the former's powers expand, this should be well resourced.

In summary, the ability to investigate threats to the national security of Canada is vital. I believe that for the most part, Bill C-59 takes Canada a great step towards meeting that elusive balance between liberty and security. In my view, where Bill C-59 defines powers and process, it should enable our security services to carry out their important work with confidence knowing exactly where they stand. Further, the transparency in the bill will hopefully go some way towards building trust between the Canadian public, Parliament, and our security services.

Thank you for your time. I look forward to your questions.

● (0855)

The Chair: Thank you, Professor Carvin.

Mr. Neve, please go ahead for 10 minutes.

Mr. Alex Neve (Secretary General, Amnesty International Canada): Thank you very much, Mr. Chair.

Good morning, committee members. Amnesty International certainly welcomes this opportunity to appear before you in the course of your review of Bill C-59. I'd like you to know at the outset that I'm here on behalf of both the English and francophone branch of Amnesty International Canada, and thus on behalf of our 400,000 supporters across the country.

Amnesty International has a long history of frequent appearances before parliamentary committees dealing with national security matters, be that studies of proposed legislation or reviews of existing legislation. That's not because we're national security experts. Our expertise, of course, lies in human rights. Our interest in Bill C-59, therefore, comes directly from our mandate to press governments to uphold their international human rights obligations. Documenting and responding to human rights violations arising in a national security context and pressing governments to amend national security laws, policies, and practices to conform to international human rights obligations have long featured prominently in Amnesty International's research and campaigning around the world, long predating September 11.

National security is often blatantly used as an excuse for human rights violations, clearly intended simply to punish and persecute political opponents or members of religious and ethnic minorities. National security operations have frequently proceeded with total disregard for obvious human rights consequences, leading to such serious human rights violations as torture, disappearances, and unlawful detention. Without adequate safeguards and restrictions, overly broad national security activities harm individuals and communities who pose no security threat at all. In all of these instances, the impact is frequently felt in a disproportionate and discriminatory manner by particular religious, ethnic, and racial communities, adding yet another human rights concern.

These concerns are by no means limited to other parts of the world. Over the past 15 years, Amnesty International has taken up numerous cases involving national security-related human rights violations related to the actions of Canadian law enforcement and national security agencies. These concerns have been so serious as to be the subject of two separate judicial inquiries, numerous Supreme Court and Federal Court rulings, and several significant apologies and financial settlements totalling well over $50 million to a number of Canadian citizens and other individuals whose rights were gravely violated because of the actions of Canadian agencies. I think of Maher Arar, Benamar Benatta, Abdullah Almalki, Ahmad El Maati, Muayyed Nureddin, and Omar Khadr. This is why we bring our human rights analysis to legislation such as Bill C-59—to ensure that provisions provide the greatest possible safeguards against human rights violations of this nature.

In commenting on the bill, I will touch briefly on five areas: first, the need for a stronger human rights anchor in the bill; second, the bill's national security review provisions; third, positive changes in Bill C-59; fourth, concerns that remain; and fifth, issues of concern that have not been addressed in the bill.

The first area is the need for a national security approach anchored in a commitment to human rights. In the review that preceded Bill C-59, we urged the government to use the opportunity of the present reform to adopt a clear human rights basis for Canada's national security framework. That is an approach that is not only of benefit, evidently, for human rights, but truly lays the ground for more inclusive, durable, and sustainable security as well. Currently, other than the Immigration and Refugee Protection Act, none of Canada's national security legislation specifically refers to or incorporates Canada's binding international human rights obligations.

We recommended that those laws be amended to include provisions requiring legislation to be interpreted and applied in a manner that complies with international human rights norms. That was not taken up in Bill C-59 except for one very limited reference to the convention against torture. This is important in that it sends a strong message of the centrality of human rights in Canada's approach to national security. It is also of real benefit when it comes to upholding human rights in national security-related court proceedings.

Our first recommendation, therefore, remains to amend Bill C-59 to include a provision requiring all national security-related laws to be interpreted in conformity with Canada's international human rights obligations.

● (0900)

Second, we strongly welcome and support the provisions in part 1 of Bill C-59 creating the national security and intelligence review agency. Amnesty International has been calling for the creation of a comprehensive and integrated review agency of this nature since the time of our submissions to the Arar inquiry in 2005. This has been one of the longest-standing and most serious gaps in Canada's national security architecture. We do have three associated recommendations.

First, in keeping with the earlier recommendation I just made, the mandate of the review agency should be amended to ensure that the activities of security and intelligence agencies will be reviewed specifically to ensure conformity to Canada's international human rights obligations.

Second, the review agency must have personnel and resources commensurate with what will be a significant workload. We endorse the recommendation made by Professor Kent Roach that the provision allowing for a chair and additional commissioners numbering between three and six is inadequate, and would suggest that the number of additional commissioners be raised to between five and eight.

Third, we continue to be concerned about the review specifically of the Canada Border Services Agency. Unlike many of the agencies that will be reviewed by the new agency, the CBSA does not have its own stand-alone independent review body. The new review agency will have the power to review CBSA's national security and intelligence-related activities, but there still is no other independent agency reviewing the entirety of CBSA's activities, despite the growing number of cases where the need for such review is urgently evident, including deaths in immigration custody. This imbalance will inevitably pose awkwardness for the review agency's review of CBSA, and it underscores how crucial it is for the government to move rapidly to institute full, independent review of CBSA.

We'd like to highlight improvements. First, our concerns about the overly broad criminal offence in Bill C-51 of advocating or promoting the commission of terrorism offences in general have been addressed by the proposed revisions to section 83.221 of the Criminal Code, which would instead criminalize the act of counselling another person to commit a terrorism offence, which was already a criminal offence essentially.

Second, the threat reduction powers in Bill C-51, which anticipated action by CSIS that could have violated a range of human rights guaranteed under the Charter of Rights and under international law have been significantly improved. However, we think it needs to go further, and there needs to be specific prohibition of the fact that CSIS will not involve threat reduction of any kind that will violate the charter or violate international human rights obligations. We also welcome the changes made to preventive detention, but have some recommendations as to how that can be improved.

We remain concerned about the Secure Air Travel Act provisions, which we do not think address the many serious challenges that people face with the application of the no-fly list. Much more fundamental reforms are needed, including a commitment to establishing a robust redress system that will eliminate false positives, and significant enhancements to listing and appeal provisions to meet standards of fairness.

Because I know my time is limited, let me end with some provisions that remain unaddressed in the legislation.

One of the most explicit contraventions of international human rights in Canadian national security law, going back over 20 decades now, is the provision in immigration legislation allowing individuals in undefined exceptional circumstances to be deported to a country where they would face a serious risk of torture. It's a direct violation of the UN convention against torture. UN human rights bodies have repeatedly called for this to be addressed. Bill C-59 passed on the opportunity to do so. We would recommend that be taken up.

Finally, Bill C-59 also fails to make needed reforms to the approach taken to national security in immigration proceedings. There were very serious concerns about Bill C-51's deepening unfairness of the immigration security certificate process, for instance, withholding certain categories of evidence from special advocates.

● (0905)

There needs to be a significant rethinking and reconsideration of immigration security certificate proceedings, rolling back those changes that were made in Bill C-51, and addressing still the other areas of concern with respect to the fairness of that process.

Thank you.

The Chair: Thank you, Mr. Neve.

Ms. Damoff, you have seven minutes, please.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): I would like to welcome you both to our study of Bill C-59 and thank you for being here. I'm going to start with Amnesty International.

I'm just going to quote you. On your website, where you've written about Bill C-59, you say that you'd “also hoped that the government would act to address longstanding concerns about the failure to...reject torture in Canada’s intelligence sharing arrangements with other countries.” You've mentioned that here as well.

Ministerial directions were put in place in September, and those had obviously been a decade old since they had been updated. First of all, the ministerial directions prohibit sharing information if there is a reasonable ground to believe it could lead to torture. How did these improve on the previous directions, which I mentioned were decades old?

Mr. Alex Neve: Thank you very much for the question.

We did welcome the new directions that came after the earlier statement you're noting, which was our reaction to Bill C-59 when it was tabled in June.

Ms. Pam Damoff: Okay. Thank you for clarifying that.

Mr. Alex Neve: We did highlight that we think they are a very significant improvement over the previous directions, which were of serious concern. We have highlighted that they do not go far enough. It's hard to please advocates, especially when it comes to something as fundamental as human rights protection and protection against such a crucial human rights concern as the absolute prohibition on torture. We're still concerned that there are provisions in the directions that do allow for the possibility that intelligence could be used, even if it has been obtained through torture.

We have made recommendations for further reform, but do welcome the steps that have been taken.

The issue that I highlighted today is a separate but related concern about the fact that in our immigration legislation—so again, it's this broad concern about being complicit in torture—we still have these provisions that would allow individuals to be deported to a situation of torture in extreme circumstances. We do very much call for that to be addressed.

Ms. Pam Damoff: Thank you very much, and thank you for being with us again as well.

Dr. Carvin, I thank you for being here and for your testimony.

You had an article published yesterday in *The Globe and Mail*, along with our panellists who are appearing in the next hour. You had stated that:

> C-59 also builds up the powers of Communications Security Establishment....
>
> Even more critically, it finally tries to draw CSE into the constitutional tent by creating a unique independent approval system for its intelligence activities. We think there are some important amendments to be made in these areas....

I'm just wondering if you could highlight for us what amendments you would like to see in Bill C-59 to improve the oversight mechanisms of CSE?

Prof. Stephanie Carvin: Thank you very much for this question. That particular passage has been written by Craig Forcese, who will be speaking on that a lot.

● (0910)

Ms. Pam Damoff: Okay.

Prof. Stephanie Carvin: I think his entire presentation will actually be on that, so I don't want to pre-empt what he is going to say. Again, it just gets to section 8 of the charter, making sure that people are protected from an unreasonable search in CSE's operations. As to the specific legal details, I don't like to defer but I will in this particular case. Thank you.

Ms. Pam Damoff: That's fine, especially since they are here today. Thank you for that.

You've also called for better transparency for Canadians about what types of threats the government is presently facing. You referred to two models that the government could look at. I wonder if you could maybe explain for us what those two models are, and if you think that should be something that we legislate or if it could be done by regulation.

Prof. Stephanie Carvin: Thank you. This is an issue that I'm very passionate about. It's a great question.

One of the first examples out there is the worldwide threat assessment that's put out every year by the Office of the Director of National Intelligence. We used to call it the Clapper report. It will now be called Coats report.

What I would say is that every year they put out a 15- to 20-page threat assessment that lists what the priority threats are to Americans. It's a very useful report because it's indicative of where the security services are putting their resources and what the major concerns are. It also shows the shift over time. If you look at the reports over time, you can see that they've gone from putting al Qaeda—particularly al Qaeda in the Arabian peninsula—as the number one threat to now putting cyber as the number one threat.

It's interesting that we've seen that shift in the American national security landscape, and I think Canadians should know as well. Right now, the only way we really have of knowing these things is through the threat environment section in CSIS's annual report, but that's no longer an annual report. It now comes out every three years. Also, now it's not even really a report anymore. The last report was a YouTube video of the director sitting in front of a camera, and I don't think this is sufficient to explain what the national security threats are to Canadians.

First of all, I don't understand why that report is no longer an annual one. It absolutely should be an annual report. When I testified on Bill C-22, I said we needed to make sure that there are annual reports discussing what these threats are, along the lines of the worldwide threat assessment. I think that would be one area.

The other area that we have is the public report on the terrorist threat, which is again supposed to come out every year. I don't believe this year's report has come out yet; I'm not entirely sure why. That is the only inter-agency report we have on any threat to Canada, not just terrorism, and it's in just one area. We don't talk a lot about espionage and we don't talk a lot about cyber, and these are things Canadians need to know.

Ms. Pam Damoff: I only have 20 seconds left—

Prof. Stephanie Carvin: Sorry.

Ms. Pam Damoff: No, that's okay.

Did you say that it should be something that's legislated, or can it be done by regulation?

Prof. Stephanie Carvin: When I testified on Bill C-22, I suggested that it should be legislated and should be required every 365 days. I believe Canadians deserve that transparency.

The Chair: Thank you, Ms. Damoff.

[*Translation*]

Mr. Paul-Hus, you have seven minutes.

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

Hello, Ms. Carvin.

In your presentation, you said that Bill C-59 would change the powers of CSIS officers. It is often said that Bill C-51 gave CSIS too many powers. There have been many calls to change that, and I would like to better understand the reason for those requests. Since you worked for that organization, you are familiar with the field. I would like to know more about that.

Prof. Stephanie Carvin: Thank you for your question.

[*English*]

I will respond in English. Thank you.

I think one of the issues is that, without guidance, the security services do not know where to step. There is concern, for example, that with the broad scope of Bill C-51, knowing where the limits were was a challenge. One of the things that the service always worries about is another commission of inquiry. This is the number one thing you want to avoid because of the drain on manpower, resources, and these kinds of things. Without adequate oversight, without clear guidance as to where the lines are, the service becomes very scared about where it can actually proceed.

We've seen that, of course. Michel Coulombe and the new director have stated that they haven't really gone for the warranted powers in Bill C-51 that allow it to violate the charter, as far as I'm aware. You want powers that are clearly defined in law and that you know have the backing of the government and the backing of the courts, or else a kind of paralysis develops, in the sense that you don't want to do anything that could eventually end up with a commission of inquiry again. This is why I strongly support clearly defined disruption powers.

I believe disruption is important. One of the things I saw during my time was just the speed at which terrorism investigations sped up. They could go from being over two years to being a couple of weeks, when people saw the propaganda and would make the decision to leave.

These disruption powers are important, but I think grounding them in the charter and in interpretations of the law is absolutely vital to the actual operations of the agency.

● (0915)

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

In your statement, you also spoke a lot about the agencies' various review mechanisms or bodies. All we want in the end is to protect ourselves against various potential threats.

Do you think that once Bill C-59 is passed it will be effective in countering threats?

[*English*]

Prof. Stephanie Carvin: Yes, sir, I am. In particular, I am happy to see the cyber-powers of CSE legislated. Importantly, I think it signals to our allies that Canada is committed to a robust defence of, not only ourselves but also, for example, NATO operations and the Five Eyes agencies as well. These are things that we absolutely need. I think having these powers is important. Putting them on statutory footing, so that Canadians and our allies know that they are there, is going to make us more transparent but also a more reliable, dependable partner going forward.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

Mr. Neve, I think you also wanted to speak to my first question.

[*English*]

Mr. Alex Neve: In a very complementary way, I was going to highlight that we too absolutely agree that the need for a much more careful delineation of CSIS's powers, when it comes to threat reduction, is essential. That's why there is this need to enshrine a clear prohibition—and the line absolutely needs to be drawn—to make it clear that actions that will violate the Charter of Rights.... Very importantly, we would add that Canada's international human rights obligations, which are binding and which take our actions into a global context, play a very important role there.

[*Translation*]

Mr. Pierre Paul-Hus: I will continue on the topic of the charter.

One of our main concerns right now is balancing the powers, that is, finding a balance between what we can do and what the charter requires us to do to uphold the freedom of Canadians.

In terms of security and potential threats to Canadian citizens, to what extent should the charter be applied consistently and fully? Criminals don't care about the charter. Criminals and terrorists have no intention of respecting anything. For our part, we endeavour to uphold the charter as much as possible, while they couldn't care less about it.

In your opinion, is the charter the ultimate tool to which we should pay the greatest attention? What are your thoughts on that?

[*English*]

Mr. Alex Neve: It will probably not come as a surprise to hear from me that it should be protected in 100% of cases and we always add to that the surrounding context of Canada's binding international human rights obligations as well. In saying that, I think that it's very important to underscore that the human rights framework is, by no means, inattentive to security threats and other kinds of challenges that governments face in ensuring safety for their citizens.

In fact, the international human rights architecture is entirely based on a very clear understanding that governments do face those threats and then has specifically incorporated that into how human rights protection needs to be upheld, like some human rights international law, with freedom of expression being an obvious one. Therefore, in their very definition in international treaties, a balancing is incorporated. It's a very limited provision for restrictions or infringements, but it is there.

In international law, other rights are clearly recognized to be so absolutely important that no circumstance—torture is an obvious example here—ever justifies infringement, which recognizes that it's devastating from a human rights perspective. It is also counter-productive when it comes to security because allowing torture in the name of security only creates more marginalized community, keeps us more insecure, and leads to more terrorism.

● (0920)

[*Translation*]

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

Mr. Dubé, you have seven minutes.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

[*English*]

I'm going to try to get through all these points quickly because I only have the seven minutes.

Dr. Carvin, on the intelligence commissioner issue, I'm just wondering about the length of the term and whether five years is enough to have some kind of independence from the government apparatus. Given the fact that, potentially, they can be reappointed for a second term, would there not be incentive to have some kind of job security in that sense?

Prof. Stephanie Carvin: It's interesting, in that you want someone who is familiar enough with what's happening and doesn't lose touch, but you're right, there is that potential conflict. I think a lot of it is also going to depend on the people around the intelligence commissioner and the support staff they actually have.

The intelligence commissioner is going to have considerable responsibilities on review and oversight. I believe the advantage is going to be having someone who has recent experience and understands the context and things like that, but even more importantly, I think ensuring that the people around this individual are well staffed and well funded is going to make a difference.

Mr. Matthew Dubé: That's on the institutional memory side.

Prof. Stephanie Carvin: Yes.

Mr. Matthew Dubé: In terms of independence, does it cause potential conflicts by keeping the person as non-reliant on the executive branch as possible for their job security?

Prof. Stephanie Carvin: I have to believe that our judges are sufficiently pensioned such that this is probably not going to be that much of an issue. I'm going to refer to my friend Emmett Macfarlane, who has written considerably on the courts in Canada and has written passionately that the judges actually are independent. I'm going to base my expertise on him and the conclusions of his research.

Mr. Matthew Dubé: The other question was on the part-time nature of the work. Again, that probably connects to how they'll be staffed. Is there any potential issue, especially given that it's actual oversight and not review? Could it cause any problems to have it on a part-time basis?

Prof. Stephanie Carvin: I think we're going to have to wait and see how a lot of these things operate in practice. I would hope that this committee would keep an eye on that, to make sure that the problems you may be suggesting aren't going to manifest.

Mr. Matthew Dubé: Okay, great.

The last question is on the intelligence commissioner. Given that it's oversight and not review, there's obviously something novel in that, and that's important. I want to make sure I'm understanding correctly that we're looking more at general authorizations as opposed to specifics, in terms of the actions being carried out by different agencies. I want to make sure I'm understanding that right. They're not actually looking at a specific action being posed but rather at the reasonableness of a general direction that an agency might be going in. Am I understanding that correctly?

Prof. Stephanie Carvin: Right. I don't know if you've been referred to Craig Forcese, who will be on the next panel. He has developed a decision tree. It's actually more complicated than your daily Sudoku. He might be better placed to answer that question.

It's my understanding that, yes, it is general, but there are some very specific cases where the intelligence commissioner will have to make calls, in particular, in defence of critical infrastructure. This is where some of my concerns about ministerial oversight arise.

● (0925)

Mr. Matthew Dubé: Great. Thank you.

The next question is for both of you, moving to the national security and intelligence review agency. The complaints investigation function omits agencies like Global Affairs Canada, which obviously has a huge role to play.

From your perspective in particular, Mr. Neve, when it comes to our international human rights obligations, what importance does that have? Is keeping it to three agencies, with the fact that we're keeping an information-sharing regime in place, problematic?

Mr. Alex Neve: No. We would definitely support a more expansive reach for the agency. I think we know from past instances —I highlighted some of the cases at the beginning of my remarks— that involvement, responsibility, and even culpability certainly go beyond those operational agencies that may be doing the daily work around a case. In cases like Maher Arar, and in the cases that Justice Iacobucci examined in his inquiry, Global Affairs is certainly implicated as well. There needs to be some review of those decisions and actions.

Prof. Stephanie Carvin: I would largely support that. There is something I didn't talk about in my testimony—and I'm going to use this as a quick aside. One of the concerns I have is that DND is not excluded from this. If you look at all the different kinds of intelligence that will be going to this review agency, one of the concerns I have is that the way intelligence is used at CSIS versus at the Department of National Defence is extremely different, particularly because the Department of National Defence actually has the legally authority to kill people.

When the review agency is looking at all the different agencies, they're going to have to develop the expertise in how intelligence is used in each agency. DND has never been through this process before. They've never had their intelligence reviewed before, so this is going to be some serious learning for DND. As well, one of the important things for the NSIRA is that it will actually have to learn to differentiate the different ways intelligence is used by different government departments in Canada. That is a concern I have going forward.

Mr. Matthew Dubé: Thank you very much.

There is one last question I wanted to ask. You talked about the importance of having legal grounds for the operations that CSE does. There are different parts that I've been looking at. I don't have enough time to get into some of those details, but there is one I was asking them about with proposed section 24, about testing and studying information infrastructure. There's also proposed section 28, which is about the minister authorizing cybersecurity—essentially, authorization to protect federal infrastructure and non-federal infrastructure.

Could the bill benefit from more clarity as to what exactly CSE can be doing in those particular contexts?

The Chair: Answer very briefly, please.

Prof. Stephanie Carvin: Very briefly, I would say I am happy for the intelligence commissioner to have a good review and oversight discretion, particularly with the defence of critical infrastructure, because that is a very vague concept and our idea of what it is actually changes over time.

With regard to proposed section 24, I'm going to leave that to Craig Forcese, given the time.

The Chair: Thank you, Mr. Dubé.

Mr. Erskine-Smith, welcome to the committee.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much.

Thank you to you both for your testimony.

Ms. Carvin, you mentioned that in the total architecture of review you still had some concerns about efficacy. You mentioned Professor Forcese a few times. In a paper that he and Kent Roach wrote they talk about this three-legged stool and there is a parliamentarian committee on efficacy, there's a super-SIRC for propriety review, and then they talk about an independent monitor of national security law built on the U.K. and Australian model.

When we look at Bill C-59 and Bill C-22 together, do you see that largely meeting the overall review architecture?

Prof. Stephanie Carvin: That's a very interesting point.

When I testified on Bill C-22 I suggested that much of the focus of that committee should be on efficacy. One of the issues we have is that it's not really clearly defined yet what the differences are between what NSIRA and NSICOP are going to be doing, and that's a concern not just for myself but also other people who formerly worked in this area. You don't want them both going after the same thing.

It should be clear that the Bill C-22 committee should probably be taking a 60,000-foot view of what's happening and let the NSIRA get into the legal weeds. What I'm concerned with is that there is no division of labour, but where I think the efficacy review should be taking place is probably in the Bill C-22 committee.

● (0930)

Mr. Nathaniel Erskine-Smith: I would agree. That makes sense, which would suggest that maybe we don't have a gap in efficacy review with Bill C-22 on the table.

In any event, the new super-SIRC committee and the new commissioner don't have the exact same powers in replacing SIRC and replacing the current CSE commissioner. I have a note here, for example, that the CSE commissioner has certain authorizations under the Inquiries Act that the new commissioner would not have, that the reporting requirements for SIRC are more stringent in some cases, including the number of warrants that have been authorized for CSIS.

When we roll CSIS into this super-SIRC, when you roll CSE into the new commissioner role, shouldn't they have the same reporting requirements and the same powers? If not, why not?

Prof. Stephanie Carvin: I didn't see those limitations in the legislation when I read them as perhaps you put it. It seems to me that the NSIRA actually has an extremely broad mandate and that is a very good thing because they should be able to have that authority.

I know that Wesley Wark, who will be speaking today, is an authority on review. I would encourage you to ask that question to him as well, but in my understanding, I did not see that limitation necessarily in the—

Mr. Nathaniel Erskine-Smith: I put it to both of you, the expectation ought to be that the same powers and authorities should be granted to the new super-SIRC committee and the new commissioner. Is that fair?

Prof. Stephanie Carvin: I would say that's the case, and if you believe that's not the case, I would try to make sure that it is to your satisfaction.

Mr. Nathaniel Erskine-Smith: Mr. Neve.

Mr. Alex Neve: We would totally agree with that. One of the problems we've seen in the past has been the unevenness of the powers and mandate of various review bodies. That leads to confusion and it certainly means that the ability to coordinate review across agencies, which is, of course, one of the things we're really looking for in this new approach, gets hampered.

Mr. Nathaniel Erskine-Smith: Mr. Neve, you had raised some concerns about the Secure Air Travel Act, about the failure of a "robust redress mechanism". I think those were your words. Special advocates in other contexts have been a useful solution and they were recommended by this committee. I'll start with you, but put it to both of you. Do you think a special advocate system, which is missing in this legislation, would be a useful fix for the Secure Air Travel Act?

Mr. Alex Neve: It would be a useful contribution, but it would not be the fix. There's so much more beyond it that is needed, but it is of concern and we, and others, have certainly highlighted that it's peculiar to us actually that here we have an area where once again there are concerns about secrecy and withholding of evidence and there is a mechanism that exists and it's not being used at all. But it needs to go much further than that in ensuring the proper robust redress system we need is developed.

Prof. Stephanie Carvin: I would defer to Alex's comments.

Mr. Nathaniel Erskine-Smith: Okay.

We rename SCISA to SCIDA. There are a few other changes, though. I sit on the privacy committee and we had a more fulsome report on that specific point of information sharing. The government did provide a response and there are some changes, more substantive changes beyond a title change, in the new SCIDA. One is the definition. I don't know if either of you have comments on the new definition and whether it's sufficient to meet the concerns that were raised in the course of the national security review.

Mr. Alex Neve: Do you mean the new definition of threats to security?

Mr. Nathaniel Erskine-Smith: That's correct.

Mr. Alex Neve: No, we're still concerned. We think it is still overly broad and it stands in contrast to definitions that are used in the CSIS Act, for instance. There is a number of ways in which that definition and how it interplays with other provisions leaves open the possibility that people will be subject to information-sharing processes simply because they've been involved in protest and advocacy in a context where it perhaps connects up with opposition to critical infrastructure like pipelines, etc. That area of concern, which was of course a very serious problem in Bill C-51, in our view, has not been wholly addressed.

Mr. Nathaniel Erskine-Smith: There is an amendment that "significant or widespread" has been added in relation to undermining core infrastructure and other things. That hopefully gets away from certain protests.

There are a couple of other changes. There's a debate about the disclosure threshold of relevance versus necessity. Certainly this committee and the ethics committee recommended a necessity threshold in accordance with the Privacy Commissioner. We don't see that in this bill, but we do see an increase, I think, from relevance to "contribute to the exercise of the recipient institution".

Is that adequate in your view, Ms. Carvin or Mr. Neve?

● (0935)

The Chair: You'll have to answer very briefly again, unfortunately.

Prof. Stephanie Carvin: I have a general comment. Do you have something specific?

Mr. Alex Neve: Obviously we would always support the stronger protections from a human rights perspective.

Mr. Nathaniel Erskine-Smith: Better, but not as good as you might—

Mr. Alex Neve: Exactly. "Necessity" offers better protection.

The Chair: Thank you, Mr. Erskine-Smith.

Mr. Motz, you have five minutes.

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

Thank you to both of you for being here today.

I'm going to focus on you for a couple of minutes, Dr. Carvin, if I could. Specifically, your past as a strategic analyst with CSIS intrigues me a bit. As you know, there are several oversight groups created or adjusted in the new bill. What pitfalls might you see in effectively communicating intelligence and threats with the new structure?

Prof. Stephanie Carvin: Are you referring to the SCISA-SCIDA changes?

Mr. Glen Motz: Yes.

Prof. Stephanie Carvin: If anything, I actually thought the definition was probably widened in the current legislation as it stands. There was actually a limitation in C-51. I know I keep referring to Craig, but we podcast a lot, so we're kind of melding into one. First it was the chapeau piece, and that actually was taken away, so if anything, actually the ability to share information is technically broader under this legislation, which I think some people have concerns with.

But I agree that we absolutely, fundamentally have to protect information sharing, so if reforms are made, we have to bear this in mind. It's not just important for terrorism. Usually the classic example of passports is used—trying to stop someone with a passport from leaving the country—but also the Investment Canada Act, the ability to share information under that, is absolutely essential to our national security.

As it stands, I don't see major changes in this bill, but if reforms are coming from this committee, I think that should be kept in mind.

Mr. Glen Motz: Thank you.

Again from your experience, how do you think the front-line security staff would respond to and see the changes we just talked about?

Prof. Stephanie Carvin: My view is that they actually want clear guidelines. They want to know where they can step and where they can't step. The reason is that they want cover in a sense that they want to know that where they're actually operating is in the correct legal area. Providing them that, which I believe this legislation does, while of course leaving important things like datasets up to more review in oversight rather than a specific legislated guidance, is the correct approach to take.

Mr. Glen Motz: Okay.

You spoke in your statements at the front end about the security reports, the documents, the threat analysis, and threat assessments that have been done. Can you give us some pros and cons of the current threat analysis documents and how experts in the community can make use of them differently with C-59?

Prof. Stephanie Carvin: Do you mean the public reports?

Mr. Glen Motz: Yes.

Prof. Stephanie Carvin: In some ways I think what we're going to learn from these reports is how these powers are being used, how often they're being used, and whether our security services are having difficulty complying with the law. What they're not going to necessarily reveal is what the threats are that these powers are being used against.

People are worried about foreign fighters. We've seen that in the last month's coverage of the foreign fighter issue and I can understand why Canadians are concerned. However, at the end of the day, if we communicated these threats better, in a more reasonable manner, and provided a separate threat assessment or a more robust threat assessment by the national security community, I think that would go some way to help.

Where the transparency is going to be valuable, for someone such as me who is trying to know, is where you can see, for example, whether these powers are being used more or being used less, why they are being used more, whether there an increasing threat, and so on.

Mr. Glen Motz: That's from a public document perspective.

As you know from your life, and for my colleague Mr. Picard and me, information sharing is absolutely critical to any type of national security and sharing of information. Do the new changes in this act provide for front-line people what they require to do their jobs, rather than the siloing that has occurred and can occur? Is the information sharing going to be effective with this new legislation?

● (0940)

Prof. Stephanie Carvin: Again, I don't see any overly broad restrictions here in terms of sharing information in the legislation. As I noted earlier, if anything, it's actually in a lot of ways wider than the previous legislation, so I believe that won't be a problem.

In terms of how the guidance is translated if the legislation as written is passed, a lot of this will depend on their managers and how this is specifically done, but that will be seen in the review process.

The Chair: Thank you, Mr. Motz.

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

Mr. Michel Picard (Montarville, Lib.): I'll go to French, if you don't mind.

[*Translation*]

My first question is for Mr. Neve.

You raised the issue of torture. In this regard, our security agencies all do the same job with the same objective, regardless of the government in power: they must verify the information obtained and make sure it is not the result of torture in another country. How can we protect the good faith of our agencies in this process?

[*English*]

Mr. Alex Neve: It can be a tough question, but there are processes, mechanisms, and expertise that can be drawn on to make those assessments. It obviously involves careful analysis of law enforcement and security practices in the country from which the information is being received, both in a general sense and in a specific context. There is no perfect equation or process through which information can be filtered and a clear and conclusive determination made that it has or has not been the result of torture. That's why there's a threshold here. What we're looking for is whether there is a serious reason to believe it has been attained through torture.

[*Translation*]

Mr. Michel Picard: If the information was obtained through torture in another country, it is very likely that we will learn that after the fact, not before. That is rarely indicated on the report providing the information.

How should we manage that information, considering that we unfortunately did not learn until after the fact that the information was contrary to its own values?

[*English*]

Mr. Alex Neve: If there are serious reasons to believe it has been obtained through torture, and even more so, if conclusively it has been possible to determine that it has been obtained through torture, then in our view it should be disregarded and not used in security and intelligence practices.

[*Translation*]

Mr. Michel Picard: That is true, provided that we have not taken action yet. That said, we rarely have three or four weeks to react to information, especially if the threat is imminent. Action must be taken fairly urgently if the lives of Canadians are at risk. I am referring to cases in which, unfortunately, we learn after the fact that the information was tainted.

[*English*]

Mr. Alex Neve: We would propose that other means of investigation be used, not relying on torture-tainted information.

Number one, relying on torture-tainted information only encourages more torture, both in the short term and in the long term. It is sending a message to torturers that there is a market for the fruits of their crimes, and we want to counter that. We want to break that cycle.

Second, we also have to remember the reality that torture-tainted information is very often unreliable. You will hear it very powerfully —not just from human rights experts, but more so from law enforcement and security experts—that relying on torture-tainted information excessively can be distracting and can take agents away from the real lines of investigation that will give rise to strong intelligence.

[*Translation*]

Mr. Michel Picard: Rest assured that I completely agree with the principle you have just stated. Yet we also have to look at the practical application. In practice, the texts are not always adaptable.

Ms. Carvin, you said there are more reports and that there is a need for transparency. How does it help people to inform them of the current level of security or danger? I am not referring to security professionals and legislators, but to people who work in a store, a restaurant, a factory, and so forth.

● (0945)

[*English*]

Prof. Stephanie Carvin: Thank you for your question.

Again, I would refer you to the worldwide threat assessment. It is a 10- to 15-page report written in very basic language that provides guidance as to the priorities and concerns of the U.S. national intelligence committee. It's there for anyone to read, and I think Canadians would benefit. Certainly someone like me, who teaches threats to critical infrastructure, would certainly be using any kind of document like that in teaching. I am sure I'm not alone.

There are a lot of university campuses now that are teaching terrorism and national security. We need to educate students about the kinds of threats they will be working on if they choose to go into a law enforcement career or a national security career.

The Chair: Thank you, Mr. Picard.

On behalf of the committee, I want to thank Mr. Neve and Professor Carvin for their contributions to our deliberations. We appreciate the very thoughtful presentations.

With that, we'll suspend for a couple of minutes and then re-empanel.

● (0945)

(Pause)

● (0950)

The Chair: Let's get started again.

We have with us two witnesses, Professor Forcese and Professor Wark.

I don't know whether you two have decided who goes in what order. Maybe you should play rock, paper, scissors. The alternative is to go with seniority. I'll leave it to the two of you to sort that out.

Professor Craig Forcese (Professor, Faculty of Law, University of Ottawa, As an Individual): Wesley has pointed at me, so I will go first.

I wish to extend my sincere thanks to the committee for inviting me here to speak on Bill C-59. It's always an honour to be asked to share my observations before this committee.

My colleague Kent Roach is appearing before you next week. He and I have divided up Bill C-59. Today I shall be addressing the new Communications Security Establishment act and the amendments to the CSIS Act.

I support most of the changes Bill C-59 makes in these areas. I recognize the policy objectives they seek to address. I believe the statutory language is usually carefully considered and robust, but I do have one serious concern.

I'll begin with the CSE act and make my single recommendation for today. I respectfully submit that this committee should amend proposed subsections 23(3) and 23(4) to indicate CSE may not, without ministerial authorization, contravene the reasonable expectation of privacy of any Canadian or person in Canada. Those two provisions are found on page 62 of the PDF of the bill.

I have provided a brief to this committee describing the rationale for this change, and I should disclose I've been an affiant in the current constitutional lawsuit brought by the British Columbia Civil Liberties Association challenging CSE activities, but today I appear on my own behalf.

To summarize my concern, while engaged in foreign intelligence in cybersecurity activities, CSE incidentally collects information in which Canadians or persons in Canada have a reasonable expectation of privacy. This is done without advance authorization by an independent judicial officer, and thus likely violates section 8 of the charter.

Bill C-59 attempts to cure this constitutional issue through a ministerial authorization process, one that involves vetting for reasonableness by an intelligence commissioner, a retired superior court judge. This is a creative and novel solution. It preserves a considerable swath of ministerial discretion and responsibility. It is not a full warrant system. Still, given the unique nature of CSE activities, I believe it is constitutionally defensible.

The new system will only resolve the constitutional problem if it steers all collection activities implicating constitutionally protected information into the new authorization process. The problem is this. Bill C-59's present drafting only triggers this authorization process where an act of Parliament would otherwise be contravened. This is a constitutionally under-inclusive trigger.

Some collection of information in which a Canadian has a constitutional interest does not violate an act of Parliament, for example, some sorts of metadata. The solution is simple. Expand the trigger to read as follows: “Activities carried out by the Establishment in furtherance of the foreign intelligence” or cybersecurity “aspect of its mandate must not contravene any other act of Parliament or involve the acquisition of information in which a Canadian or person in Canada has a reasonable expectation of privacy”, unless they are authorized under one of these ministerial authorizations that are subject to vetting by the intelligence commissioner.

This may seem a lawyerly tweak, but if we fail to cure the existing problem with CSE's collection authorization process, a court may ultimately determine that CSE has been collecting massive quantities of data in violation of the Constitution. Such a finding would decimate relations with civil society actors, placing CSE squarely in the crosshairs of a renewed controversy, and making it very difficult for private sector enterprises to partner with CSE on cybersecurity without risking reputational fallout themselves. With Bill C-59, we have a chance to minimize this kind of problem.

I turn to the CSIS Act changes. Bill C-59 does three things. First, it permits CSIS new authority to collect and potentially retain so-called datasets. Here the tension lies in balancing the operational need for CSIS to be able to query and exploit information against the privacy imperative. Rather than prescribe hard standards for what may be included in datasets, Bill C-59 opts for a system of in-advance oversight.

● (0955)

The intelligence commissioner is charged with approving the classes of Canadian datasets that the minister has deemed may be initially collected, and the Federal Court authorizes any subsequent retention of actual datasets. While I am wary of the idea of datasets, I cannot dispute the rationale for them and I can find no fault with the system of checks and balances. I have one concern with the retention of information that's queried in exigent circumstances. I don't know that the bill has the same checks and balances there, but I'm happy to address that further in questions.

The second change to the CSIS Act relates to revisions to CSIS's threat-reduction powers introduced in Bill C-51 in 2015. These provisions were rightly controversial. For our part, Kent Roach and I did not dispute the idea of threat reduction, but we worried that CSIS threat reduction done as a continuation of our awkward, siloed police and intelligence operations runs the risk of derailing later criminal investigations and prosecutions. This would be tragic from a security perspective.

From a rights perspective, Bill C-51 lacked nuance. It opened the door to a violation of any charter right subject to an unappealable, secret Federal Court warrant. The regime was radical, and in my view, almost certainly unconstitutional. It was, therefore, unworkable, whatever the strength of the policy objectives that propelled it.

Bill C-59 places the system on a much more credible constitutional foundation. It ratchets tighter the outer limit on CSIS threat reduction powers. By barring detention—a power I sincerely doubt the service ever wished—it eliminates concerns about the many charter violations for which detention is a necessary predicate. By legislating a closed list of activities that could be done where a warrant is authorized, Parliament tells us what charter interests are plausibly in play—essentially, free speech and mobility rights. I believe that if threat reduction is to be retained, this new system reasonably reconciles policy and constitutional issues.

Lastly, Bill C-59's CSIS Act changes create new immunities for CSIS officers and sources engaged in intelligence functions that may violate law during those activities. The breadth of Canada's terrorism offences makes it certain that a confidential source or undercover officer will commit a terrorism offence simply by participating with the terror group that they infiltrate. An immunity is necessary. The issue is whether there are sufficient checks and balances guarding against abuse of this immunity. Again, I think Bill C-59 does a good job of festooning the immunity provisions with such checks.

I will end, though, with a caution. Our conventional manner of siloed police and CSIS parallel investigations lags best practices in other jurisdictions that employ more blended investigations. As the Air India bombing inquiry observed, we struggle with what is known as intelligence to evidence. The government is working on this matter. We should be conscious, however, that what CSIS does in its investigations, whether in terms of immunized criminal conduct in intelligence investigations or authorized threat reduction, could derail prosecutions if not done with a close eye to downstream impacts. This issue might usefully be a topic of inquiry for the new security and intelligence committee of parliamentarians.

Thank you for your attention. I look forward to any questions.

● (1000)

The Chair: Thank you, Professor Forcese.

Professor Wark.

Professor Wesley Wark (Professor, Graduate School of Public and International Affairs, University of Ottawa, As an Individual): Mr. Chair and members of the committee, I thank you for this opportunity to testify on Bill C-59, the national security framework legislation.

I'd like to begin with a look backwards. I had the privilege 16 years ago of testifying before a House committee on the original Anti-terrorism Act. I think it might have been, in fact, in this beautiful room. One of the lessons I drew from that experience was that Parliament, if given the chance, could have a significant impact on improving draft legislation and on enabling a strong, if inevitably contentious, public debate. Given the professed openness of the Minister of Public Safety to constructive suggestions, I am optimistic that a similar result will occur from deliberations on Bill C-59.

Bill C-59 represents a very ambitious and sweeping effort to modernize the Canadian national security framework. It should not be seen as just a form of tinkering with the previous government's Bill C-51. There are so many elements in Bill C-59, and as you will have appreciated from testimony by my colleagues, I, like them, am going to focus on only a few elements of this.

The ones I want to focus on are what I call the key forward-looking elements of Bill C-59. By “forward-looking” I mean the genuinely new elements in this legislation, which pose particular challenges for a committee like this in terms of trying to understand their precise potential impact and efficacy. Those three brand new elements, I think, are particularly visible in parts 1 to 3 of the legislation, so that's what I am going to concentrate on, but I'd be happy to take questions on other aspects of the bill.

Part 1 of the act creates a national security and intelligence review agency. I fully support this concept and its rationale, and it is exciting to me to see it embraced by the government. The challenge will be ensuring that the architecture can be made to work. To bring the legislation to light, it will be important to ensure that NSIRA, as I'll call it, has the right fiscal and logistic resources, a high-quality talent pool in its secretariat, excellent working relationships with the security and intelligence agencies, and a viable work plan. It will also be important to ensure that the bodies that are to be reviewed have the resources and proper approach to the enhanced scrutiny they will undergo.

NSIRA part 1 needs, in my view, a few fixes. One has to do with the mandate, in proposed section 8. I believe that the national security and intelligence activities of the RCMP should be specifically listed at proposed paragraph 8(1)(a). It is important to be clear in the legislation that NSIRA will take over some of the current review activities of the Civilian Review and Complaints Commission for the RCMP as it is doing for SIRC and for the Office of the CSE Commissioner. This should not be left simply to coordinating amendments buried in the back of the legislation.

The committee will also note that NSIRA enacts only a partial solution to the problem of dealing with national security complaints, at proposed section 16 and following. Its complaints remit is restricted to CSIS, CSE, and complaints regarding the RCMP that have a nexus in national security, and I would urge the committee to hear from the commissioner of the Civilian Review and Complaints Commission for the RCMP about how well they think the legislation enables the NSIRA complaints mandate when it comes to the RCMP.

Finally, there's an important issue of membership, as you've already heard, in NSIRA. This is at proposed section 4 of the bill. The procedures proposed are, disappointingly to me, an automatic carry-over from SIRC, but SIRC membership has had a sometimes deeply troubled history. Membership size and profile need, I think, to be rethought. In my view, the SIRC membership should be enlarged to allow for more diverse and expert representation and to reduce the burdens on members hearing complaints.

NSIRA membership should also reflect, in my view, a wider range of expertise in security and intelligence issues, including expertise in security threats, on intelligence practices, on international relations, on governance and decision-making, on civil liberties, on community impacts, and on privacy. Those are seven sets of expertise right there.

The ability of NSIRA to get up and running once legislation is passed will be vitally dependent on the continued strength, capacity, and forward planning of the Security Intelligence Review Committee, which will be NSIRA's core. It would be very unfortunate if anything occurred to weaken SIRC in the transition.

Part 2 of the bill is on the intelligence commissioner. Legislation to establish an intelligence commissioner to engage in proactive oversight of aspects of the work of CSE and CSIS is a novel concept that has no counterpart that I'm aware of among our Five Eyes partners. We are being truly innovative here. The concept that's been adopted, I believe, is a made-in-Canada solution to ensuring the legality and charter compliance of some of the most sensitive and important operations conducted by our main intelligence collection agencies, CSE and CSIS.

● (1005)

With regard to the function of the intelligence commissioner, I would like to offer two thoughts and one recommendation.

One thought is that it would be important that the system is and is seen to be a way of ultimately strengthening rather than diluting ministerial accountability, even while it gives some oversight powers to the intelligence commissioner. The second thought is that the ability of the minister to retain traditional powers of accountability while ceding some decision-making authority to the intelligence commissioner is linked in turn to the working of new reporting mechanisms proposed in part 1 of the act.

NSIRA will produce a much stronger stream of reporting to the minister on the activities of the key intelligence agencies, which, if that stream of reporting can be properly digested by the minister and his office, should ensure that the minister can issue authorizations that will pass muster with the intelligence commissioner. In this way part 1 and part 2 of Bill C-59 are intimately linked.

The recommendation I have to offer is that the intelligence commissioner function must not go dark. The Office of the CSE Commissioner, on which the function will partly be based, produced an annual report to the minister that was tabled in Parliament. This has been the practice since the commissioner's office was established in 1996. There is no such requirement at present for the intelligence commissioner. I believe the intelligence commissioner should be required to table an annual report that would review the commissioner's activities and findings.

Then there is part 3, the CSE act. I fully support the importance of creating separate, modernized legislation for CSE, distinct from the National Defence Act. CSE is one of Canada's most important, if not the most important, intelligence collection agency. It provides our principal contribution to the Five Eyes intelligence partnership. Getting the CSE act right is vital to Canada's interests and deserves close attention by the committee.

CSE received its first enabling legislation with the passage of the Anti-terrorism Act back in 2001. It is that legislation that is being modernized with Bill C-59. There were no changes to CSE legislation proposed in the previous Bill C-51.

The CSE act expands the current three-part mandate of CSE by adding two additional powers for what are called active cyber-operations and defensive cyber-operations. Let there be no mistaking that these are major new powers for CSE.

Both kinds of operations require ministerial authorization. Active cyber-operations engaging overseas targets require the consent of the Minister of Foreign Affairs. There have been some concerns raised in Parliament about the need for such consent. I think it is absolutely essential, given the volatile nature of such operations and their potential for blowback against Canadian international interests.

Active cyber-operations are what I call a digital form of covert operations, somewhat akin to classical Cold War covert operations designed to destabilize the capacities of a foreign adversary. In addition to blowback effects, they can also engage an escalatory spiral, as we saw, for example, in the aftermath of the cyber-operation known as Stuxnet, which targeted the Iranian centrifuge cascade that was central to their uranium enrichment program and nuclear weapons development. Active cyber-operations require high degrees of intelligence knowledge and technical skills, but they also require high degrees of political oversight and strong agency command and control.

It is also important to understand that many, if not all, of the operations that CSE might conduct in the future under its active cyber-operations mandate will be mounted within a Five Eyes context. I don't think we're going to be going it alone on these ones. This is all the more reason for there to be what has been called "a dual-key approach". Neither active nor defensive cyber-operations require the consent of the intelligence commissioner, which is something the committee might want to look into, but such operations will be subject to review by the new national security and intelligence review agency.

The CSE act is a very complex piece of legislation. It might be a lawyer's dream, but it would be a layman's nightmare to read. It contains some very important provisions that are sprinkled throughout the bill with little connecting narrative thread. My recommendation with regard to part 3 is that there should be a values principle built into the legislation, perhaps at the proposed mandate section, to draw together some of these different component parts, and I will provide a brief on that.

I was going to add a brief set of remarks about what isn't in the legislation, but I'm happy to address that in questions.

Thank you.

● (1010)

The Chair: Thank you, Professor Wark.

I don't know whether you or I should be more depressed. I think I was in this room 16 years ago as well on the justice committee sitting right there listening to your presentation.

Ms. Dabrusin, you have seven minutes, please.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): Thank you to both of you. There's a lot to cover, and you've done a really great job of bringing us across a whole lot of this.

The first thing I was going to ask was actually a slight homework piece.

Professor Forcese, I saw that you had drafted some flow charts about decision-making. I was wondering if you would be able to provide copies of that to the clerk for the committee to be able to use.

Prof. Craig Forcese: Sure, absolutely, although I fear the translator may be driven mad by the effort to turn my microprint into French.

Ms. Julie Dabrusin: No, that's great. Thank you.

First, this is quite lengthy legislation that we've been discussing. One question that comes to me when I speak to people in my community—and we do have a private member's bill in the House that's proposing it right now—is to just repeal Bill C-51 and leave us where we were pre-Bill C-51. On that broad question, if I can ask either one of you, why not just repeal Bill C-51 and leave us where we were?

Prof. Craig Forcese: My response would be that, certainly from my perspective, Kent Roach and I did not dispute the policy objectives that Bill C-51 was trying to accomplish, with one exception, and that is the new speech crime. We thought it was unnecessary. If one were to repeal those provisions that Bill C-51 introduced, one would be left still with the policy issues that would have to be addressed. I see Bill C-59 is dealing with those same policy issues but putting each of the powers on a more sustainable footing.

I would agree with what my colleague Professor Carvin said earlier, that not only is this just a question of constitutional niceties. It's also a question of certainty. Many of the powers that were introduced by Bill C-51 were clothed with such vagueness that the services might be disinclined to try to test them for fear they would run afoul of a court or a commission of inquiry subsequently.

Again, the policy objectives were real. The drafting, in my view, was insufficient.

Prof. Wesley Wark: Just briefly, I would say something very similar but expressed slightly differently, which is that in my view, Bill C-51 had good elements and bad elements. I think that was also the Liberal Party's position, frankly, when it was the third party in opposition, that there were some elements they could support and some elements that they were committed to overturning, if they ever came into office.

Bill C-59 represents some effort to fix the so-called problematic elements of Bill C-51, but it also provides space to add what I think are important new dimensions that were not addressed in Bill C-51. I would think it would be a time-wasting exercise, frankly, to go back and just repeal and simply eliminate all of Bill C-51 from the law books. Better is the approach that's been taken here.

Ms. Julie Dabrusin: Thank you.

Professor Forcese, when you were talking about datasets, I had a couple of questions. First of all, do you find that the definition for "dataset" in part 4 is sufficient?

Prof. Craig Forcese: Datasets are not robustly defined, so the definition of "dataset" is fairly open-ended. It's an electronic record characterized by a common subject manner, without further resolution as to what that means. Left with a vague definition, I turn instantly to what checks would exist to rein in an egregious, overbroad understanding of what a dataset might be, as compared, say, to the Security of Canada Information Sharing Act, where I agree with what was said before: that concept is overbroad as well.

Here this overbreadth is controlled by in-advance authorizations by independent individuals: the intelligence commissioner in relation to authorizing classes for purposes of initial acquisition; scrutiny then by a limited, designated employee, for purposes of then approving, at least for Canadian datasets; retention of that dataset by a Federal Court judge, who is entitled to superimpose requirements on how it can subsequently be queried and exploited. The definition is broad, but there's a dynamic means of limiting its scope so that there are individuals independent of government who can look over the shoulder of the service and make sure it has not run amok.

● (1015)

Ms. Julie Dabrusin: Professor Wark, did you have something on that?

Prof. Wesley Wark: Sure, just very briefly. I would say, just in a slightly broader context, that the world of intelligence collection and national security protections that we live in now is one that absolutely requires intelligence agencies around the world to engage in the collection of datasets. I think it's better to have this presented to the public in legislation as an acknowledged fact of life in the intelligence world. The challenge is how to control the use of datasets, which mostly consist of metadata.

From my perspective, the legislation does not do a bad job in that regard. The biggest concern I have about it is that the legislation would like to draw distinctions between foreign datasets and Canadian datasets, and surround each of them with different legal protections. I understand that in theory. In practice—and I've raised this with CSIS and CSE officials—I'm not sure how that's going to be done because we're talking about a much more blended pool of information.

I would encourage the committee to hear some more precise testimony from officials involved in thinking through the dataset problem, as to whether you can really distinguish between these two things. If you can't, the legal surround that we're trying to provide for it doesn't make a whole lot of sense.

Ms. Julie Dabrusin: I only have a minute and a half so I wanted to jump to the retention issues you raised and concerns with datasets.

Can you outline those briefly, please?

Prof. Craig Forcese: My single concern really relates to the circumstances in which the director of CSIS can authorize a query of a dataset that hasn't gone through the regular retention process involving the Federal Court, for instance. There's no indication in the statute as to what the service can then do with the product of that query. For regular queries there are rules about retention and in what circumstance they can be retained. For exigent queries those rules are not there so I'm not sure whether this is a glitch in the drafting or whether this is intended. It seems to me it would be very easy to pull the results of those queries into the regular retention regime but at present I don't see how it does so.

Ms. Julie Dabrusin: Do you have any suggestions, in 30 seconds, as to how we would word that, if we would word that?

Prof. Craig Forcese: Off the top of my head I would just make it clear that the results of queries done in exigent circumstances under proposed section 11.22 should be tied into the rules on retention that you find in proposed section 11.21. Obviously, that's going to require some tinkering.

Ms. Julie Dabrusin: Thank you.

The Chair: Thank you, Ms. Dabrusin.

[*Translation*]

Mr. Paul-Hus, you have seven minutes.

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

In her remarks, my colleague Ms. Dabrusin drew a comparison between Bill C-51 and Bill C-59. That is important for the committee. It is my understanding that Bill C-51 was enacted in response to an emergency at that time. It was very important for national security. Today, Bill C-59 is simply a refined version of Bill C-51. The latter was useful when it was adopted, but we want to clarify certain things.

Is that also your understanding?

[*English*]

Prof. Craig Forcese: I wasn't party to the drafting of Bill C-51 so I can't comment on the circumstances that drove its manner of drafting. Certainly, Bill C-51 opened the door to the service doing threat reduction of any sort, which before was a disputed issue. We know from what the director has said approximately 30 times now that, I believe, the service is engaged in threat reduction, albeit never crossing the line to threat reduction that might violate a Canadian law or transgress a charter right. Bill C-59 opens the door to a more assertive use of threat reduction where it could violate a Canadian law, which would require a warrant, but sets up a warrant system that I think would survive an inevitable Constitutional challenge. It broadens the ambit of useful powers for the service.

I can give you an example where this may come up. In the course of an investigation, the service is engaged in an intelligence investigation, and it decides for a public safety reason it needs to swap out an explosive materiel in the possession of a target with an inert material so that it no longer poses a security risk as the service continues its security intelligence operation. Now it's possible for the service to get with warrant authorization to do threat reduction to break and enter for the purpose of swapping out that material, and Bill C-59 makes it more likely that confronted with that request the court would think this regime was plausible.

● (1020)

[*Translation*]

Mr. Pierre Paul-Hus: Okay, thank you.

We have not talked about it this morning, but you spoke recently about the no-fly list and the problem of false positives. I would like you to elaborate on that.

[*English*]

Prof. Wesley Wark: There are a couple of things.

One is that false positives are a regrettable reality, I suppose, of any list of this kind, whether it's a Canadian list or a list composed by our allies. An effort has to be made to try to ensure that the number of false positives are as small as possible and if false positives do emerge it's a recourse mechanism.

As you'll be aware, the government is working on regulation and technical practices that would allow the government to control the SATA, the Secure Air Travel Act list, rather than it being in the hands of airlines to determine who should board or not board, in consultation with the government. It would be a centralized function. I think that's a very necessary reform. Government officials have testified before this committee that it's going to be a complex reform and it's going to take some time. It's certainly worth pressing the government to make sure that this key measure takes place. As it takes place, it will make the government responsible for false positives rather than a murky responsibility shared between airlines and the government itself and they will be better placed to try to address it. They're engaged in temporary measures of redress, which may or may not be satisfactory, but the overall solution, I think, will have to come with that centralized mechanism and the funding for it.

Prof. Craig Forcese: There are two sorts of false positives. There's the false positive that stems from when the person has the same name as someone who's on the list, and that's the discussion we've been having as of late. That's where a redress system—"I'm not really that person"—is effective. There are also false positives in the sense of a person who is the person the government has targeted, but who feels they've been wrongfully listed. At that point, there's an appeal process, but the appeal process is done in a secret environment where there's no special advocate. One of the recommendations is to have a special advocate who can provide an adversarial challenge in that appeal process.

[*Translation*]

Mr. Pierre Paul-Hus: Will Bill C-59 help solve the problem of false positives? That is mentioned in the bill. In your opinion, will the provisions of the bill be enough to solve this problem?

[*English*]

Prof. Wesley Wark: Not completely, Monsieur Paul-Hus, and I think perhaps the government would recognize that. It's creating a different circumstance in which the minister has to respond to appeals for redress. That's a small fix, but the real fix goes beyond the legislation and is contained in steps the government has promised to take but hasn't yet unveiled.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

I would like to go back to Part 1 of Bill C-59, which pertains to the National Security and Intelligence Review Agency.

The National Security and Intelligence Committee of Parliamentarians was created, pursuant to Bill C-22, and Part 1 of Bill C-59 includes this committee.

Our party was in favour of creating this committee, but we expressed reservations about the information being centralized in the Prime Minister's Office, and so we voted against the bill.

I would like to hear your thoughts on that.

[*English*]

Prof. Wesley Wark: Both Craig and I have testified previously on Bill C-22, and my view is that it's important to be realistic about what is proposed in C-22 as a practice, and what is necessary. Any time you give a committee of parliamentarians access to highly sensitive information, you have to surround that access with controls and protections. The challenge is to make sure that, in doing that, you don't intrude too much on the work of the committee itself.

From my perspective, C-22 reaches a reasonable balance in that regard. I don't regard the control, as you put it, of the Prime Minister's Office over the information flow as something that is likely to impact, in practice, the ability of the committee to do its work. It has many challenges ahead of it. It has only just recently, as you know, been set up in terms of members that are going to appear. The executive director has not yet been appointed. It's very much in its infancy, but my view is basically that the legislation should hit a reasonable balance until we learn otherwise through experience.

● (1025)

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

Mr. Dubé, you have seven minutes, please.

Mr. Matthew Dubé: Thank you, Chair, and while you're reminiscing, I'll spare you the knowledge of where I was 16 years ago, because that might be embarrassing for all of us.

I want to focus on the changes to CSE, because I don't think we quite have the institutional memory on that aspect given that it's mostly been something that National Defence has dealt with in the appropriate committee.

Does the amendment you suggested, Professor Forcese, affect proposed sections 27 through 54, which deal with the different authorizations that the minister can give? There's a lot of mention of acts of Parliament in those sections of the bill.

Prof. Craig Forcese: The amendments I'm proposing would affect the foreign intelligence authorizations and the cybersecurity authorizations that are alluded to in proposed section 23, to ensure that in those two contexts information that triggers a constitutional interest is steered through the authorization process by a minister and then the intelligence commissioner.

My amendments do not then also superimpose that authorization process on defensive cyber or active cyber. This is confined only to the surveillance competency of the Communications Security Establishment.

Mr. Matthew Dubé: Staying within the authorizations, you get proposed section 37, where we talk about the periods of validity of authorizations, and then in proposed subsections 37(2) and 37(3), it talks about the extension. Proposed subsection 37(3) specifically mentions that they're not subject to review by the commissioner under the intelligence commissioner act.

Do you believe it's appropriate that the minister be able to extend without undergoing the same review process that he would be subject to while making the initial authorization?

Prof. Craig Forcese: My preference is to steer every new change through the intelligence commissioner process. The issue here is that these authorizations are broadly textured. At present, for example, for foreign intelligence I understand there are three ministerial authorizations and one cybersecurity authorization. They cover a whole orbit of specific activities.

If what the minister is proposing is novel and new, then it should be steered through the regular process involving the intelligence commissioner. If it's an extension of an existing authorization, I'd have to think about that. There is the prospect, of course, that the conduct of the minister is always subjected to back-end review by the NSIRA. I'd have to go back to the act to see how narrow the circumstances are for the minister to renew unilaterally.

Mr. Matthew Dubé: I'm just having trouble with something like this because it seems that, in a lot of instances in the bill, the minister basically can't move ahead without getting the commissioner's authorization. Then in that instance you'd be able to extend without the commissioner's authorization.

I'm just wondering if it creates a difficult situation when it comes to the chain of command, for a lack of a better term.

Prof. Wesley Wark: Let me just respond very briefly to this, Mr. Dubé.

I think one thing that's not entirely clear in the legislation is.... My understanding would be that any extension of a current authorization would only occur at the request of what is now called the chief of CSE, a title that part 3 of the bill might want to omit and change, incidentally. I think it would be much more comfortable. It's an offensive and archaic title.

However, the authorization would occur at the request of the CSE head. As Craig indicates, these ministerial authorizations are for broad categories of activity. We're talking about a continuity of effort.

I think probably what was in the minds of the drafters in this regard was that they wanted to ensure, again, the difficult balance between sustaining ministerial accountability and responsibility and the powers of the intelligence commissioner. From my perspective, I would prefer to see that balance maintained rather than giving an additional power to the intelligence commissioner in this kind of circumstance.

Mr. Matthew Dubé: Okay. Thank you.

Moving backward to an earlier section of part 3 of the bill, proposed section 24 is one that I'm particularly concerned about. There are a few elements that I want to get to. I want to skip ahead to proposed subsection 24(4) because it does mention information acquired incidentally, which was something that was raised in your remarks. Proposed subsection 24(4) says:

> The Establishment may acquire information relating to a Canadian or a person in Canada incidentally in the course of carrying out activities under an authorization issued under subsection 27(1), 28(1) or (2) or 41(1).

Are there sufficient safeguards beyond these vague notions of privacy for that kind of information being collected through the course of CSE's activities?

● (1030)

Prof. Craig Forcese: Essentially proposed subsection 24(4) constitutes that, for greater certainty, it is possible legally for the CSE to acquire information incidentally in the course of its properly authorized foreign intelligence and cybersecurity conduct. That incidentally acquired information would presumably then be pulled into the retention rules and how you're supposed to govern that information. There are provisos about protecting the privacy of Canadians.

The other aspects of proposed section 24 are a little bit different. If you'll forgive me, I'll just comment on those. The other ones allow the service—notwithstanding the general admonishment that it's not supposed to direct its activities at Canadians or persons in Canada—to overcome that barrier for certain limited reasons, for research, for instance.

The issue then for me is what happens to the personal information that might be acquired over the course of that authorized conduct. How is that information going to be dealt with? Is there a requirement that it be expunged or be deleted, if done for research purposes? Are there other safeguards in place?

Mr. Matthew Dubé: Lastly, very quickly to both of you because I'm on my last minute here, I'll just go to another part of the bill on the metadata or the datasets, depending on your preference—that seems to be the synonym, more than anything, but....

I tried to ask the director of CSIS about issue. It seems unclear to me in what way it will parse through...because its operations will be authorized, it seems to me, in a more general way. The way it chooses to retain doesn't necessarily seem to be subject to the same kind of scrutiny. It's not going to be piece by piece of the information, but rather this sort of general collection of datasets.

Am I misconstruing that? I'm just seeking some clarity in my last 30 seconds.

Prof. Craig Forcese: The classes of Canadian datasets have to be approved by both the minister and the intelligence commissioner. Then, if the service chooses to retain individual datasets, that retention is subject to court approval, and the court could impose conditions on queries and exploitation. The individual dataset, then, is subject to closer scrutiny by an independent judge.

The other aspect of datasets is that it's more than metadata. It doesn't have to be metadata; it can be content information.

The Chair: We're going to have to get a fuller response at some other date.

Mr. Fragiskatos, you have seven minutes.

Mr. Peter Fragiskatos (London North Centre, Lib.): Thank you both for being here today.

You're both well aware of the ministerial directives that were issued by Minister Goodale in late September with respect to the use of information obtained by torture, but for the purposes of the record and for the millions watching at home on CPAC.... I'm sorry, that was a little levity.

The rules prohibit the use, by the RCMP, CSIS, and CBSA, of information that was likely obtained through mistreatment in three main areas, except when it is necessary to prevent loss of life or significant personal injury. Use of this information is prohibited if it could lead to further abuse or torture, and with respect to information obtained through torture, it can no longer be used to prevent risks to property.

These are directives. It's not legislation that we're talking about. Could you give us your thoughts on whether the directives are good enough, or do we need these principles enshrined in law? Obviously, if they're enshrined in law they will be harder for any future government to change.

Prof. Wesley Wark: I'll begin. I think both Craig and I have commented publicly on the ministerial directives.

I would say first of all that the current ministerial directive that was recently released is a great advance on the original versions in 2011, which I think were very problematic in terms both of protecting Canada's duties and obligations under law and providing for security.

The thing that I think is most advantageous about the current directive is that it makes a distinction between what is often called “inbound” and “outbound” information, and it is particularly strong in trying to ensure that Canada is not complicit in acts of torture by sharing information with overseas bodies that might have a very poor record in that regard. This has been the source of many of our problems in the past.

With regard to inbound information, there is always the challenge of knowing exactly whether it was derived from torture. You can have your suspicions, but no foreign intelligence agency is going to tell you directly, “By the way, we got this from torture.” What the current directive provides for is the use of some kinds of information in very extraordinary circumstances, which probably are unlikely to arise in practice.

From my perspective, it's a good question whether this should be brought forward into legislation or regulation. I am pleased that it's in regulation and that the regulation is public. I think it is very important to have that ministerial directive in public. Insofar as it is in public, which is a change from past practice, perhaps that is good enough.

● (1035)

Prof. Craig Forcese: In response to your question, yes, I would prefer to see it in legislation.

Mr. Peter Fragiskatos: Can you expand on that?

Prof. Craig Forcese: It's for the reasons you've described. For one thing, it is embedded and more difficult to change. For another, in the past, ministerial directives were not always transparent. We know about only the 2009 and 2011 ministerial directives through the use of access to information. As a policy matter, the government is more proactively disclosing ministerial directives, but of course it would be nice to ensure that going forward there was always transparency in this area. Again, then, there's a transparency aspect.

Mr. Peter Fragiskatos: Thank you very much.

Mr. Wark, I want to quote a couple of things here.

This is a sentence from an article you wrote in *The Globe and Mail* shortly after Bill C-51 was introduced. You say, “Strengthened accountability may well be our best bet to ensure that new security powers are balanced against rights protections.”

After Bill C-59 was released, you wrote, “Canada may have restored its place in the world as it pertains to national security review and democratic controls, a place we gave up after 1984.”

This is a general question. I think it shows that Bill C-59 has made an important advance, but I wonder whether you could give us your thoughts on where we were and where we are now as a result of Bill C-59.

Prof. Wesley Wark: Briefly I would say that once upon a time, going back to 1984 and the passage of the CSIS Act, Canada was a bit of a global leader in terms of providing for accountability for security and intelligence, albeit in a relatively limited realm. That was augmented when the CSE commissioner's office was created in 1996.

However, after that time I think we fell behind advancing practices among our counterparts, particularly our Five Eyes members. We didn't have across-the-board integrated review. We weren't covering many aspects of an increasingly integrated practice of intelligence and security. We had no parliamentary capacity to really dig into the classified information, which is the lifeblood of the security and intelligence system.

My view is that with regard to the creation of NSIRA, the intelligence commissioner, and the legislation that has been passed to create a National Security and Intelligence Committee of Parliamentarians, that package puts Canada, I would say, in a leading position in the world in terms of providing for accountability, in theory. Now we'll have to see how well it is actually put into practice. However, we certainly have the bones of a very impressive system for accountability, and now we'll just have to make sure we can make it work.

Mr. Peter Fragiskatos: Thank you.

With about a minute and a half left, I wonder if you could expand, Professor Wark, on what you said in your opening remarks about the consent that would be necessary from the Minister of Foreign Affairs for active cyber-operations. You said that you think this is a good idea. Could you go into that a little more?

Prof. Wesley Wark: Sure. Very briefly, I think it's absolutely vital.

In an earlier draft of my remarks to the committee, I was going to cite some examples where additional eyes on issues like this might have been helpful. I'll just take advantage of this moment to say that "thanks" to the Snowden leaks, we know of some instances of CSE operations that probably needed more careful thought before they were implemented. I think the most egregious example was the operation in which CSE was involved. It was part of a Five Eyes operation to target the Brazilian Ministry of Mines and Energy, and it was clear from the prime minister at the time's comments on that operation, when it was revealed in public, that there wasn't any particular political scrutiny of that at a high level.

I think if we go into the realm of active cyber-operations, what we're talking about are taking some very sensitive operations against foreign targets, foreign states, and foreign entities of all kinds—adversaries. We'll be doing this in a Five Eyes context. We will have to be in a position to understand the likelihood of success or failure, and the possibility of what kind of blowback may occur from this, whether we're encouraging an escalatory spiral.

That was the reason I mentioned the Stuxnet attack on the Iranian infrastructure, which was designed to damage their nuclear weapons program, but resulted in the Iranians ultimately launching a cyber-attack on the Saudi Arabian oil industry. There is that escalatory blowback dimension of this, and I think the Minister of Foreign Affairs needs to be involved in terms of providing consent to give eyes to the international dimensions of what might happen if we decide to do this, to really give more eyes to the question of costs and benefits.

● (1040)

The Chair: Thank you, Mr. Fragiskatos. I suppose after 1984, Bill C-59 puts us in a brave new world.

Mr. Motz.

Mr. Glen Motz: I have no comment about 1984.

As we know, you can't wrap regulations and ministerial directives together. They're not the same. We know that. With that in mind, do both of you believe that these regulations allow accountability and public record with the ability to be more nimble? Rather than having everything in the bill, is there some value in having some provisions that require nimbleness to be in regulations?

Prof. Craig Forcese: Absent a specific suggestion in this bill, I don't know that I would single anything out as better embedded in regulation. Professor Wark and Professor Carvin this morning both mentioned that the concept of dataset is broadly clothed. If we were to define it rigidly in the act, then we may have a problem. However, we don't. We have an open-textured definition of "dataset" that's then subject to scrutiny by independent oversight entities. That's an example of flexibility. There's also the prospect of "exigent circumstances", which the bill recognizes in several instances.

I don't see this as overly restrictive, and to a certain extent, I think a lot of these changes surface internal guidelines that the services have in fact employed. I think codifying it in legislation is actually important because it creates a sense that these are agencies that do comply with the rule of law that people are otherwise unaware of because these standards are opaque and buried in operational policies. I think that's important in terms of credibility.

Mr. Glen Motz: Thank you.

Prof. Wesley Wark: I would just add very briefly that probably the ideal thing would be to have a balance between legislative direction and regulation in detail. I think one of the things that Bill C-59 does in particular through its accountability provisions is to ensure that if that combination of legislative direction and ministerial regulation isn't working properly, that will appear in the kinds of review reports and reporting to the minister that the body will do.

I would also say that although this remains a work-in-progress on the part of the government, I think it will be very important to roll out as quickly as possible the government's commitments on national security transparency, what has sometimes been referred to as the transparency charter. Transparency is a second dimension to accountability that I think will help ensure that balance between legislative direction and ministerial regulation is effective.

Mr. Glen Motz: Thank you very much.

Professor Wark, you had indicated at the close of your opening remarks that you didn't get a chance to explain what you believe isn't in Bill C-59. I'm hesitant to give you the floor to do that but nonetheless I'm curious to know what you think those might be.

Prof. Wesley Wark: Mr. Motz, I greatly appreciate the opportunity. I'll be very brief on this. I think these are very important issues and of course no piece of legislation, as sweeping as it might be, is going to capture them all, but there's lots of work to be done to truly modernize Canadian intelligence.

I'll give you my short list—there's a longer list—and Professor Carvin referred to these things in a different kind of dimension. I think Canada needs a comprehensive national security strategy. We've only issued such a thing once back in 2004, and we need a commitment to updating it. I think that we need, crucially, because Bill C-59 in terms of new powers is all about collection, an integrated, properly resourced, centralized intelligence assessment function. This is one of the great gaps in the system.

I think—this is a subject for another debate—we need a dedicated foreign intelligence agency distinct from CSIS. We need to move forward, as I said, with the proposed national security transparency charter. We need a revision and an updating of the Security of Information Act, which was part of the old Bill C-51 and is now I think completely out of date. We need modernized access legislation, particularly to resolve issues around access to basic subscriber information. There's more but that's my short list.

Mr. Glen Motz: In the final 30 seconds that I have left, could we ask as a committee that you would provide those to us in writing at your convenience?

Prof. Wesley Wark: Absolutely. I will do that.

Mr. Glen Motz: Thank you very much. I appreciate it.

The Chair: We have maybe a minute, and three questions.

Mr. Nathaniel Erskine-Smith: I have three questions and need yes-or-no answers.

First, we have on record that Mr. Forcese wants special advocates. Mr. Wark, do you think we should have special advocates in the no-fly list system, just yes or no?

● (1045)

Prof. Wesley Wark: Yes.

I feel like I'm on *Jeopardy.*

Mr. Nathaniel Erskine-Smith: Perfect. Both of you testified before the ethics committee and before this committee on SCISA, now SCIDA. You suggested fixes that are not in this legislation. Do you suggest that we tweak this further or do you think we should...? Clarifications in the definition have occurred, there's now "contribute" versus "relevance".

Do you think there's a "wait and see" mode to allow the review bodies to do their work and report to Canadians as to the acceptability of the sharing, and then make further changes down the road or do you want this committee to make further changes now?

Prof. Craig Forcese: Further changes.

Prof. Wesley Wark: Further changes.

Mr. Nathaniel Erskine-Smith: This is my last question. We promised Canadians to improve the accountability of national security agencies. We promised to fix the overreaching and in some cases unconstitutional nature of Bill C-51, and then Bill C-51 overall with Bill C-22 and Bill C-59.

Do you think we've done that?

Prof. Craig Forcese: Yes, subject to my concern about personal information that might be swept into the ministerial authorization or not swept into the ministerial authorization.

Prof. Wesley Wark: My answer is yes, and there's more work to be done. It never stops at one particular piece of legislation.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: Thank you, Mr. Erskine-Smith, for your very brief intervention.

I want to thank both of you on behalf of the committee for not only your presence here today but your thinking and your contributions to the shaping of this legislation. It is indeed a really good example of the government and non-government community working together to shape what I think pretty well everyone is agreeing is a better piece of legislation.

Thank you and with that we'll adjourn.

The meeting is adjourned.