HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

# Standing Committee on National Defence

NDDN • NUMBER 016 • 2nd SESSION • 41st PARLIAMENT

**EVIDENCE**

## Thursday, March 27, 2014

## Chair

**The Honourable Peter Kent**

# Standing Committee on National Defence

**Thursday, March 27, 2014**

● (1105)

[*English*]

**The Chair (Hon. Peter Kent (Thornhill, CPC)):** Good morning, colleagues.

We are here today pursuant to Standing Order 108(2) to continue our study of the defence of North America.

We have three witnesses with us today: Ms. Jill Sinclair, the assistant deputy minister of policy, Canadian armed forces; Major-General Christian Rousseau, chief of defence intelligence, Canadian armed forces; and from the Department of Foreign Affairs, Trade and Development, Artur Wilczynski, director general, international security and intelligence bureau.

Colleagues, although we are all quite conscious of recent events in Crimea and Ukraine, I would urge you to focus your attention on the topic at hand, in light of the changed context of our large northern neighbour.

We will start with opening statements.

Ms. Sinclair, you have the floor for 10 minutes, please.

**Ms. Jill Sinclair (Assistant Deputy Minister, Policy, Canadian Armed Forces, Department of National Defence):** Mr. Chairman, thank you for the invitation to appear and for the work that you're undertaking with your study on the defence and security of North America.

I was pleased to have been able to appear last year to speak to the committee about NORAD and I am pleased to be here again. I have a few brief and general comments to situate our discussion today.

[*Translation*]

My remarks today will situate your work on the defence and security of North America in the context of the Canada First Defence Strategy, defence and security cooperation with the U.S., NORAD, and emerging challenges in continental defence.

[*English*]

It all begins for us with the Canada First defence strategy, which is our capstone defence policy document set out in 2008. As you may know, we will be refreshing it, as was announced in the Speech from the Throne in 2013.

The Canada First defence strategy is the government's foundational defence policy statement. It lays out the roles and missions for the Canadian armed forces. Being a strong and reliable partner to the United States in the shared defence of the continent is among the key mission sets for the Canadian armed forces and an enduring role for the defence team.

Our partnership with the United States is unique. It shapes all aspects of our work. We cooperate at every level, from the operational to the strategic. We're interoperable with the U.S. military and exercise and share personnel on a systematic and regular basis. At the strategic level, we have a number of foundational arrangements with the United States for consultation and cooperation, from bilateral strategic policy dialogues to the Permanent Joint Board on Defence. Our ministers meet regularly in Canada, in Washington, at NATO and elsewhere in the world.

We have a very well-developed structure for our work. Since 1940, the Permanent Joint Board on Defence , the PJBD, has met twice a year to discuss and advise on defence matters. The board now also includes the input of important security partners and stakeholders, including Public Safety Canada and the U.S. Department of Homeland Security, in addition to the State Department, Foreign Affairs, and the Coast Guard, and other players as required. It continues to be the most senior defence advisory body and plays a crucial role in fostering critical senior military and diplomatic contacts, as well as frank discussion on the range of dynamic issues affecting continental defence and security.

On the domestic front, our close cooperation is reflected in a wide array of bilateral institutions and agreements between Canada and the United States on the defence and military side. In fact, there are more than 800 arrangements that govern the day-to-day military relationship, including increasingly among the three key commands of our Canadian Joint Operations Command, NORAD, and the U.S. Northern Command, which together provide for the security and defence of North America in cooperation with each other.

NORAD, North American Aerospace Defense Command is core to the defence of the continent. For more than 55 years, binational cooperation through NORAD has encouraged unprecedented interoperability between the Canadian armed forces and the U.S. armed forces. There are currently nearly 300 Canadian Forces members posted to NORAD headquarters. We also have a number of Americans on exchange in Canada.

I spoke about treaty obligation and an operational military-to-military relationship. NORAD holds a distinctive place in the overall management of the strategic and operational Canada-U.S. defence relationship. It fulfills the aerospace warning, aerospace control, and maritime warning missions. It undertakes it 24 hours a day every day. It also plays an important role in ensuring Canadian sovereignty and security, serving as a deterrent against potential attacks and providing a crucial surveillance capability.

● (1110)

[*Translation*]

But, defence at home begins abroad. The threat environment is dynamic and evolving and there are a range of challenges that we must be prepared to meet.

Beyond partnership with the U.S., success will lie in working collaboratively with both other government departments and international partners as the traditional divisions between security and defence continue to blur.

[*English*]

I will leave you with two examples to consider.

The first is cyber. Threats in cyberspace, as we know, know no boundaries, and while cooperation with the U.S. is crucial, we also work globally, including with the U.K., Australia, and New Zealand, as well as with our NATO partners.

As with all other sectors of security, the Canadian armed forces depends more heavily than ever on cyberspace for command, control, communications, and other mission critical functions and must be able to protect its ability to operate in the face of rapidly evolving threats and vulnerabilities. Similarly, National Defence plays an important role in supporting whole-of-government efforts to strengthen national cyber security.

In Canada, cybersecurity is led by Public Safety Canada, but we work increasingly closely and coordinate with other partners as we seek to ensure seamless cooperation in assessing and responding to cyber threats to Canada.

The second thing I'd like to mention briefly is the Arctic. While threats to the Arctic aren't currently military in nature, National Defence works in close support with our whole-of-government partners that have the lead in the Arctic. We already work together with the U.S. through NORAD and through tri-command cooperation and other multilateral fora in support of these civilian departments and agencies that have the lead in the Arctic. We work more broadly with international partners, for example, through the northern chiefs of defence venue, which is where chiefs of defence work to discuss their cooperation and support of civilian lead agencies.

In conclusion, I'd like to say that the defence of North America is the sum of many parts, working together with Foreign Affairs—I'm delighted that Artur is here from DFATD—Public Safety, and other government departments, and in partnership with the U.S. and with other friends and allies to ensure we deal with threats to North America, whether traditional or emerging, like cyber, as far away from our shores as possible.

[*Translation*]

I would be happy to answer your questions.

Thank you very much.

[*English*]

Thank you.

**The Chair:** Thank you very much, ADM Sinclair.

General Rousseau, you have the floor.

**Major-General Christian Rousseau (Chief, Defence intelligence, Canadian Armed Forces, Department of National Defence):** Mr. Chair and members of Parliament, thank you very much for the invitation this morning.

It's my distinct pleasure to address you and provide our views on threats to North America. I'm glad to be sitting here with my confreres to help you in your deliberations and study of this very important topic.

[*Translation*]

Before I talk about possible threats to Canada, as we see them, I would like to provide some background to my role as Chief Defence Intelligence and Commander of Canadian Armed Forces Intelligence Command. My team's role consists in helping the Department of National Defence and the Canadian Armed Forces make sound decisions in the exercise of their duties. Whether conducting operations in the Arctic, providing support to the Vancouver 2010 Olympic Games, responding to a terrorist threat, or carrying out oversees operations, the Canadian Armed Forces have need of the most accurate and up-to-date intelligence in order to achieve their military objectives and ensure the security and protection of their personnel.

Defence intelligence is also a key element in the ability of the Government of Canada to make informed decisions on defence issues, national security and foreign affairs. In carrying out our mandate, I can say with pride that our intelligence capability is world-class and offers the necessary tools—24 hours a day, 365 days a year—to give our leaders an intelligence advantage. Allow me to repeat that intelligence is the main factor in operational success.

[*English*]

Canada's defence intelligence relationship with the U.S. is one of the most important of our international defence partnerships. It is a long-standing relationship dating back to the Second World War and reinforced over the years through our binational command at NORAD, our partnership in NATO, and our participation in coalition operations like in the Balkans or Afghanistan.

A permanent liaison office in Washington manages the relationship for me. There are Canadian defence intelligence liaison and exchange personnel positioned in all the main agencies, components, and commands of the U.S. defence intelligence community.

● (1115)

[*Translation*]

I should also note here that we benefit from productive relationships with our national partners. You, and the Canadians whom you represent, may be certain that your intelligence organizations are promoting the interests of this country in the areas of defence and security.

[*English*]

Now I shall turn to the subject at hand, threats to North America.

Over the past year you have visited several defence-related locations, and I know that you plan to visit several more. I appreciate the opportunity to help situate the committee and your subsequent report in relation to what we see as the current threat environment. I focus the vast majority of my energy on foreign military threats and support to CF operations abroad.

We define threat as a combination of intent and capabilities. Having the desire to harm Canada but no capability to do so does not represent a threat from an entity. Once it has discerned the intent of a foreign actor to harm Canada, the intelligence apparatus will have as its job to track any advancement in capabilities and recognize when that entity becomes a threat.

Tracking or predicting changes in capabilities is sometimes challenging, but usually possible within a reasonable margin of error. Gauging current and evolving intent is more complicated, but still possible. Predicting future intent and staking one's security only on that prediction is highly risky. Whereas a state may not exhibit hostility while it is developing a capability, once acquired, that capability remains in its arsenal whatever changes happen in its political calculus and intent.

With that definition in mind, I can say that at this time we do not see a state actor that has both the capabilities and the intent to harm Canada militarily. We view the proliferation and potential use of weapons of mass destruction, including chemical, biological, radiological, and nuclear and ballistic missiles against the North American continent, as worrisome. Such states of key concern as Iran and North Korea will likely continue in their attempts to acquire, develop, and improve weapons of mass destruction and the ballistic missiles capable of delivering them.

The dual-use nature of most biological and chemical-related technologies makes monitoring warfare programs and procurement involving these materials difficult. Furthermore, the ostensible civilian application of nuclear technology can mask its military application or intention.

Weapons of mass destruction attacks against North America could take many forms, including covert or non-traditional delivery, such as aircraft or vehicles by either states or non-state actors. It is important to note, however, we assess that only states could master the complexities of ballistic missile delivery systems.

In the case of lran, its current missile arsenal lacks the range and complexity to strike targets within North America. On the other hand, North Korea has expressly indicated that it wants to be able to target North America with its nuclear armed missiles. While it is actively developing ballistic missiles that could potentially reach North America, whether or not they have developed a practical nuclear weapon remains unclear.

My two areas of interest as CDI with regard to the cyber environment are the threats that affect the ability of the Canadian armed forces to operate and the cyber capabilities of foreign military actors. As mentioned earlier, the bigger picture of cyber threats, i.e., threats against Canada in general and threats emanating from non-military actors, are the purview of the Department of Public Safety.

The potential exists for foreign states to employ computer network exploitation capabilities in support of strategic intelligence collection. To be clear, they're using computers to spy on Canada. They may also use network reconnaissance in support of planned or anticipated computer network attacks, that is, looking at our computer system so that at the moment we would be defending ourselves or attacking, they would do a cyberattack, thereby rendering our command and control systems inoperable so that we cannot use the Canadian armed forces in an effective way. Also, they may use network attacks against private and government data and communications networks on which we rely. As CDI, we'd be interested in all such attacks, because they affect the ability of the Canadian armed forces to operate.

Mr. Chair, this concludes my presentation. Thank you very much for the opportunity. I look forward very much to answering your questions.

● (1120)

**The Chair:** Thank you very much, General.

We now turn to DFATD and Mr. Wilczynski, please.

[*Translation*]

**Mr. Artur Wilczynski (Director General, International Security and Intelligence Bureau, Department of Foreign Affairs and International Trade):** Thank you very much, Mr. Chair.

Ladies and gentlemen members of the committee, I am very happy to be here today with you along with my colleagues from National Defence and from the Canadian Armed Forces.

I would like to thank you for giving me the opportunity to speak to you today as part of your study on North American defence and, in particular, on the nature of your relationship with United States.

Defence and security cooperation has been ongoing between our two countries for a long time. It is rooted in common values and interests as well as our common desire to defend North America.

[*English*]

The whole-of-government approach to the relationship, as was indicated by Ms. Sinclair and General Rousseau, demonstrates and reflects the complexity, the depth, and the importance of the relationship that we have with the United States.

As director general of the international security and intelligence bureau at the Department of Foreign Affairs, Trade and Development, I am responsible for the management of the foreign policy dimension of Canada's defence and security relationships. This includes our relationship with key bilateral allies and partners, but also includes engagement with key multilateral organizations such as NATO and the OSCE and other institutions.

My bureau is also responsible for advancing Canadian positions to address international crime and terrorism, for assessing threats to our missions abroad, and for acting as a focal point within our department for intelligence matters.

[*Translation*]

As Ms. Sinclair mentioned, the North American Aerospace Defence Command, or NORAD, is pivotal in our defence relationships. It plays a critical role in the defence and security of North America by preventing air strikes on the continent, protecting sovereign airspace in Canada and the U.S., and providing maritime and aerospace warning capacity.

[*English*]

I'd like to add to what Ms. Sinclair said by informing the committee that Foreign Affairs, Trade and Development Canada complements the engagement by National Defence and the Canadian Forces by also working directly with the NORAD commander. Our department provides a senior level policy adviser, or pol ad, to the commander to provide advice and information that informs the commander on broad Canadian policy objectives and to act as a liaison with our organization.

As Ms. Sinclair also noted, the Permanent Joint Board on Defence is yet another key pillar of our defence cooperation with the United States. It is a strategic policy body that oversees bilateral defence issues between our two countries. As someone who has participated in PJBD meetings from both Foreign Affairs and Public Safety perspectives, I can attest to the value that this important interdepartmental and inter-agency forum brings to the relationship. It serves as a touchstone that brings together senior officials, both civilian and military, to discuss key defence issues of mutual concern.

This efficient mechanism has served Canada well, providing us with favoured access to American political and military processes, and is an opportunity to deepen interoperability and cooperation in areas ranging from security in Mexico and Central America to the Arctic and to maritime domain awareness.

[*Translation*]

The United States is also Canada's main partner in the Arctic. Our two countries have long collaborated in the fields of science and technology, environmental protection, infrastructure development, search and rescue, border patrols and law enforcement and surveillance.

[*English*]

Neither Canada nor the United States perceives a military threat in the Arctic for the foreseeable future. Given the harsh terrain and environment, the Arctic is a region that commands cooperation, and Canada and the United States are partners in this respect. Our cooperation at the Arctic Council has been close, and the succession from Canada's current chairmanship to that of the United States in 2015 is an opportunity for us to advance in a number of key areas of common interest.

Canada and the United States are close partners in our defence engagements elsewhere in the world as well. Our partnership includes collaboration to enhance security in our own hemisphere and to address threats before they reach our shores, such as those posed by transnational criminal organizations in the trafficking of illicit substances.

Canada and the United States are leading security donors in the hemisphere, delivering programs to build the capacity of our partners in the Americas. We work closely with the United States in the planning and delivery of our anti-crime and counterterrorism capacity-building programs, ensuring that our efforts and those of the United States are mutually reinforcing

For example, together Canada and the United States have built capacity in the Caribbean for forensic ballistic tracking and information sharing. Most recently, Canada has delivered this training and equipment in Jamaica and in Trinidad and Tobago, while the United States has funded the installation of this equipment in Barbados.

● (1125)

Both Canada and the United States are allies in NATO. The alliance is a cornerstone of Canadian security and defence policy, is a major contributor to international peace and security, and binds the transatlantic security relationship between North America and Europe. Through NATO, we have worked side by side with the United States on important issues and operations such as the ISAF mission in Afghanistan and Operation Unified Protector in Libya.

[*Translation*]

Like the United States, Canada is aware of the Asia-Pacific regions' ever-growing contribution to world prosperity. And in light of that, we are strengthening dialogue and cooperation with the region.

Last year, with our American partners, we launched the bilateral strategic dialogue on Asia. This mechanism provides another opportunity to have regular dialogue and to examine the cooperation between Canada and the United States, bolstering Canada's objectives in the region.

Our strong defence relationships rest on some of the best-integrated defence industries in the world.

[*English*]

We have established a range of cooperative mechanisms to support the joint development of defence technology, increase the interoperability of our forces, and ensure a ready supply of defence goods for both countries.

Canada and the United States enjoy a unique, multi-faceted, and dynamic defence relationship based on shared interests, common values, and a joint commitment to the defence of North America. This relationship remains a top priority for Foreign Affairs, Trade and Development Canada.

Thank you. I'm happy to answer your questions.

**The Chair:** Thank you very much, Director General Wilczynski.

We will now commence our opening round of questioning with seven-minute segments.

Go ahead, Mr. Chisu.

**Mr. Corneliu Chisu (Pickering—Scarborough East, CPC):** Thank you very much, witnesses, for being here today, and thank you very much for your valuable presentations.

The following question is for Ms. Jill Sinclair.

Can you outline how the Canadian armed forces' policies in the Arctic are continuing to evolve as this region becomes increasingly relevant, and also, looking at the recent developments with one of the members of the Arctic Council which is flexing its muscles not only somewhere else in the world but also in the Arctic, how they are increasing capabilities, modernizing capabilities, and paying attention in the north?

**Ms. Jill Sinclair:** Thank you for the question.

Over the last number of years, the government has systematically and assiduously invested in the Arctic and in our capabilities, obviously, from the Canadian armed forces perspective, defence, but also whole of government. I will cite just a few examples.

In addition to NORAD, which we've talked about, and its continuing work in terms of surveillance and awareness and domain awareness, we have forward operating bases up in the high north, Yellowknife, Rankin Inlet, Iqaluit, Inuvik. We have our joint task force north, where we have people deployed. We have a headquarters in Yellowknife. We have the investment in the Arctic offshore patrol ship, which will give us an armed seaborne surveillance capability. Construction will begin in 2015 on that. We have the Nanisivik refuelling facility, which will be up and running by 2017. It's on Baffin Island. We have the Canadian Forces Arctic Training Centre in Resolute Bay. It was opened last August, I'm pleased to say. We've increased the number of rangers we have from 3,000 to 5,000, which gives us eyes and feet on the ground and people who are very familiar with the terrain. We have an ongoing series of exercises. The biggest ones are Nanook and Nunalivut, which you may have heard of. The Canadian armed forces exercise all year, winter and summer, to make sure we have our sovereignty presence and we have the capability. We also established northern chiefs of defence meetings a couple of years ago to make sure we had a venue for chiefs of defence of northern countries to cooperate.

We really have, I think, increased our presence in the Arctic not just in policy terms but in real terms. I would also add that with the RADARSAT Constellation that is supposed to be launched in 2018, Canada will then have four times a day surveillance of the Arctic. It will be the most surveillance and awareness capability of any country in the world.

● (1130)

**Mr. Corneliu Chisu:** Thank you very much.

Now, I have a question for General Rousseau.

In addition to providing support to military operations, for which I was grateful when I was in Kandahar, Afghanistan, the fusion centre, the Canadian Forces intelligence group, provides expertise on strategic threats to Canada and allied governments; indication and warning intelligence on international, political, and military activities; strategic and crisis coverage of regional security developments that may affect Canadian security interests; or engage Canadian Forces and scientific and technical intelligence with a defence or security focus. Threats such as terrorism and international criminal activities are monitored.

What sorts of threats could develop within North America that we are currently monitoring? I know the west coast is well covered by an intense cooperation between the United States and Canada. What is going on on the Atlantic coast, where we have Denmark and Norway? Eventually, somebody would be interested in that area in Canada.

**MGen Christian Rousseau:** Thank you, sir, for the question.

You talked about threats emanating within North America, and it would not be an issue for me. I very much look at supporting Canadian Forces in defending Canada from foreign actors. Any threats inside of Canada would be dealt with internally, by RCMP or CSIS.

In terms of some of the other powers, state actors out there who would have competing views of the world, I would come back to my initial context. In the world where we look at capabilities and intent, we do not see a current military threat to North America. There are competing requirements or demands in terms of economics or things like that, which would not be a military issue. The military, in its support to whole of government, does provide some situational awareness of maritime approaches to Canada and air approaches to Canada, but it's very much to support, not in the view that we think there's a military threat approaching Canada.

Did you want to add something?

**Ms. Jill Sinclair:** Sure. Thank you.

If I might say a supplementary word, I think the question points to the very interesting dynamic, and Artur talked about this a bit. When you look at the defence of North America and the threats to North America, so many of them are not military. It's illegal migration. It's drug flows.

With regard to the integration of all of the key government actors working together to look at all those threats, and that includes cyber threats, we have something called the marine security operations centres. We have one on the east coast and one on the west coast, and the RCMP has one on the Great Lakes. What's interesting about that, and it's sort of a microcosm of how to deal with the security of North America, is that Canadian Forces, DND, Canada Border Services Agency, Fisheries, the Coast Guard, Transport Canada, and RCMP all sit together in a fusion centre to basically take stock of what's going on on the maritime approaches or in the Great Lakes.

I would just posit that because I think it's interesting to keep that broader sense of how you actually defend North America and where do the threats come from. They are not all military.

**The Chair:** Thank you very much.

The time has expired, Mr. Chisu.

Ms. Michaud, please.

[*Translation*]

**Ms. Élaine Michaud (Portneuf—Jacques-Cartier, NDP):** I would like to thank the witnesses for their presentations.

I will take advantage of this opportunity to get more details on the role that you play in terms of cyber-security and cyber-defence.

How does the mandate of your respective organizations differ from that of the Communications Security Establishment of Canada? What is your relationship with the CSEC? It is a bit unclear to me. What is the nature of your collaboration? How far do your mandates extend, both in terms of defence intelligence, and compared to the International Security and Intelligence Bureau? If you could provide me with some information on that subject, it would be greatly appreciated.

**Mr. Artur Wilczynski:** I will answer first.

Several departments are involved in this file. As was mentioned in our presentations, it is really the Department of Public Safety which is in charge of cyber-security. We work closely with all organizations in our field to advance the interests of Canadians in the area of cyber-security.

In my office, for example, we work on cyber-security only to a limited extent. However, our department works to promote Canada's broader interests where the Internet is concerned, for example in terms of freedom of access, which is a multidisciplinary field, or in terms of promoting human rights.

All of this occurs in a context of interdepartmental cooperation, and each of our organizations provides a complementary perspective to help advance Canadian interests.

● (1135)

**MGen Christian Rousseau:** I will continue along the same lines.

As I explained at the beginning, my main mandate is to help the Canadian Forces in their job. There are always cyber-actors who try to keep us from doing our job. Maintaining the security of our own networks is what interests us above all. We also want to understand how military forces outside of Canada who could one day become a threat use cyber-security.

Representatives of Communications Security Establishment Canada have both knowledge and expertise. It sometimes happens that we consult them to know what they think of a given subject. However, we are not responsible for them, and vice versa. It is a partnership, really.

**Ms. Élaine Michaud:** I suppose that there is still a sharing of information or common strategies that could be implemented by the different organizations.

**MGen Christian Rousseau:** If we find that an Internet user from another country is using particular tactics or techniques, we will check with our national and international partners to find out if they have already dealt with that type of threat or attack. So in that sense, we work together. We ask them if they know that type of activity coming from one cyber-actor or another, and how they reacted to best coordinate their defence.

**Ms. Élaine Michaud:** Would it be advisable to increase the role that the Department of National Defence plays in cyber-security in Canada, or in your opinion, is the current system sufficient?

**MGen Christian Rousseau:** This is how the responsibilities are currently divided.

I am only responsible for the security of our networks and for responding to threats. I try to understand what external actors are doing in order to better meet the needs of National Defence and the Canadian Forces.

As for the needs of the rest of the Government of Canada or the needs of Canadian industry, they are not a part of my current mandate. So I cannot really say if they are being well served by the current system.

**Ms. Jill Sinclair:** I would like to add a few comments on the subject.

[*English*]

Seamlessness of whole-of-government cooperation in cyber is absolutely essential, so to your question about cooperating and sharing information, according to our mandates and in the appropriate ways we share. We share in terms of identifying what the threats are in terms of bringing our common expertise to the table in terms of dealing with the responses.

The Canadian Forces in the last number of years, I think like other militaries around the world and just about every organization of government or business, for that matter, have recognized that the cyber threat is increasing. We have about 200 people at the moment who are engaged in various elements of the cyber effort for the Canadian Forces. In 2012 we established a director general of cyber, basically looking at the requirements for the Canadian Forces, what's the environment, what do we need by way of expertise, how do we continue to protect our own networks so that, as General Rousseau said, we remain resilient and robust in case there's a threat, and how do we take a deliberate and careful approach to integrating cyber-intermilitary operations.

It is very much a work in progress. It is one of the most whole-of-government efforts, I think, that exists around the federal government, also working, of course, through Public Safety, with private industry and also with the territories and provinces.

[*Translation*]

**Ms. Élaine Michaud:** Thank you.

Now I would like to move on to another subject.

During our last meeting, we heard from different witnesses who told us, among other things, about a ballistic missile defence system. Notably, Professor Philippe Lagassé told us that if Canada maintained the condition that the Prime Minister set out in 2005, namely that Canada would not become a member of a system unless no costs were associated with it, then Canadians might accept joining such a system.

Given the growing threats that we may have to face, do you think that the United States would be ready to agree that Canada would make no additional investment? Of course, we already have resources that are invested directly or indirectly in the system. However, if the United States had to invest considerably more money in this system, I wonder to what extent they would agree to Canada's participation in this project without more or less reciprocal investments.

I would like to hear your opinion on this question, because I found professor Lagassé's perspective fairly unrealistic.

● (1140)

[*English*]

**Ms. Jill Sinclair:** Perhaps I'll begin, Mr. Chair, and then I'll ask my colleagues to supplement.

**The Chair:** A short response, please.

**Ms. Jill Sinclair:** Absolutely.

The government's position was taken in 2005, and it wasn't cost related. It was that we would not participate in ballistic missile defence, and that's the extant position, as General Rousseau said.

Since that time the missile defence issue, in terms of who could have capability, has changed a bit, but the government's position is very clear: since 2005 we are not part of ballistic missile defence.

**The Chair:** Thank you, and the time has expired.

Ms. Gallant, please, for seven minutes.

**Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC):** It's been reported that the Chinese military uses its cyber assets to steal information from corporate North America. This is a type of asymmetric warfare in that they manipulate our economies, and that manipulation is being used to weaken our countries financially. When economies lag, defence spending decreases, thereby allowing for vulnerabilities which may not exist were spending restraints not in place.

When incursions into the Republic of Georgia were made by Russia, their communication system was down, under cyberattack. Estonia also suffered a cyberattack, which they believe was perpetrated by a historic local aggressor. Given that state actors, not to mention non-state actors, are progressive in using cyberactivities as weaponry, in addition to the counterattack measures that we're already putting in place, does it make sense for us to start utilizing cybercapabilities for offensive use as well when we come under attack?

**MGen Christian Rousseau:** Thank you very much for the question. It's a very important one in terms of how the history of warfare develops. It's exactly there.

In agrarian days when we were soldiers or farmers and the aim of war was to actually capture land, it was because that's how you made money. Land was how you made money. Now that the economy has moved, how you make money is through dealing with information and exchanging information. Having the capability to affect that is the new domain of warfare. Most militaries have recognized this, that to be able to prosecute war or defend against any war or attack, there needs to be a cyberdomain.

As you mentioned, some countries have that specific doctrine. For Russia and China, it's actually written in their doctrine; there's no secret about it. They've worked very hard to invest a significant amount of resources to do it, so we need to do the same thing in terms of being able to defend against that. The component of what becomes offensive, what is counterattack, and all of this, is still an evolving part of a warfare domain doctrine. That argument still happens in western countries. In terms of developing our doctrine into this, not just Canada, but the rest of the west is not as far advanced as Russia or China would be.

**Ms. Jill Sinclair:** Mr. Chairman, perhaps I could add a brief comment. Thanks again for that question.

I'd just like to broaden the context a tad, and Artur may want to add to this.

We tend to talk a little bit more about cyberincidents than attacks. Again, I work at the Department of National Defence, and I don't want to sound like I'm not concerned about defence. I am. But not every incident is an attack and not every attack requires a military response.

The thing about cyber, of course, is that it's so complex. Where does it come from? What's its intent? Is it simply a modern variation on a theme of spying? That doesn't make it any better, but there are a couple of old professions in the world, and spying is one of them. The question is, how do you best deal with that? How do you make your systems robust? How do you take preventive action? How do you mitigate that if indeed you do believe you're under any sort of attack? As you say, it can come from a non-state actor or from a state actor. It can come from a company too. There's a lot of diffusion in cyberspace.

I don't know, Artur, if you'd like to add to that.

● (1145)

**Mr. Artur Wilczynski:** I've just a couple of things to add. Part of my responsibility is to also look from a threat perspective, in terms of threats to our missions abroad, and cyber threats to our missions abroad are one of the things that we have.

I completely echo what Jill just said about not always being able to see who that actor is. The importance here quite frankly is to make sure that you have the policies, practices, and capabilities in place to defend and protect your information against those kinds of attacks. Part of that means working in partnership with close partners and allies on that. For us, a key element of that is our relationship within the Five Eyes community, to work very closely, to share capabilities, to share information about intent, and to make sure we can protect our systems and protect our information from the actors that you've identified.

**Mrs. Cheryl Gallant:** Thank you.

What capabilities do our sovereign forces have in place to detect, and if necessary, deter submarines that are beneath our Arctic ice?

**MGen Christian Rousseau:** The way we track submarines starts well before they are anywhere close to Canada. We try to keep an eye through imagery and other means if they are in port, and that's usually even something like Google Earth. You can probably find something like that. Once they move, then we try to track where they go. In terms of our situational awareness of where the submarines are, we have a fair idea of where that goes. Of course, the right to innocent passage for submarines, for any vessels that are on the surface, is not the issue at play here. I think what you actually mean are submarines that would be submerged to do that.

With our allies, there are capabilities to track some trigger points in the oceans where submarines cross. In terms of being able to say where those are and how the technology works, it would be a bit difficult to do here.

**Mrs. Cheryl Gallant:** Do we defend this through our allies? Is it not sovereign assets that we have to meet the full requirements of this?

**MGen Christian Rousseau:** The best way to do this is to actually see when they leave the port and as they go in specific constraining areas in the ocean. you know that they were there. It is a system of systems that we participate in.

**The Chair:** You're out of time, Mrs. Gallant.

Ms. Murray, please.

**Ms. Joyce Murray (Vancouver Quadra, Lib.):** Thank you for being here and giving us information. I find this very fascinating and educational.

The two key threat areas are around the Arctic and cyber. That's what we were told at a previous committee. We're hearing here that the threats to the Arctic are not military in nature currently or for the foreseeable future. Can I extrapolate from that to assume this is not seen to be a concern in terms of the defence of Canada and North America, military threats whether they be in the Arctic or elsewhere?

**MGen Christian Rousseau:** If I may answer that question, Madam, we do not see a threat to the Arctic that would be different from a threat to the rest of Canada. There is nothing except for its pristine nature and all of this, but there is no reason that a foreign actor on the military side would attack the Arctic or the rest of Canada.

**Ms. Joyce Murray:** Okay, you were talking about the threats are other things, and you mentioned illegal immigration—

**Mr. Artur Wilczynski:** Transnational crime.

● (1150)

**Ms. Joyce Murray:** Could you tell me what are the top five?

**Mr. Artur Wilczynski:** From our perspective when we're looking at threats to Canada, there is a wide range whether it's things such as terrorism, illicit trafficking of drugs, whether it's human smuggling, weapons smuggling. There are a number of threats to Canada that don't necessarily fall specifically in the military domain. They are broad threats to the security of Canada. The way we work on that is again that whole-of-government approach.

**Ms. Joyce Murray:** I just wanted to know what the top five were, and you mentioned a number of them.

In terms of maritime security and defence, is the policy that our maritime capability should be directed towards those other kinds of threats and military threats are not as...? I live on the Pacific coast and of course I'm interested in what we do there, what capacity we have, what needs to be improved, and what the impact is of having a supply ship that is probably kaput and may not be replaced for 10 years or so.

Anybody can speak to those.

**MGen Christian Rousseau:** If you don't mind, I'll start with your question.

Military capabilities are developed to respond to the worst-case threats, so attacks on North America, attacks on Canada. I said that there are no such threats today, but as I mentioned before, sometimes intent changes very quickly. There are countries that have capabilities that have no intent of threatening North America but one day could and in the past have. That's why we develop those military capabilities. You can't just invent them overnight.

Having those capabilities in a whole-of-government approach, sometimes those capabilities can be used in support of other government departments that have other mandates. This is how this actually works out. This is why the MSOCs, the marine security operations centres, allow us to have visibility of what goes on around North America for—

**Ms. Joyce Murray:** Are those adequate for our needs, or what needs to be improved?

**Ms. Jill Sinclair:** If I might, Mr. Chairman, thank you.

Back to the broader issue of what the threats to North America are and how you defend, it becomes this amalgam of all the government departments. Some of the threats would be environmental. Some of them are going to be illegal migration, and all of those things.

In terms of what we have and what needs to be improved, maritime domains are increasingly important and maritime domain awareness is increasingly important. NORAD, for example, which started off as an aerospace warning, actually encompassed the maritime domain awareness. NORAD now looks out also in terms of the maritime domain awareness to be able to track what's coming into North America, the issues you'll know being on the coast, container ships and those sorts of things. What it really requires is this close partnership with the lead civilian agencies, because so many of these things have to do with coast guard surveillance, or they have to do with your transport department.

**Ms. Joyce Murray:** I have another area of questioning I'm interested in, so thank you for that. It's a big topic, and very concise answers.

We keep hearing about all of the departments collaborating. I was on the health committee when there was the H1N1 virus. We learned there were 12 departments, or there were a lot of departments with different responsibilities all collaborating. It turned out that it was pretty chaotic and that there was no one in charge, so it was not clear what everyone's role was. It was a whole lot of expenditure of time and effort to try to cooperate without a clear structure. One of the challenges with that, of course, is budget, because it takes more money and time to set those things up.

With the budget cutting that's happening now, which is, according to one defence analyst, a $30-billion downfall from where we would be today under the defence strategy, is that impacting the ability to optimize cooperation? Can you speak a little bit about whether it's optimal now, perhaps? I doubt it, knowing organizations. What are the key things that are needed to have that collaboration be more effective?

● (1155)

**Ms. Jill Sinclair:** Thanks for the question. We're always trying to optimize cooperation. That is absolutely the right terminology.

One of the things that might be a little different than, say, the health domain is that the organizations here and agencies, whether it's Canada Border Services Agency, Transport Canada, Defence, Foreign Affairs, there is a little bit more of a history of exercising. One of the key things that you have to do is not just wait for the crisis, but to practise well in advance. I think we have advanced a lot in terms of learning lessons on how we respond to certain crises, and that is how we work in response and in support of civilian agencies. That's one of the things we do with our exercises up north. It's all about the inter-agency process. It isn't just theoretical, waiting for the crisis. We actually exercise that. We have terms of reference. We have established procedures that we use. We are always exercising and improving, so we always have to optimize because we're always preparing for the last crisis.

**The Chair:** Thank you, Ms. Sinclair. Time has expired.

That completes the opening round of questioning. We'll now go to the second round with five-minute segments.

We'll begin with Mr. Williamson, please.

**Mr. John Williamson (New Brunswick Southwest, CPC):** Thank you to the witnesses for being here today. Your testimony has been very interesting, and very informative as well. In fact, you've covered a number of my questions.

I have a brief question for the Department of National Defence. I wonder if perhaps you're downplaying a little bit the rising importance of the north and the challenge this country is going to face given not only the fact that the shipping lanes are going to open up and more ships will be in the north—I'm not just talking about sailing between Canada and Russia—and potentially coming through what we perceive and we claim rightly to be our territory. Coming through Canadian territory, other nations will declare the right of innocent passage. My first question is about the ability to police and monitor that.

In addition, we see, for example, growing interest from militaries around the world. The Chinese are building Arctic icebreakers, for example, and the threat that's going to play, and how are we going to be there on the ground?

Ms. Sinclair, in your testimony you listed a number of areas where we've beefed up our capability, but I am concerned about the ability to have ships in the water to enforce our sovereignty, not just claim it from a faraway capital, Ottawa, but to be there on the ground to intercept ships, to be able to monitor them and intercept them if necessary.

**Ms. Jill Sinclair:** Thanks for the question.

On the importance of the north, thank you for giving me the chance to clarify, because I didn't want in any way to downplay it. In fact, I think we're all cognizant of the rising importance of the north. With climate change, conditions are changing and there's going to be more activity. What we need to do as we look at that is to ask what the nature of that activity will be.

I think what you've heard from all of us is that at the moment, we don't see the principal nature of that being of a military threat. There will be a lot more human activity, which means the chances for oil spills, environmental challenges, search and rescue, even disease and pandemics. All of that will become a new dynamic. The work the whole-of-government teams are doing all the time is designed to make sure that we're kind of ready for that in terms of civil security issues, if I might call them that, rather than military security issues. Having said that, deterrence is an extremely important part of maintaining sovereignty, so there's being able to project out, having the awareness, the ability to do the surveillance. As I said, I think that we have upped our game considerably.

There's been a lot said about the United States announcing its new Arctic strategy. They are kind of late to that game and there's no investment line in that, whereas Canada has actually been investing, because we recognize that the Arctic is us.

In terms of the challenges that you talked about, Chinese Arctic icebreakers and other things, we are investing in new capability, whether it's satellite or the Arctic offshore patrol vessels, the investment in the Canadian coast guard capability, too. It's important. In terms of ships transiting Canadian waters, we have said that as long as they ask us for permission to go through our waters and they can comply with the right environmental standards and all of that, then they will perhaps get permission and be welcome.

It's all about being aware, being able to be clear about what we expect of people, and people recognizing that the Arctic is not an ungoverned territory. There are sovereign countries that have responsibility for that sovereignty. We exercise it every single day, so not to downplay it at all....

● (1200)

**Mr. John Williamson:** General, do you have any comments to make on that?

**MGen Christian Rousseau:** I would possibly reinforce the concept of policing and monitoring, and the advance that we have made, first with Canadian technology in terms of the RADARSAT-2 that's up there now, but then the RADARSAT Constellation mission that's going to be operational in 2018, that will allow us to understand very much who transits the Arctic, and then be able to cue other resources to target and ask those specific questions. We'll be much more aware of what goes on in the approaches to North America than any other country can be.

**Mr. John Williamson:** Mr. Wilczynski, on a different topic altogether, I'm curious to know if the intelligence bureau of the Department of Foreign Affairs monitors the situation of Canadians going overseas to engage in terrorist activities. How does the department work with other departments in this regard to monitor them when they're away and of course when they come home to Canada?

**The Chair:** A brief response, please.

**Mr. Artur Wilczynski:** We don't have an intelligence gathering function so we don't monitor Canadians, period. What we do, though, is we are engaged in conversations with key partners, whether it's the United States, other allies, even countries of destination of Canadians who are travelling abroad for terrorist purposes, to try to get a better understanding of the phenomenon, to work in partnership to share information through our legal frameworks to address the threat they pose, particularly when they return.

This is one of the areas where we work very closely as a whole-of-government team with our security agencies, with RCMP, with CSIS, to make sure we share information about the phenomenon and put in place appropriate policies to address those challenges. Again, we work very closely with Public Safety in that regard.

It's a key element of Canada's counterterrorism strategy, to address that particular point. I participate in numerous multilateral and bilateral conversations where we exchange information about the phenomenon and compare notes about what are effective strategies to address it. It is a key component of our counterterrorism bureau.

**The Chair:** Thank you, Mr. Wilczynski, *et maintenant Monsieur Larose.*

**Mr. Jean-François Larose (Repentigny, NDP):** Thank you to our guests.

I have three areas of questions, so could you make your answers brief since we don't have much time.

Concerning the Arctic, considering the ships that are going to be built will take a long period of time, and 15 to 20 years from now we have no idea what's going to be happening, what have been the alternatives put on the table and looked at?

I understand the capacity for cooperation, which generally can take a certain amount of time, but when it comes to rapid intervention, what has been looked at?

There have been suggestions to

[*Translation*]

to arm the Coast Guard and to see if the ships that are already available could be bought.

[*English*]

Is that being looked at so we have a strong capacity quickly?

**Ms. Jill Sinclair:** In terms of the capacity you're talking about, I'm not sure if you mean just militarily or more broadly.

**Mr. Jean-François Larose:** More broadly.

**Ms. Jill Sinclair:** More broadly then. Certainly you're right. Things take a while to come online. That's where cooperation is so important, because as we look at some of the immediate challenges —and this isn't the purview of the department of any of the folks here—say the environmental issues for example, cooperation is absolutely essential.

This is an austere environment. It requires very highly specialized techniques. Some of those techniques are actually found in, say, Finland or Norway, or other countries. In that sense there is cooperation.

We have an Arctic SAR treaty, Arctic search and rescue treaty, which actually Canada helped facilitate. It was the now Chief of the Defence Staff who negotiated it for Canada, recognizing that if we're going to respond to those challenges, we need to do it in partnership with others.

**Mr. Jean-François Larose:** Okay, but in that cooperation it doesn't mean we have.... There is no one commander who dictates the schedule of the cooperation of where the navies are, where the helicopters are, or whatever. If they happen to be there because we have cooperation, they may be able to intervene. We're talking about the Arctic here.

Is there anything else we're looking at so we have something a lot quicker?

● (1205)

**Ms. Jill Sinclair:** The exercise regimes are extremely important. You have the domain awareness. You're looking out to try to anticipate if there's going to be a problem or a crisis. Obviously, that's a little bit of what Christian was talking about, queueing the resources, so if you have a sense that there's a ship that's floundering or something that's coming in that's going to create a problem, and actually having those relationships in place so you can pick up the phone, or do whatever it is immediately to get the assets where they are required. That's exercised on a pretty regular basis.

There's no substitute for sort of 24-7 coverage everywhere, but it's the most practical way of—

**Mr. Jean-François Larose:** For now.

**Ms. Jill Sinclair:** —trying to figure out exactly how to mitigate the threat while being ready.

**Mr. Jean-François Larose:** Major-General, you mentioned actors, and I thought that was very important. I think the complexity of actors when it comes to the different threats that can exist, whether they have the capacity or the intent of using it.... You mentioned countries, but I think it's getting more and more complex where it's small groups, even criminal groups, that have military, or associations with terrorist groups. The complexity is there.

Do you think the threat would be more ballistic or in any other form? What's generally on the table in terms of nuclear, chemical, and even EMPs we haven't seen but could eventually be there? It could be in a suitcase, or in a van.

Is it more the probability within the capacity that's there than actually a country building up an armament with diplomatic intent?

**MGen Christian Rousseau:** It's a very important question, because whereas most of the complex threats emanated at one point from nation states, from states that could build it, some of it now could migrate to less capable nations, or even groups, as you mentioned.

For weapons of mass destruction, including chemical weapons, biological weapons, and nuclear devices, we track very closely who produces those and where they could be proliferated, in what other parts of the world. We do that with others to make sure....

**Mr. Jean-François Larose:** Where would the best investment be put? Would it be in diplomacy, other types of detection, or to pour in billions of dollars within the American program for BMD? We do not know if they function properly, they haven't been tested, and they don't have that many either.

**Ms. Jill Sinclair:** If I might, Mr. Chairman, it's always hard to know where to invest, but I think prevention is what you really want to do. When you look at things like whether it's ballistic missile technology proliferation, nuclear weapons capability proliferation, chemical, biological, Canada is a member of a number of arrangements that work with a large number of international partners to try to track and prevent sensitive material getting into the wrong hands. That includes state and non-state actors.

My own sense would be that prevention is always going to be the best way, which probably lies a little bit more on the diplomatic side, but there are what are called supplier control regimes that deal with missile technology control regimes. There is one to deal with the precursor chemicals for chemical weapons. Canada has a strong voice at these tables.

**The Chair:** Thank you very much, Ms. Sinclair and Mr. Larose.

Mr. Norlock, please.

**Mr. Rick Norlock (Northumberland—Quinte West, CPC):** Mr. Chair, through you to the witnesses, thank you for being here this morning.

I only have five minutes. I wish I had five hours. I'm going to concentrate on a couple of areas, and I ask these questions as if I'm speaking to the folks at home. In other words, through you to them.

What I usually tell folks is Canada has the same population and gross domestic product of the State of California, yet we have the second largest land mass in the world, and probably—I believe it is—the largest coastline in the world. We have to make use of all our assets. I was very happy to hear about the marine security operations centre and the way Ms. Sinclair explained it. Thank you very much for that because we have to keep in context our ability as a nation to afford the things and to do the things that we want to do.

What really struck my interest, thinking back to the cold war, was when you talked about the right of innocent passage. I recall during the cold war—and this is with a view to our Arctic and Ms. Sinclair saying provided somebody asked for permission, etc., in our waters—the Soviets would have an innocent looking fishing boat which really had radar or electronic eavesdropping, etc.

When we talk about the right of innocent passage, could you be succinct in explaining what it is and how you believe we can overcome some of those old...? Somebody may say this is just an oil tanker or a fishing boat going to look for northern cod or whatever fish is up there. Working with our allies, how do we approach that issue?

● (1210)

**MGen Christian Rousseau:** Thank you. I will start and you can jump in if you want at one point.

I mentioned the right of innocent passage in the context of submarines. If submarines are submerged, that's not considered innocent passage. They have to be sailing on the surface.

**Mr. Rick Norlock:** If I could just interject, but we do know that the surface is usually frozen at least half the year.

**MGen Christian Rousseau:** Yes. As we relate back to the Arctic, when ships do go into the Arctic, that ask permission, whether we think they're covert for something else, that fishing boat with lots of antennas, we have a fairly good idea of what is actually on that boat. We do track specifically where they would go and what they would be doing, and particularly if they're close to Canadian Forces operations, that also tips us off. That doesn't make it into the press every time somebody comes, but we have a very good idea of what goes on, who goes through the Arctic even if they pose as fishing boats.

**Mr. Rick Norlock:** Thank you very much.

Ms. Sinclair, your being the ADM, I think this question would be best put to you.

We have a very strict acquisition regime in this country. We were talking about the lag time for a ship to replace another ship. We all know what has transpired very recently with trying to get shipbuilding capacity back into Canada by purchasing ships that are made in Canada.

When people try to intimate that it takes 10 years to get a ship, well it does take quite a long time to do that because of all the rules we've set up around it. We might be able to go out in a year and a half—well, a year and a half is a bit too short, but two to three years—and buy an off-the-shelf ship that might meet somewhat our standards, probably not [*Inaudible—Editor*].

Could you address some of the reasons surrounding the acquisition of certain types of ships, and what Canada's policy currently is in acquiring those ships? Could you also address the time requirements?

**Ms. Jill Sinclair:** Mr. Chair, let me apologize in advance that I'm not the assistant deputy minister for materiel, who could give you a very detailed answer, but I will give you a general answer on that.

First of all, you talked about the long lead times. One of the interesting things in defence procurement, of course, is that with the help of people like General Rousseau, we try to project what the security environment is going to be 20 to 40 years out, because you need to be able to plan a long time out. Every military in the world keeps its equipment for a long time. It's expensive and it actually has a very long shelf life. You can continue to modernize the systems and keep those things floating and flying and doing what they need to do.

Defence procurement is highly complex. It requires many years to try to determine what the capabilities are that you require, and you challenge that: Do you really need all of that? Are you really looking at the future security environment? This is just to tell you that the overall time in any nation's procurement strategy is very long.

In terms of Canada, I would briefly say that on the ship front we had the national shipbuilding strategy, which was designed to situate Canadian shipyards, Canadian industry, and to give the Canadian Forces the capability, the Royal Canadian Navy the capability that it needed, by getting out of the boom and bust cycles, giving a bit of a heads up to industry to say that this is what we need and this is where we're going to invest. I think people are familiar that we have a Vancouver shipyard and we also have Irving. Between them they are working on the fleets of ships that we need for the next number of years.

In addition, I would just mention the government's announcement of the national procurement strategy, which is designed, again, to make sure that we get the folks of the Canadian Forces the capability and the equipment they need, but in a way that makes that investment real and brings it back to Canadian industry and builds Canadian jobs.

**The Chair:** Thank you, Ms. Sinclair. Time has expired.

Mr. Harris, please.

● (1215)

**Mr. Jack Harris (St. John's East, NDP):** I apologize for not being able to be here to listen to your presentations. I was giving a speech in the House of Commons, but I am glad to see you both here.

Thank you again, Ms. Sinclair, for coming to our committee. My first question is for you.

Canada-U.S. relations start with the Ogdensburg agreement, the so-called treaty by press release of five sentences.

You do note that the joint defence board—they tell us someone in the U.S. called it the peanut butter and jelly board, or something—the Permanent Joint Board on Defence still seems to be the major interactive group here on the, and I don't know if the official level is the right way of putting it, but certainly on the military and policy levels. You indicate there are 800 separate arrangements of one sort or another. I'm not sure we'll be able to review all them, Mr. Chair, for our defence of North America. It seems that we have a very complex relationship with the U.S.

The PJBD seems to be still operating as the prime relationship. How many members do we have? I gather MP Laurie Hawn is one member. I don't know if he's the senior member for Canada. Who else is on that board for Canada?

**Ms. Jill Sinclair:** Thank you for the question on the Permanent Joint Board on Defence. It was Bob Gates who called it the peanut butter and jelly board.

The PJBD since 1940—it just shows what a succinct press release can do—generated quite an extraordinary relationship. We are now on, I think, our 232nd meeting, which will take place in June. It is actually established by the President and the Prime Minister, so it's at that level. They designate co-chairs. On the Canadian side at the moment Mr. Hawn is the Canadian co-chair, and a gentleman by the name of Mr. Spratt is the U.S. co-chair, both politically appointed.

Beneath that I chair it in support of our co-chair with my U.S. counterpart. We have a number of participants from the Department of Foreign Affairs, the Privy Council Office. We have a very rich range of military representatives at that table. We have in the last number of years.... I was proud to say that I brought in public safety, the coast guard, to reflect this broader approach to the defence of North America that we need to look at, to make sure we didn't miss any dimension of how we looked at the security of North America.

It meets on a regular basis. The 800 arrangements you point to go from very detailed, how we buy and sell fuel for each other to much more strategic ones. I think it's very complex because our relationship is very deep and long-standing.

**Mr. Jack Harris:** Thank you.

I'll follow up on Mr. Norlock's point that, of course, we have a long coastline and vast territory. Do you see there being any challenges with respect to domain awareness by Canada of our half, or more than half, I guess, of North America, from a defence perspective?

**Ms. Jill Sinclair:** If I might, Mr. Chairman, I'll answer and maybe General Rousseau will want to jump in. I mentioned previously—sorry, Mr. Harris—one of the interesting things was that NORAD expanded to look at maritime domain awareness too, which is very good because that brings the combined resources of Canada and the United States to that effort.

In terms of looking out, we also have our marine security operation centres on the east and west coasts, and also in the Great Lakes area. If we look to the Arctic, for example, we have manned overflight and surveillance and stuff at the moment. We will be launching in 2018 RADARSAT Constellation, which will give us visibility four times a day on the Arctic approaches. I'm not sure that a military person would ever say you have enough domain awareness, but certainly we're investing, and I think we have a pretty good sense of what's going on.

**Mr. Jack Harris:** Thank you.

You mentioned the maritime surveillance. I'm going to ask a somewhat pointed question to General Rousseau. Did Sub-Lieutenant Delisle work for you? Well, whether he did or he didn't, I guess it was suggested that the events and his action didn't do any harm to our relations to our friends in the Five Eyes. I don't think I believe that. Can you tell us what has been done? What assurance can you give that this kind of thing can't happen again? It seems to me it was a rather amateurish effort on Sub-Lieutenant Delisle's part that allowed him to obtain information and share it with the Russians.

● (1220)

**MGen Christian Rousseau:** Thank you for your question. I think it's a very important one that goes deep into the business of intelligence.

Sub-Lieutenant Delisle, or Mr. Delisle now, did not work specifically for me, but was an intelligence officer who worked for the Royal Canadian Navy.

Intelligence is based on sharing of information that doesn't happen if there is not trust. The Delisle event did put into question the trust in the same way as some of the other allies when they had issues of insider threat causing questions about trust.

In the sharing arrangements and in the way we deal with information, there were some evolving changes we had started to do that were not completely done, which allowed Mr. Delisle to do some of the spying and passing of information that he did.

We have continued those efforts of making our systems stronger, more robust, and completely...with our allies too. Our allies have also had issues of insider...coming out. Together we're working on the best way to do that, so absolutely, we're working to make the system better.

**The Chair:** Thank you, General. Time has expired.

Mr. Bezan, please, for five minutes.

**Mr. James Bezan (Selkirk—Interlake, CPC):** I want to thank the witnesses for sharing their knowledge and expertise with us today in our study on the defence of North America.

General, when I'm looking at your testimony today, you talk about the definition of a threat, and that having the desire to harm Canada but no capabilities to do so does not represent a threat from that entity. You go on to say that you do not see a state actor that has both the capabilities and intent to harm Canada militarily.

I look at some of the things that are happening in the world right now and at special forces that are being used by some international players. I look at Iran with their Qods force and the fact that they've moved them into Syria and other areas to cause destabilization. They often carry certain capabilities with them. Definitely they can easily integrate into a civilian setting and cause a great deal of harm.

I'm just wondering if in the intelligence-gathering systems that the Canadian armed forces deploy, along with the whole-of-government approach that we have with other players both internationally and within the domestic context, if we're looking at actually military people using terrorist-type approaches when dealing with our own national security.

**MGen Christian Rousseau:** Thank you very much for the question, sir.

I specifically referred to a state posing a threat to Canada. There are terrorist entities that would like to harm Canada, whether it's by a military threat, an asymmetric threat or a threat to safety. The way we organize the definition is not relevant, because in the end, for Canadians it will have an impact.

The groups that at one point would have been part of a state or even have been supported clandestinely from a state would potentially represent espionage threats or other threats, but a military threat of invasion of Canada or of harm to Canada does not exist presently.

**Ms. Jill Sinclair:** Mr. Chairman, if I may, I would like to say a word, too.

I think what you've pointed out here is a confluence of actors and interests in the contemporary security environment that is very worrying, because non-state actors, terrorists work with states, states work with terrorists, money funds everybody, and those lines are much more fluid. In looking out at our interests and the defence of Canada, we're conscious of those flows. This consciousness relates to everything, from how we do financial tracking to how we list terrorist entities that we know are state-sponsored.

Artur.

**Mr. Artur Wilczynski:** On that, here are a couple of things.

One is that the government passed a number of years ago the Justice for Victims of Terrorism Act, which identified state sponsors of terrorism or called for state sponsors of terrorism. The government identified both Iran and Syria as state sponsors of terror.

In terms of the kinds of actors who are out there and the type of action that we take, we have focused on a number of threats from that perspective. The specific organization that you mentioned, the IRGC Qods force, is actually a listed entity under Canada's Criminal Code as a terrorist organization. We approach that threat using other instruments, whether it's policing, intelligence services in Canada, or engaging with partners to address that specific threat.

● (1225)

**Mr. James Bezan:** I'll follow along that line of thought. We have talked about drug trafficking. The Canadian Forces have played a major role in drug trafficking, especially in what we've seen along the eastern coast of Africa. HMCS *Toronto* just had a very successful mission there. She captured a number of shipments of narcotics that could actually have gone into funding terrorism.

Look at what's happening in Mexico and in the North American context. There is a lot of activity happening there and definitely there's a lot of work up and down the coastline. What are we doing, and on that basis, how do we perceive this as a potential threat to the Canadian situation?

**Ms. Jill Sinclair:** Mexico is a key partner for us. Clearly, they have a very difficult and challenging situation, which unhappily they share with some of their neighbours, too. If you look at Mexico, Guatemala, Belize, we all track it. Public Safety does it principally, but we keep our eyes on tracking the location of the funding and where the organizations are.

We're increasingly working with Mexico. Again, this is much more Public Safety's lead and the work of the RCMP. Foreign Affairs does work here too.

Canada established with the United States two years ago a trilateral defence ministers table. The next meeting of the trilateral defence ministers will take place in Mexico City next month. This is an opportunity where we sit down and look at what their security threats are and what ours are, too. Clearly, the flow of drug trafficking, the money, everything that it generates that is a negative for our society is on our agenda, even if it isn't strictly a National Defence lead.

**The Chair:** Thank you, Ms. Sinclair.

The time has expired.

We'll go to Mr. Harris for five minutes, please.

**Mr. Jack Harris:** General Rousseau, I'm interested in the question of cyberactivity. I just briefly looked at your opening remarks, so I don't know whether this has been dealt with before. I believe your presentation was that from the military point of view, your work is to ensure that military assets are defended against cyberattacks so that you could carry on in the event of an attempt to compromise your ability to operate as a military force.

To what extent can you assess that as being necessary? Do we have other actors who are actively pursuing the creation of offensive cyberactivities, and what is the extent of it? Are we worried about it? Do we know that there are actors who are developing that capability?

We are told that the Americans have an offensive cyber command that is exploring that sort of thing as well. I take it, first of all, that we don't at this point, but can you tell us which actors do have cyber capability or are developing them for use as a weapon in conflict?

**MGen Christian Rousseau:** Absolutely, sir. Thank you very much for the question. We did touch a bit on it before, but this will allow me to put more definition to it.

Actually, most militaries recognize cyber as an important domain to be cognizant about, to understand, to at least defend, if not use in an attack. The countries that are most advanced in this understanding of cyber as a potential area of warfare are Russia and China. They actually have doctrine that talks about how they would use cybertools to dislocate enemies or adversaries before they would attack. We've actually seen some of those in action in past conflicts. Not only have they developed potential tools, but they've developed specific doctrine on how they would use these tools to attack.

**Mr. Jack Harris:** Would that include just military targets, or also disrupting civilian operations, such as finance, etc.?

**MGen Christian Rousseau:** My most immediate concern is how they would disrupt our ability to command and control, but any disruption to the power grid, or anything like that which would stop us from being able to operate in the environment that we are in would also be of interest. Certainly those tools are being explored as possibilities by those countries. They certainly talk about it as part of the doctrine of how they would use cybertools.

● (1230)

**Mr. Jack Harris:** Can we defend against that? How good are you at defending it?

**MGen Christian Rousseau:** Certainly, in terms of defending our networks, the networks that we operate, we have quite a good understanding of what enemy capabilities are. We think we can deal with those attacks or events as they would arise.

One of the distinctions we talked about a bit earlier was, what is an attack? What is just looking, inspecting, spying? We are under constant spying, if you will, or attempts to get into our networks to try to map them. We note that and we react to that also.

**Mr. Jack Harris:** Do you have a big capability in terms of manpower, or budget for that?

**MGen Christian Rousseau:** There's the capability in terms of understanding what goes on in our networks now and what we think we would need in the future. The capability to defend our systems now, I think, we're quite good at, but we do recognize that in the future we would need to look at that.

I'll pass to Ms. Sinclair in a second, but we have, in our fourth development, looked at how we would beef that up.

**Ms. Jill Sinclair:** I'll just say a quick word, Mr. Chairman, and that is to say that looking forward, one of the things the Canada First defence strategy refresh will look at, in particular, is cyber. This has obviously emerged since 2008 as much more serious. We recognize that cyber is now another instrument in the hands of states and other non-state actors who would like to take advantage of whatever element of Canadian systems or societies, whether it's military or whether it's civilian or whether it's business.

In terms of the current capacity, we have a couple of hundred people who are working on that. We work very closely in a whole-of-government context here to detect when there are threats, to look at the mitigating responses. Obviously, the CF has a particular responsibility for protecting and making sure that we are resilient against those sorts of attacks so that we are there, available as an instrument of the Government of Canada to deal with challenges as they arise.

**The Chair:** Thank you, Ms. Sinclair.

This is our final five-minute question segment. Mr. Bezan.

**Mr. James Bezan:** I just want to follow up on the discussion on cybersecurity. Professor Sloan from the University of Ottawa was here on Tuesday. She made a suggestion that we should actually have a cyberdivision within the Canadian armed forces, along with the army, navy and air force. I want to get your feedback on that. Right now you say Public Safety is the lead. With cyberwarfare, it's not just about defending against attacks, but something you have to counterattack. That becomes very much a national defence issue and not public safety. I wanted to get your feedback on that suggestion.

**Ms. Jill Sinclair:** Thanks for the question.

Cyber is an emerging domain, and I think all countries are trying to figure out the best methodology for dealing with it. The United States is almost pretty much, I don't want to say alone, but singular among the allies in having a stand-alone cybercommand as such militarily. They structured themselves in quite a specific way. Almost all of the other countries and partners that we deal with have a variety of public safety or homeland security kinds of leads, working with their foreign ministries and working with their defence institutions.

I think the question is, how can you best posture your country to be able to defend and respond to cyberattacks?There are a lot of different ways of doing it. At the moment I think we've determined that cyberincidents...if you put a strictly military lens on everything that happens in cyber, you will be looking at a strictly military response. The fact is, at the moment most cyberincidents are designed to spy; they're designed to disrupt; they're designed to do all sorts of things. Understanding the intent behind them, and then determining the best instrument of government to respond to that is extremely important.

At the moment we feel that what we have through the Canadian Forces in terms of identifying where the threats are coming from, protecting our systems, being able to provide that expertise to the whole of government to be able to mitigate...working with close partners.... The United States is a key partner here when it comes to things like critical infrastructure in cyber, and NORAD even looks at cyber now. That's part of how we're dealing with it.

I don't think anybody has found the perfect method for it.

● (1235)

**Mr. James Bezan:** You mentioned NORAD, and I want to come back to RADARSAT. The Constellation is supposed to be up and running for 2018. Does that make the radar array we have there obsolete, or do we still have to have land-based radar systems to work in collaboration with RADARSAT?

**Ms. Jill Sinclair:** I think that from a defence military perspective you always want systems to systems and you want redundancy. Having the satellite there is going to be fabulous, but you need every other bit along the way too, so that you have that redundancy in something as sensitive and important as Arctic surveillance.

**Mr. James Bezan:** Under the Canada First defence strategy, we've already made some strategic investments. What further investments are we making under the current Canada First defence strategy, and then as we move forward with the reset on the Canada First defence strategy, what future investments do you foresee?

I'll put that to all of you.

**Ms. Jill Sinclair:** On the Canada First defence strategy, there are a number of investments across, whether it's with regard to our naval, our land, or our air capabilities. Those were all outlined in CFDS 2008.

As we look forward, we will be bringing particular attention to things like cyber and space, and also intelligence capability. What the reset of the CFDS will be is what have we learned since 2008. The world was very different. We have enormous amounts of experience coming out of operations.

We think immediately of Afghanistan and Libya, but we look at our humanitarian assistance efforts, whether they've been within Canada, helping the United States, or globally. What have we learned and what do we need to be robust and agile going forward?

I think things like space and cyber really commend themselves in that regard. It's how we can do our partnerships more effectively with key partners like the United States, our NATO allies, and others globally, because none of us will ever have everything we need to deal with the whole array of security threats, which are totally global in nature.

**MGen Christian Rousseau:** I don't think I would have anything else to add, sir.

**The Chair:** Thanks to all of our witnesses this morning for an enlightening and very important round of testimony.

**Ms. Joyce Murray:** I have a point of order, Mr. Chair.

This agenda suggests that this meeting goes until 12:45.

**The Chair:** It will take at least 10 minutes to clear the room, Ms. Murray, so—

**Ms. Joyce Murray:** I have not had an opportunity to ask a second question, whereas both parties have had many opportunities.

**The Chair:** Well, we've gone through the first and second rounds of questioning as provided, and unfortunately, today there's no opportunity for a complete third round.

I'll thank our witnesses again for your attendance here today and we will go in camera for committee business.

[*Proceedings continue in camera*]