HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on National Defence

NDDN • NUMBER 077 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, January 30, 2018

Chair

Mr. Stephen Fuhr

Standing Committee on National Defence

Tuesday, January 30, 2018

● (0845)

[*English*]

The Chair (Mr. Stephen Fuhr (Kelowna—Lake Country, Lib.)): I call the meeting to order.

I'd like to welcome everybody to the defence committee this morning.

Colleagues, welcome back. Gentlemen, welcome.

Today we have Len Bastien, defence chief information officer and assistant deputy minister, information management, and Commodore Richard Feltham, director general, cyberspace, for our continuing discussion of Canada and NATO under the realm of cyber. Thank you very much for coming.

I'll give the floor to Mr. Bastien. You have up to 10 minutes for your initial remarks.

Mr. Len Bastien (Defence Chief Information Officer and Assistant Deputy Minister, Information Management, Department of National Defence): Thank you, Mr. Chair.

[*Translation*]

I am very pleased to be here with you this morning.

[*English*]

As assistant deputy minister for information management and defence chief information officer, I am responsible for ensuring that defence has a reliable, secure, and integrated defence information environment to support business and military operations. I am accountable to the deputy minister for administration and financial and human resources, and I am accountable to the chief of the defence staff for force development and readiness, including cyber.

The director general for cyber is embedded within my organization, and Commodore Feltham, who is with me today, will address you on this subject in more detail in a few minutes.

As you know, Canada's new defence policy represents a new vision: to be strong at home, secure in North America, and engaged in the world. As a G7 country and a founding member of NATO, Canada has a strong interest in global stability. To that end, we will pursue leadership roles and interoperability in our planning and capability development to ensure seamless co-operation with all our allies and partners, particularly NATO.

As DND's representative at the NATO consultation, command, and control board and the NATO agency supervisory board, I am here today to discuss Canada's involvement in NATO as it pertains to information management and information technology, IM/IT. I am supported by experts from across the Department of National Defence who participate in several multinational capability panels. Canada is a significant contributor to the programs that drive IM/IT policy and technical development activities overseen by the board.

Interoperability across the alliance depends in large measure on consistent application of, and compliance with, NATO IM/IT policies. There are three main compliance organizations.

The first is the North Atlantic Council, where Canada is represented by our ambassador to NATO. The council approves the consultation, command, and control policy compliance framework and mandates the NATO enterprise organizations to implement the policies and inform the council on waivers, policy changes, or new policy.

The second is NATO's consultation, command, and control board. It is the senior multinational policy body reporting to the North Atlantic Council and the defence planning committee on policy matters, including the interoperability of NATO networks and national systems. Its focus is on information sharing and interoperability, which includes cyber-defence, information assurance, joint intelligence, and surveillance and reconnaissance. Consultation, command, and control board strategy signals a commitment to deliver these capabilities and emphasizes the need for the modernization and interoperability of the force contributions of NATO nations and partners.

The third is the agency's supervisory board. It is the organizational governance body of the NATO communications and information agency and is responsive to the North Atlantic Council. The agency supervisory board ensures that the communications and information agency is set up to succeed by governing its resources and its performance. Canada has assumed the chairmanship of the board of this agency for the next two years.

The NATO communications and information agency was established in 2012 to provide NATO-wide IM/IT services, procurement, and support in areas such as command and control systems, tactical and strategic communications, and cyber-defence systems.

In April 2017, my group here in Ottawa hosted a three-day NATO industry conference where 750 experts from across NATO, nations, industry, and academia took a close-up look at NATO business opportunities and procurement specialists. It marked the first time this event was hosted in North America and it set records for its level of participation, all in an effort to give better exposure of Canadian-based industry to NATO business opportunities in our area.

In December 2017 the communications and information agency awarded the Canadian-based MDA, a business unit of Maxar Technologies, a $14.9-million contract to deliver NATO's project Triton, a maritime and control information systems project.

If I were to summarize Canada's focus in its role in IM/IT in NATO, I would prioritize information sharing and interoperability. Canada's new defence policy puts forward 111 initiatives, many of which detail positive steps to enhancing defence intelligence capabilities both at home and in the world. One of the initiatives, initiative 65, is our commitment to improve cryptographic capabilities, information operations capabilities, and cyber capabilities. We will focus on cybersecurity and situational awareness, cyber-threat identification and response, and the development of military-specific cyber and information operations.

At this time, I would like to turn over the floor for opening remarks to Commodore Richard Feltham, who will speak to cybersecurity and our contribution to NATO's cybersecurity efforts.

● (0850)

Commodore Richard Feltham (Director General, Cyberspace, Department of National Defence): Good morning. Thank you for allowing me the opportunity to speak before this committee today. I am Commodore Richard Feltham, and I am the director general for cyberspace. In this role, I'm responsible for force development of military cyber capabilities that enable cyber operations, as well as strategic and operational command, control, communications, computing, and information.

Force development identifies the necessary changes to existing capability and articulates new capability requirements for the Canadian Armed Forces. For example, our current cyber force development efforts include scoping what requirements need to be fulfilled to successfully conduct cyber operations, designing the potential solutions to meet those requirements, and then helping to build and validate capability once a solution is chosen and implemented, respectively.

To date, Canada's international cyber-defence engagement has been focused on our Five Eyes partners and NATO's cyber-defence activities. The foundational work for a future concept of overall NATO cyber-defence is being developed by the allies now. As part of this, in 2016 the allies, including Canada, made a cyber-defence pledge to enhance their national cyber-defences as a matter of priority. The cyber-defence pledge reflects our international commitment, spelling out the priorities of developing strong individual cyber-defence through facilitating co-operation in the areas of education, training, exercises, and information exchange.

Further, we have taken an active role in numerous ongoing neighbour cyber-projects and policy bodies. While a final configuration of NATO cyber-defence has not yet been built, Canada has been taking an active role in its formulation to ensure not only its effectiveness but also our ability to contribute and function effectively in its eventual formation.

While the scale of Canada's commitment has not been large, we have selected areas of activity that fit well with our strengths and lead to mutual benefits both for NATO and for our own interests. In particular, one area of Canada's contribution is through the multinational cyber defence capability delivery, or MN CD2 for short. This is a smart defence project whereby allies have co-operated to develop, acquire, and maintain military capabilities to meet current security problems, in accordance with the NATO strategic concept.

Canada has been active since 2013 in contributing representatives and financial support. In addition to the value provided to NATO, our participation directly supports our own goals, furthering the direction and outputs we have pursued under the “Strong, Secure, Engaged” initiative 65, which was referred to earlier by Mr. Bastien.

Examples of mutually beneficial projects under this initiative include the cyber-information and cyber-incident coordination system and the malware information-sharing platform, which were developed for NATO cyber-defence. Both have proven valuable for Canada.

Other areas of Canada's contribution to NATO cyber-defence are through exercises in which Canada has engaged in NATO cyberwarfare exercises primarily as an observer. Thanks to our success in building our cyber-defence personnel, however, we'll be able to send participant teams this year.

In Exercise Locked Shields, for example, we will work with teams from two dozen nations to test our abilities to detect, defend against, and investigate cyber-attacks while exercising decision-making and command-and-control procedures. The Cyber Coalition exercise will see our team challenged not only with cyber-attacks through malware but also with social media and other hybrid challenges. This will test our operational and legal procedures, information exchange, and our work with industry and defence partners.

We have further combined cyber-defence experimentation with our targeting development, using the experience and facilities offered by the NATO cyber centre of excellence cyber range in Estonia. The upcoming NATO coalition warrior interoperability exercise, or CWIX for short, will directly benefit our command and control, as well as NATO interoperability.

Finally, Canada has been actively involved in the NATO cryptographic capability team and allied cryptographic task force since 2005. We have been able to provide leadership and expertise, as well as obtaining valuable insight that has guided our own cryptographic development efforts. We have been able to build communications and networks that address our own needs and are aligned with secure and reliable communication systems operated by our NATO allies in a cost- and time-effective way.

I will conclude by reiterating that Canada's defence policy outlines a new framework for how we will implement the vision of “strong at home, secure in North America, and engaged in the world”. We will continue to be a trusted partner to our allies as we work to develop our own cyber capabilities by anticipating, adapting, and acting.

● (0855)

The Chair: Thank you, gentlemen, for those opening remarks.

I'm going to go to the first round of seven-minute questions. The first question is going to go to Mark Gerretsen.

Mr. Mark Gerretsen (Kingston and the Islands, Lib.): Thank you very much, Mr. Chair.

Thank you, gentlemen, for coming before the committee today.

I'll leave the question open to either of you, whoever would like to answer. You talked about Canada being a significant contributor to the programs that drive the IM/IT policy and technical development activities in NATO. Can you elaborate on the importance of Canada's contribution, perhaps with some concrete examples or concrete ways in which Canada's contributions help to accomplish the NATO objectives?

Mr. Len Bastien: Thank you for the question, Mr. Chair.

We do participate actively in NATO. Let me explain the constructs of how and where we participate.

You may have heard of the term “within the NATO construct”, and I'll define our contributions within that construct. There are also entities that contribute to NATO that are not within the NATO construct. For example, the NCI Agency I referred to is actually outside of the NATO construct. It was created in 2012 and was put outside the NATO construct deliberately so it could behave with a little bit more agility and more like an industry service provider. That came with hand-offs and exchanges around how our contribution gets calculated, because it is actually outside the NATO construct when it comes to looking at credits like flags to posts and our ability to work within the NATO construct.

Let me give you some numbers. Within the NATO construct, currently National Defence is contributing over 200 positions at a fill rate of about 96.6%. We are very active and very committed to filling our positions within the NATO construct.

Outside the NATO construct, our contributions are measured in approximately 120 to 130 positions that participate in activities in direct support of NATO operations or NATO support services, just by way of example.

Financially, the contributions are again spread across the different constructs of NATO. Let me see if I can give you some more detailed examples.

By way of example, in 2016 Canada's cost share of NATO was about 6.6% overall. In terms of funding for something like the agency, Canada was contributing about $20 million, and another $20 million was being contributed to the military budget. There were two contributions, in terms of the way you would add them up, but one would be inside the NATO construct and the other would be outside.

In terms of CIS support, which was part of the agency in 2018, the budget allocation was about $48 million. Canada's portion of that amount in 2018 is approximately $3 million. The agency needed, across the partner nations, about the first amount, and Canada's contribution is anticipated to be about $3.1 million, by way of example.

Mr. Mark Gerretsen: Because I have limited time, I want to switch to interoperability among the NATO allies. I know that a lot of it depends on adherence to and consistent application of the NATO policies. Can you give some perspective as to where NATO allies, and more specifically Canada, are being compliant with the policies?

● (0900)

Mr. Len Bastien: Thank you again for the question, Mr. Chair.

NATO compliance with policy, governed by the command and control NC3 board—one of the boards I described—is governed by the board itself. I think the best example of compliance would be the cyber pledge that my colleague referred to. It's a cyber pledge committed to by the partner nations, through which, basically, nations have signed up to commit to a certain level of cyber-hygiene that will allow us to interoperate together with the confidence we need to work and—

Mr. Mark Gerretsen: We've signed up for it. How are we actually doing? Are we there?

Mr. Len Bastien: Richard, I'll defer to you.

Cmdre Richard Feltham: Thank you, Mr. Chair.

To add some data to that point, here's a concrete example of how Canada is involved in NATO policy and structures.

The FMN, the federated mission network, is not necessarily within NATO but is supported by NATO in its overall structure. We deployed a network to Latvia recently that is consistent with those standards and protocols. I think Canada is leading in that respect by demonstrating the deployment of a deployable network in adherence to NATO standards. That's a good, positive example.

Mr. Mark Gerretsen: That's what I was looking for. Thank you.

What about other allies?

Cmdre Richard Feltham: I cannot comment on the progress of other allies within that domain. My apologies.

Mr. Mark Gerretsen: How much time do I have?

The Chair: You have about a minute.

Mr. Mark Gerretsen: On the same theme, can you talk about the benefits of making sure that interoperability is maintained? How important is it?

Cmdre Richard Feltham: No matter what operations we look at, whether military or non-military, the key to any successful operation is communication. More and more of our communication is done via network and data. If we can't interoperate with our allies, it gets harder and harder to communicate with and control our military forces. Our ability to operate with our allies, both within the Five Eyes community and the NATO community, is of the utmost importance to us. We've put a lot of emphasis and time into ensuring that we're able to do that. That's one of the primary goals of all of the working groups that Mr. Bastien referred to: ensuring interoperability. I cannot overstate the importance of that.

Mr. Mark Gerretsen: It's critical, therefore.

Cmdre Richard Feltham: Yes. It's critical.

The Chair: Mr. Paul-Hus, welcome. The floor is yours.

[*Translation*]

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): Good morning, gentlemen.

My question concerns not only Canada, but NATO and all of its member countries. What kinds of cyber-attacks are being carried out currently? Are certain countries conducting cyber-attacks? What types of cyber-defence should we use?

Mr. Len Bastien: Thank you for your question.

[*English*]

If I understood correctly, you're interested in learning more about the kinds of attacks or cyber-threats that we manage, whether nationally or within our alliance with NATO.

[*Translation*]

Mr. Pierre Paul-Hus: From the perspective of the global NATO framework, I would like to know where the major threats are coming from.

NATO currently has 29 member countries, but they do not all have the same capabilities. Certain member countries are probably victims of cyber-attacks on a more regular basis.

Can you provide any general information on that?

Mr. Len Bastien: I understand your question.

[*English*]

Let me start by explaining some of the conditions that are set out in the cyber pledge. One of the things that has been established is that nations are responsible for their own cyber, respectively. When a coalition comes together under the authority of NATO, its cyber is delivered by the agency. Therefore, I really can't speak to the integrity or vulnerabilities that may exist inside that cyber-environment.

I can speak to our National Defence cyber-environment. To that end, I can assure you that we take that very seriously and that we monitor and manage our networks with the utmost integrity when it comes to cyber-threats.

[*Translation*]

Mr. Pierre Paul-Hus: There are no borders in cyberspace. The Internet is planetary. If we function in isolation, there is no cohesion.

Our study on NATO seeks to determine whether there is cohesion within NATO and whether concerted efforts are being made. If Canada makes investments in cyber-defence or develops plans to deal with cyber-attacks and other countries do not align with those, we have a problem. We want to know if we are playing alone in the team or not.

● (0905)

Mr. Len Bastien: Thank you for the question.

[*English*]

The concept of cyber being borderless is an actuality. The biggest threats that we monitor and pay attention to come from the Internet, a network that we all interoperate in because we have to.

When we create interoperable environments with our allies, we take the same prudent approach by creating firewalls and gateways that can control the traffic such that we can monitor it and manage our equities. It's not an open network that is unfettered. To give you the impression that somehow we're interconnected with our allies without any protection would be wrong. We do a lot to manage our security inside the Department of National Defence.

[*Translation*]

Mr. Pierre Paul-Hus: Canadian troops have been deployed in Latvia. The purpose of that deployment is to have a physical presence on the ground with regard to Russia. At the same time, we know that there are cyber-attack and cyber-defence operations.

Are there a lot of Canadian resources allocated to defence in Latvia?

[*English*]

Mr. Len Bastien: Mr. Chair, I agree with that statement. With our allies, we have invested significantly in that part of the world.

I believe you were asking about what risks or threats we are worried about. Let me explain how we operate inside National Defence.

Cyber, although relatively new, is an established environment of military operations, like land, air, and sea, and as is done for land, air, and sea, the institution of National Defence prepares capabilities inside the department. I'm mandated to help prepare the cyber equities for eventual use in deployed operations.

That said, it's actually the commander of Joint Operations Command who utilizes those capabilities to operate and control his mission. I can't comment on how he's using those capabilities. I can tell you, however, that I am accountable and responsible to prepare them, to generate them, and to get them ready for his use, and we do a lot to make sure that the men and women of the Canadian Armed Forces deploy with the best possible chance of success. Our cyber equities being deployed are the best we can possibly produce for them.

[*Translation*]

Mr. Pierre Paul-Hus: I don't know if you can answer this question, but I'd like to know if Canada is currently conducting offensive operations.

[*English*]

Mr. Len Bastien: Thank you for the question, Mr. Chair.

Let me tell you that cyber-defence operations have been a part of our reality for many years. We've been doing this for a long time, with no real concerns. It's an area of expertise that we've developed and enhanced over that time. Recently, in the announcement of our policy of “Strong, Secure, Engaged”, there is explicit direction from the government to make even further investments in cyber, in cyber-active operations. That will involve the opportunity for us to use offensive cyber capabilities to enhance our mission success.

I'm going to hand it over to Commodore Feltham, because he can provide some more tangible information around what that might look and feel like.

Cmdre Richard Feltham: Thank you, Mr. Chair.

In terms of what Canada writ large is doing, I can't comment on it because I'm not there, but from a DND perspective, as Mr. Bastien mentioned, the recent policy has just given us the policy to do active cyber. That's to say that this is nascent. We are learning how to conduct this business. We are working with our partners within government and with our allies around the world in order to learn how to get into this business. I have not been involved in any offensive cyber operations to this date.

[*Translation*]

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

[*English*]

The Chair: Mr. Garrison is next.

Mr. Randall Garrison (Esquimalt—Saanich—Sooke, NDP): Thank you very much, Mr. Chair, to you and to the witnesses for being here today.

I want to start with some questions on procurement. We have discussed many aspects of procurement in this committee, but I think there are two concerns that I would like to talk about here.

Have we put in place restrictions on who can bid on contracts in the area of information management, given our concerns about cybersecurity? I know that we've had previous concerns raised about bids that might be launched by state-owned companies from another jurisdiction, about those dangers, and also about the abilities of people to put Trojan horses, let's say, or other kinds of things into IT systems. Are there any restrictions currently in place? Are you planning restrictions on who can bid on information management systems, given the problems of cybersecurity?

● (0910)

Mr. Len Bastien: Thank you for the question, Mr. Chair.

The function of procurement within the government is centralized with another department, PSPC. Within our department, it is authoritatively controlled by another assistant deputy minister in charge of materiel. I can tell you from experience that we have used the national security exemption when we're dealing with sensitive national security issues or concerns when procuring IM/IT capabilities. On the integrity of our procurement or supply chain, I would have to defer that question to my colleagues, who are the experts and the authoritative voice in that area. I don't procure my own contracts. I need to use those authorities to do that.

Mr. Randall Garrison: Surely you're consulted on the criteria that go into the contracts by those who are actually doing the procurement, so I guess I would go back to you again and ask you if you are inserting those concerns into the contract, because I think they will be a growing concern as we press forward.

Mr. Len Bastien: I can assure you that we do set the high-level requirements for the scope of the contract for the capabilities we're seeking. I can tell you that there is a significant effort to shore up our supply chain integrity within the government in general. I'm aware of that, but it is not under my control. Naturally, when setting my high-level requirements, I would obviously seek out the best and most secure capabilities needed to get what we want.

Mr. Randall Garrison: I guess my question, then, is more general. When you talk about high level, it sounds as though these are exceptional circumstances. My question goes to the more basic circumstances of allowing, through procurement, portals to be created that would allow access to our information.

Mr. Len Bastien: I can see why that language would have given you that impression. I can assure you that although I mentioned high-level requirements, it's not taken for granted that...

We're significantly aware and involved in making sure that the capabilities we are procuring are compliant. There are many checks in place, not only during the procurement process but also during the design and implementation, to make sure that the integrity of the capability we're procuring does not create a risk or a threat for national defence.

Mr. Randall Garrison: Thanks very much.

I want to ask a second question about procurement, which came about in kind of a strange way in my riding. I met with a constituent who is having trouble, as a small business owner, with intellectual property law in Canada and the ability of companies to retain ownership and control of, in this case, information technology.

I wonder if we're running into that problem when it comes to our efforts in cybersecurity. Certain of the large corporations try to retain control and ownership in ways that restrict the use of the technology once it's purchased.

Mr. Len Bastien: I am aware of the situation you're describing. I have been asked as an authority and have been involved in allowing the intellectual property to be released for use by industry and in future bids. In fact, the MDA contract win with NATO is an example. They worked with my organization in the past and asked for permission to use the intellectual property that was created in their bid with NATO, and they actually won the business as a result.

I can tell you that I have experience with the positive outcome of that situation. For any other details in the area of procurement and intellectual property, I have to defer to my colleague ADM in materiel in National Defence, because that is his authoritative lane.

Mr. Randall Garrison: I appreciate the positive example there. We have had, in other areas of defence, examples of attempts to prohibit the use of certain technology. The most famous example is between Britain and France over missile technology. The French government attempted to use its national law to prohibit use of intellectual property, as Britain chose to do so.

Do we have any examples of that kind of thing happening at this point?

Mr. Len Bastien: Mr. Chair, my best answer to that is that I have no awareness of any examples in my domain that I could cite to ratify anything like that.

● (0915)

Mr. Randall Garrison: At the beginning you talked about working with NATO and Five Eyes, but in all your discussion you talked about protocols with NATO.

Do we have similar protocols in existence for our Five Eyes partners, as we like to call them?

Mr. Len Bastien: The invitation to the board today was focused on NATO. However, in our introductory remarks, we did open the dialogue to—and frankly, our new defence policy is explicit in—talking about how important our partners are. We consider NORAD, the U.S. bilaterally, the Five Eyes, and NATO to all be very valuable partnerships and alliances.

We have significant investments in the Five Eyes realm. We participate actively in several governing bodies that include intelligence and defence forums, which I participate in personally. We take these relationships seriously. We've benefited from and contributed significantly to meeting with our colleagues in these other nations. Doing so allows us the opportunity not only to establish interoperability by default, as with all of our guiding principles, but also to benefit from each other's investments in certain areas, including cyber.

It's a tremendous forum for us to take advantage of, and I can assure you we participate in several levels, both on the military and on the civilian side, to make sure we keep those relationships healthy.

The Chair: Thank you.

Darren Fisher is next.

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

Thank you, gentlemen, for being here today. You've provided an awful lot of detail in your remarks. Thank you also for providing those ahead of time.

We know that Canadians are not immune to data breaches. We just saw that Bell was hacked. What is NATO doing to ensure that its infrastructure is safe from data breaches?

I think about the way the cyberworld is probably changing on a daily basis. I'm also interested in whether we are supple enough. Is NATO able to respond and react quickly to new cyber-threats?

Mr. Len Bastien: Mr. Chair, I would again restate the fact that in the established policy among NATO nations, it's the nation itself that is accountable for its own cyber concerns, which fall back to us to manage.

Your query into the cyber-health or well-being of NATO is outside my ability to answer, simply because it falls back to the fact that the mandate of cyber for NATO rests with the agency. We do participate in the supervisory board of that agency—the board of directors, essentially—where we ensure resources and policy are in place for them to succeed. Operationally, however, they're accountable to the North Atlantic Council, so it's very much NATO business. We couldn't possibly speculate as to the threat and risk of NATO cyber.

I could ask Rich to describe our awareness of how they are set up to handle incidents or how they are set up to react, but I'm not in a position to state the relative health of NATO cyber at this time.

Cmdre Richard Feltham: Yes, Mr. Chair, thank you again.

I would reiterate a couple of points that Mr. Bastien raised earlier: the NATO pledge clearly specifies where the responsibility for cyber lies, and that is within each nation's own constructs.

In terms of working in coalitions, I described earlier the federated mission network, the deployed networks that adhere to some protocols that we've all agreed to, but I would comment on one point when we're talking about collaboration and moving forward to ensure that NATO nations can improve their individual cyber capabilities by working together. I referred in my opening remarks to an example of a smart defence project. All that means is that we're sharing data in the multinational cyber defence capability delivery program—

Mr. Darren Fisher: The MN CD2.

Cmdre Richard Feltham: Those are positive examples of how we work together to ensure individual nations' cyber-equities are taken care of, but again that's an individual responsibility.

To add on to that, I can give you a positive example where an output from that smart defence project, that multinational cyber defence group, has come back to our own country, and we have used one of the outputs of that group within our own networks now. It's a give-and-take. We're sharing resources, we're sharing ideas, and we're sharing intellect to make ourselves better individually, sir.

Mr. Darren Fisher: Okay.

In trying to picture how that all works, I know HMCS *St. John's* left Halifax a couple of weeks ago for Operation Reassurance. I would assume there would be a cyberwarfare campaign against our troops. How do we respond to that? What are we doing to prepare for threats like that?

Mr. Len Bastien: Thank you for the question, Mr. Chair. I'll start and then I'll ask my colleague, given his experience in the navy, to comment on what that might look and feel like.

As I said earlier, we prepare the cyber capabilities that deploy with our navy, army, and air force. That's our mandate. We make sure that they have the best possible chance of success by making sure they have the best technology we can afford and provide to them. However, once deployed, once they have left the shores of Canada, they come under the operational control of joint operational command.

Rich can maybe explain the look and feel of what it's like to be on board a ship and what kind of force protection would be in place, and perhaps comment on the cyber-readiness that we would deploy with.

● (0920)

Cmdre Richard Feltham: Thank you, Mr. Chair.

Just to be a bit more specific, and coming back one step, whenever we send our troops into operational missions, there is a full analysis done on threat. That's been done forever, and the new threats emerging in the last 20 years have been the cyber threats.

Part of the mandate when the chief of the defence staff deploys people on a mission is that the joint operational command ensures that those deploying troops are prepared for whatever threat they may face. Cyber is one of those threats, so it's an education process, among others, that is based on that threat analysis.

Coming back to a ship deploying in a broader context, we come back to Mr. Bastien's earlier points that ships, like many other units, communicate as a necessity through networks, so we develop secure protocols and networks to communicate among the ships that are working together.

There is a twofold answer, then, to your question: from a personal security perspective, we prepare our deploying troops, whatever the threat analysis is, and from a capability perspective, the networks are designed to be secure so they can communicate and share intelligence among the units in any given group.

Mr. Darren Fisher: Do I still have time, Mr. Chair?

The Chair: Yes, you have about a minute and 40 seconds.

Mr. Darren Fisher: Okay.

You mentioned the MN CD2. I don't want to put words in your mouth, but when you talked about our important contribution, you said the scale has not been large. I think that was your wording.

Within the NATO construct, I'm interested in how our contribution is gauged. Are we investing enough? Do we have enough? In your opinion, do we need to do more within this realm that we're talking about today?

Cmdre Richard Feltham: What I can talk about is what we're doing. From a policy perspective, Canada has a full-time cyber officer within NATO headquarters to help inform NATO policies. That's what we're doing. As Mr. Bastien talked about earlier, in multiple governance groups, we are participating in these smart defence projects. I would say that the contribution is not small, so maybe I misspoke earlier. I would like to clarify that a little bit. In the MN CD2 construct, for example, since about 2013, we've contributed over 900,000 euros to that common defence effort. I would not say that's small. It's a sizable contribution, not only in treasury terms but also in intellectual capacity, as we send individuals from Canada, qualified experts in a domain, to participate in a multinational forum to help everybody come to a better option for all of us together. I might have misspoken that maybe our footprint was small.

I will come back to one other point if I have time. One of the constraints in any cyber operations field, whether in government or industry or whatever you have, is HR. We are searching for qualified people to come to work for us. Where we put people, we do it very judiciously, person by person, and we choose venues where we can have the greatest impact for the greatest common good.

The Chair: We'll go to five-minute questions now.

Mr. Spengemann, you have the floor.

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

Thank you both for being here, gentlemen. Thank you for your service and your expertise.

Building on the question that my colleague, Mr. Fisher, just asked, I'd like to mention the following example. It's too interesting to ignore. I'd like to get your comments on it.

Nathan Russer is a 20-year-old college student who is interested in international security and the Middle East. He went onto Strava's Global Heatmap with a view to taking a look at Syria. What he found was an elaborate amount of data concerning U.S. service personnel and their recreational and athletic activities right out there in the open.

From a force protection perspective, how much work needs to be done inside the Canadian Forces and our allies, including NATO, to make sure that we really think seamlessly with respect to our civilian activities, our military service, in regard to connectivity and the ability of anybody who wants to do us harm to find that kind of data in a very simple fashion?

Mr. Len Bastien: That's a fascinating example that we all read about recently and that the U.S. is reacting to.

I would come back to our current defence security posture inside our institution. We have distinct and explicit policy around any electronic or digital devices in certain areas where we operate our business. For example, there are rooms and floors in our buildings where no digital devices are allowed, including the athletic monitoring devices you referred to. We provide lockboxes for them to be checked in, and they can be picked up after the activity. We are enforcing compliance with those policies every day. We operate with that limited tolerance when it comes to taking any kind of risk in that area.

I really can't speak to other nations or NATO on how compliant they are toward similar policies, but I can tell you we take that very seriously inside National Defence and our institutions. I would offer to you that the commander of Joint Operations Command, or CJOC, would give you the same answer about deployed environments.

● (0925)

Mr. Sven Spengemann: That's helpful. Thank you very much.

My second question goes to the workforce, civilian and military, that's required or anticipated as needed in the future to do the cybersecurity and cyberwarfare work. What is the picture at the moment with respect to the Canadian Forces being able to hire through external contracts or to direct Canadian forces expertise to do this work? What's the breakdown? How much is done in-house and how much is outsourced?

That raises the question of contracts and security exemptions that may have to be put in place. For the committee and for the Canadian public, could you paint us a bit of a picture of what the status quo is and what the anticipated needs are into the next decade or so?

Mr. Len Bastien: This is a very exciting time. The announcement of our policy and the explicit direction to us to get on with investing in cyber operations is a direction that we take very seriously. An environmental scan of the current landscape would tell you that we're not the only ones investing in cyber. In fact, the entire federal government, and industry as well—indeed, the entire community—is looking to invest in and recruit and retain the subject matter experts in this area. The Canadian Forces has been directed to stand up a cyber force. I'll ask Commodore Feltham to explain what that's going to look like and exactly where we are today and where we've come in just a few short months since the policy was announced.

We are becoming very creative in our HR strategies when it comes to recruiting and retaining cyber expertise. We are looking to partner with academia. We are looking to work with industry. We are looking to share amongst ourselves and our allies in NATO and Five Eyes fora to find solutions to this challenge, because we all share the same objective, which is to find the right amount of capability to operate safely in cyber.

To that end, I think the story of what the Canadian Forces is doing is very important, because our mandate explicitly to defend National Defence, especially in cyber, will fall to that regime. I'll ask Rich to explain that.

Cmdre Richard Feltham: I would like to come back to Mr. Bastien's earlier point, from a Canadian Armed Forces perspective, about what we are doing for a cyber workforce way ahead. The policy was very clear that we shall stand up a cyber operator trade. As Mr. Bastien also mentioned, it's very exciting. The trade was stood up this summer, and we have our first members of that trade. The follow-on efforts will try to bring the reserve forces into that trade. They have also stood up a trade in the reserves to make sure that we get all the talent we can within that domain. That's moving ahead.

The next challenge is always going to be where we get the people and how we keep them. How do we attract, recruit, and retain them into that domain? That's an ongoing challenge that we're putting a great deal of energy into. To be quite frank, we are using different levels of thinking outside our standard ways of recruiting within the Canadian Armed Forces, because this is really a specialized group that we're paying close attention to.

I will come back to your specific question. As the available talent pool is so small, when contractors work for us, they are security-cleared and vetted to the appropriate level to do the work that we need done by them. From a security perspective, I'm not concerned about that. I need manpower who are qualified and willing to work within that domain. Contractors are a source, as are reserves and the regular force. I'm working with academia and industry on the broader concepts.

The Chair: Your time is up.

Mr. Yurdiga is next.

Mr. David Yurdiga (Fort McMurray—Cold Lake, CPC): Thank you, Mr. Chair.

I'd like to thank the witnesses for joining us this morning.

Mr. Bastien, my first question will go to you. I understand you have a lot of experience with IT and cybersecurity. With the IM/IT program at National Defence being decentralized, what benefits will be realized, and does decentralization make our system more secure from cyber-attacks?

Mr. Len Bastien: That is an accurate statement that IM/IT at National Defence is delivered through service providers that are in a federated governance construct. Let me explain what that is essentially.

As the chief information officer, I'm the functional authority for all IM/IT in the department. I don't necessarily have to own it to authoritatively control it. The army, navy, air force, and chief military personnel provide IT services on wings, bases, and garrisons across the country. They do so, however, under a policy construct that my group authoritatively controls.

Although we're not centrally owned, we are centrally operated, so to speak. We are centrally governed and regionally delivered. We do a lot of centralized governance in order to make sure that our investments are prudent and of value to Canadians.

The concept of cyber introduces a reality that we all have to work in collaboration. My stakeholders, my partners, and service delivery across the department have been directed by the chief of the defence staff to line up behind Commodore Feltham and his team to make sure we provide the cyber service delivery and service assurance needed to run the business of defence. The reality is that our operations in defence are very good as is. At this time, there is no direction for me to centralize or take ownership of all IM/IT equities inside the department. In fact, we're finding that strong governance and authoritative control are providing the outcomes and outputs that we need.

● (0930)

Mr. David Yurdiga: A lot of people are concerned about our cyber-integration and information sharing with our allies. This is not a concern that sharing of information is bad, but there's an element of risk when one ally is compromised. What protocols are in place to ensure that we can react very quickly if one of our allies is breached?

Mr. Len Bastien: Let me explain our technical environment in terms that are a little bit more simple than the engineering terms that my team might try to get me to use.

Essentially, as Commodore Feltham says, we want to communicate with our allies. It's an essential part of working in coalition. Whether we're communicating at a top secret level, a secret level, or designated protected B level, our networks are set up in a way that they can interoperate. However, as I said earlier, gates and firewalls are left in place to segment, in the case of an incident, the different allies from those networks. Although we haven't had any major incidents of the kind you describe, the ability for us to protect our equities nationally is always built into the design and engineering of those networks.

We meet often as allies, as Five Eyes, or as NATO to discuss that interoperability and that engineering and that design function to that end.

Mr. David Yurdiga: Thank you for your answer.

As you know, we talk about information and sharing and everything else, but we also have to look at the infrastructure issues. If one of the systems is hacked, whether it's a utility, a pipeline, or whatever it might be, that could be a bad situation that potentially causes deaths. Are we taking a holistic view that we have to protect all infrastructure, whether it's private or public? Also, are there ongoing communications between private and public infrastructure?

Mr. Len Bastien: Again, Mr. Chair, thank you for that question.

As was said earlier, the cyber environment is without borders. It's not quite as easy to put your hands around a terrestrial or geographical distinction of where the lines are. What you described is a concern for the government, I would offer. At National Defence, we are part of “cyber Team Canada”, if you will, and we are but one member. The Team Canada approach to cyber is led by Public Safety. Although we participate on committee with them to build a better cyber policy for the government and for Canadians, the answers you're looking for would be better brought forward by the lead department for the cyber hygiene of Canada.

I can tell you that there is a cyber policy being worked on. We are a member of the committee that is trying to get the cyber policy forward, so I have an awareness, but I'm not an authoritative voice on the objectives and outcomes of that policy.

● (0935)

The Chair: That's your time.

Go ahead, Ms. Alleslev.

Ms. Leona Alleslev (Aurora—Oak Ridges—Richmond Hill, Lib.): Thank you very much.

Rich, it's good to see you after 36 years, of course.

I'd like to carry on with my colleague's questioning, because I do think that once upon a time a military was mostly there to keep our sovereignty safe through protection from invasion of actual defined borders. Now, with the changing nature of warfare, there's no question that we have grey zones. Cyberwarfare is actually almost cheaper and faster and is incredibly effective.

Also, they're not going after military networks, because those in the military have done a very good job. As a result, the conversation to have today is certainly not around how great NATO is in terms of managing its own infrastructure or how great Canada is at managing its own command and control infrastructure, because we've been doing it for many years and we are particularly good.

I think our vulnerability is around the theft of critical information such as that of the National Research Council, which was hacked, and our financial data, which was hacked through Equifax, an American company. It's around our iCloud, Our Cloud, and our Google Docs, where all the information that we have as a nation is not Canadian. Look at our email infrastructure: our ability to have sovereign communications with our population is not actually within Canada.

I recognize that NATO is looking at that domestic capability as being within the responsibility of a nation; however, I would argue that our vulnerabilities domestically, at home, infringe not only on our sovereignty and our security but on the sovereignty and security of our allies as well. How are we communicating our domestic security and infrastructure as that pertains to the alliance's strengths? Any alliance is only as strong as its weakest link, and at the moment I would argue that our civilian infrastructure around information warfare is actually far weaker than our military one and therefore can affect the alliance.

Can you please speak to how we measure that and to what we're doing to mitigate that weakness, not only for ourselves but for the alliance?

Mr. Len Bastien: I need to address several areas of your statement just to hopefully provide some clarity and some context for what I will ask Rich to deal with, which is the concept of measuring our strength and reporting it into the alliance as one forum that we work with.

When you look at the Government of Canada and our IM/IT fabric and you look at the cyber for that, you see that National Defence has a mandate in the National Defence Act that clearly states we are to defend Defence, and we can do that with our abilities and current constructs.

When it comes to deployed operations, we take direction from the government. The government has to ask us whether it's land, sea, air, or cyber or space. We react to a request from the government, whether it's domestic or abroad, and that becomes a mission. It becomes an operation, and it's guided by, as I said earlier, the commander of Joint Operations Command. I would offer that the mandate to protect the government and the equities of the government's data is actually a mandate that is provided to the Canadian Communications Security Establishment, and they work closely with Shared Services Canada to do that. They help us manage the parts of our network that are involved in the government back office, so to speak, with Shared Services, but we are still authoritatively in control of defending Defence.

I just wanted you to understand that National Defence really doesn't have a mandate to protect the government or defend the government unless the government asks us to, and they have. In issues like the National Research Council or other exploits that the government had been managing, at times National Defence was asked to come in as a domestic operation and provide services to the government in that area. I just wanted to explain the command and control—

● (0940)

Ms. Leona Alleslev: Then are they reporting back to the strength, to our allies? Ultimately that is an important element. Once upon a time it was okay to be domestic, but now it's not, because our weakness at home in a cyber environment affects not just us.

Mr. Len Bastien: That's a very true statement. Thank you.

Mr. Chair, as I mentioned earlier, we participate in several fora. There is the top secret environment in which the Five Eyes intelligence agencies CIOs meet twice a year. We have a technical road map towards interoperability. We have a cyber health card that we are all mandated to provide to each other and report back to our national security advisers on. There are checks and balances in place for us to communicate to our allies our well-being in cyber at just about every level. I could take it down to the secret level, where the military command, control, communications, and computers board meets regularly and speaks to the cyber well-being of our secret network. We do communicate back and forth amongst our allies.

Ms. Leona Alleslev: Does that include our civilian infrastructure as well?

Mr. Len Bastien: We do provide updates to our allies in those meetings in that forum as a national update. At the beginning of every one of those meetings, nations are asked to speak to the goings-on of their government or nation's capital or broader perspective that would be relevant to the mandate or—

Ms. Leona Alleslev: I'm not referring just to government infrastructure. I'm talking about our domestic infrastructure, such as our hydro plants and our Facebook—or the Americans' Facebook that we use—that has been able to shape uprising.

The Chair: I'm going to have to hold it there. I let that run long. I'm happy to give the other parties a little bit more time. I think we need to get to that social media aspect of the information part and I hope we do, but I'm going to give the floor to Mr. Bezan.

I'll give you an extra minute.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Thank you, Mr. Chair, and I want to thank our witnesses for being here and for their testimony.

I want to follow up on what Leona was just questioning on. I think all of us look at cyber-defence maybe a little bit differently from the way it's been implemented. I look at National Defence, I look at our Canadian Armed Forces, and if a foreign nation flies a fighter jet near our airspace, we scramble our jets to intercept and escort them out. If a submarine popped up in the Gulf of St. Lawrence, our navy would be there immediately to defend our sovereignty. If little green men landed on Vancouver Island, I know that National Defence would ensure that our troops were on the ground to counter that, yet you're saying that if a foreign entity attacks our cyber infrastructure, if it's civilian-based—whether it's our banking systems, our subway systems, or our power grid—we're going to sit back and let Public Safety be the lead rather than have National Defence defend our sovereignty.

Is that policy, or is that legislation?

Mr. Len Bastien: Let me clarify your scenario. I believe I said that at the request of the government, National Defence equities can be brought to bear in any of the environments, including cyber, to address a national concern or interest or national security. I didn't say there was policy or legislation to prohibit us from doing that; I said we wouldn't unilaterally make that decision. It would be a decision taken by the government and administered through the Canadian Armed Forces.

Mr. James Bezan: When a foreign entity is doing the attack, doesn't that automatically become a national security matter that has to be dealt with by National Defence?

Mr. Len Bastien: Rich, would you like to elaborate?

Cmdre Richard Feltham: I think it's important to know what our mandate is and what the government wants National Defence and the Canadian Armed Forces to do. Right now, as it stands, our mandate is to protect the Canadian Armed Forces networks and provide support when we're asked.

Coming back to an earlier point, Mr. Chair, in terms of domestic infrastructure, do we report to NATO on the status of our critical cyber and domestic infrastructure? I'm not aware that's what the Department of National Defence and the Canadian Armed Forces do. Unless we're given a mandate to support civilian infrastructure, that is not within our current mandate.

Mr. James Bezan: Let's take it to the NATO level, then.

You guys have your working groups and joint operational commands. NATO members have had some hard lessons learned. We have troops sitting in Latvia with the enhanced forward presence and we have troops sitting in Ukraine. Operation Unifier is not necessarily a NATO operation, but Ukraine, Latvia, Estonia, and other partners have been attacked. Power grids have been taken out and subway systems and transportation systems have been interrupted through cyber-attacks. What lessons learned have been shared at the NATO level that we've been able to take back and share with our civilian suppliers of those services here in Canada?

● (0945)

Mr. Len Bastien: Those are excellent examples.

At this stage of our cyber interoperability evolution, as Rich mentioned earlier, to our awareness there is no hot wash, so to speak, among the nations, among the allies, that would provide those lessons learned in the current construct.

We do share at the most senior levels, in the most classified environments around intelligence—top secret, for example—more open and easier communication. It's simply a smaller environment to have to manage. The broad environments of the nations of NATO and their cyber-exploits that occur, frankly, regularly, we do not necessarily manage or monitor.

Mr. James Bezan: But I thought NATO had stood up a centre of excellence on cyber in Estonia. Aren't we tapped into that, making use of lessons learned? I just assume that they're taking attacks on civilian infrastructure as lessons learned to be shared among other nations by making sure we have the appropriate firewalls and cyber-defence posture.

Mr. Len Bastien: We are participating in that centre of excellence. It is relatively new in its evolution. It will grow and evolve quickly. I'm sure we will get more value as time goes on.

We do learn from the exploits around the world. Globally, if a vulnerability gets exploited, the entire community reacts by addressing the vulnerability, learning from it, and patching for it. We're not complacent when these events occur. We're very aware. It may not necessarily even be through our alliances with NATO or Five Eyes that we find our way to a return to service or a state of compliance by reacting to those exploits. It's done through the normal operation and maintenance of our cyber environment.

Mr. James Bezan: NATO's article 5 is summed up as an attack on one being an attack on all. It was only used once, on 9/11, and of course it was civilian infrastructure that was attacked. With Bill C-59, there's going to be a cyber-offensive posture provided to the Department of National Defence and the Canadian Communications Security Establishment. What would be classified as an article 5 in the cyberworld?

Mr. Len Bastien: It's a very good question.

Mr. James Bezan: I know it's hypothetical.

Mr. Len Bastien: The impact of an event is a case-by-case issue. It's measured as it would be in any other environment.

To try to answer your question, I would offer that a cyber-event would now be considered or looked at like any other kind of kinetic event from a military perspective, and it could qualify for article 5 if the impact to the nation was deemed sufficient to invoke that policy. It's really not for me to comment what it would take to get there.

I don't disagree with you that it's the industries of our nations that are vulnerable to these kinds of attacks. I just want to clarify our mandate for you here today, which is that we engage to help and provide service to Canadians through the national defence institution, so that you have a good understanding of what to expect from us should something like that happen.

The Chair: Thank you.

Go ahead, Mr. Robillard.

Mr. Yves Robillard (Marc-Aurèle-Fortin, Lib.): Thank you, Chair. I will share my time with my colleague, MP Fisher.

Sir, can you please highlight some of the merits that granted Canadian company MDA this $15-million contract to deliver NATO's Project Triton?

Mr. Len Bastien: Thank you for the question, Mr. Chair.

I didn't bring the details of that contract exchange with NATO with me today. It was meant to be an example of the value of return on our investment in exposing Canadian industry to the agency at NATO that spends upwards of 450 million euros a year. A lot of the work and contracting was not getting to North America. It was staying in Europe, and we were motivated to see Canadian industry have a better share in that market. It was meant to give you an example of the success, if you will, of our investment in working with the agency. If you like, we can return to you more details of the scope of what that contract will mean to MDA, but we'll have to bring that in later. I didn't bring it with me today.

● (0950)

Mr. Yves Robillard: As a follow-up, can you elaborate on Project Triton and how it contributes to the maritime and control information systems project?

Mr. Len Bastien: Thank you, sir, Mr. Chair.

As I have stated, the details of that contract.... That contract was not with National Defence but with the agency at NATO. My awareness of that is limited to the extent I've shared with you today, namely of its success for Canadian industry and its value. Should they be available, we will gladly provide you with details of the scope and requirements of that contract. I didn't bring them with me today.

Mr. Yves Robillard: Thank you, sir.

Mr. Darren Fisher: Thank you, Mr. Chair.

Gentlemen, you both mentioned initiative 65 and cryptographic capability improvements. I'm hoping you can expand on that a bit and give me some examples of some of those improvements.

Mr. Len Bastien: Again, thank you for the question, Mr. Chair.

Cryptography is the essence of our ability to communicate and share information in a secure way. To do that amongst allies requires cryptography architecture that is not only extensive and complex but that can also be responsive to our needs.

The Department of National Defence has invested a lot in the interoperability of cryptography among our allied nations. The evolution of cryptology is in response to the threat vector becoming more challenging, so the evolution of cryptography is very serious. It's mandated for us to stay compliant amongst the alliances, and it is a significant area of investment. It's laid out in our policy that we will not only maintain it but evolve it to compliancy level so we can continue to operate and interoperate with our allies and communicate securely.

Mr. Darren Fisher: That's all good, and it tells me what you want to accomplish, but how do you evolve it? What types of things can you do to improve it?

Mr. Len Bastien: I'm not technically equipped to speak to our cryptographic engineering in great detail, but let me explain.

The concept of cryptography is a concept of exchanging keys. In other words, you need two halves of the key in order to open the compartment of the document, or the “crypt”. The ability for threat vectors to misrepresent the keys or break the keys is constantly evolving, so we have to build better keys, but we can't do that unilaterally or we wouldn't be able to speak to our allies. In working together, we establish the criteria for these evolved keys, and then we go across the global network—the fabric, if you will—and upgrade and update all the hardware and software that generate the keys. It's a very sensitive and complex environment, but it's one we're actually doing really well in, and I would say we're in good shape with respect to our compliancy among our nations.

The Chair: You're about out of time, Mr. Fisher.

I'm going to give the last formal question to Mr. Garrison, to make it fair for everyone.

Mr. Randall Garrison: Thank you, Mr. Chair.

I want to take the conversation in a bit of a different direction here. I think we're running into a phenomenon here of cyberwarfare not really fitting under the normal protocols of war and the rules of warfare. It operates at the edges of those. International protocols prohibit targeting civilian targets, and those kinds of principles we're used to. I know that neither of you represents CSE, but the legislation that's before Parliament in Bill C-59 proposes to allow active use of cyber-attacks in sabotage. It's a concern for me that we, as Canadians, are stepping into an area of international conflict that's not well regulated internationally.

My question, I guess, would be directed largely to Mr. Feltham. What's your relationship with CSE in terms of their, I would say, requests for moving into active cyber-attacks?

The second part of the question is this: do you feel that you are already authorized in DND to use active cyber-attacks against both foreign states and individuals for CSE? Are you already authorized to do those things? What's your relationship with CSE on those aspects?

● (0955)

Mr. Len Bastien: I will open and then ask my colleague to follow up.

The relationship with CSE is not that complex, actually. They were a part of our department not so very long ago. When their act was originally created, they were mandated in their act to support other government security agencies with their capabilities, let's say. I can expand on their capabilities; that gets us into a different conversation. I can tell you that those capabilities would be very valuable to us in cyber. I don't think the government wants National Defence to create the equivalent capabilities inside of its institution, so we've been directed to work with CSE so that we come together as a team. We would deploy and operate in cyber as a team, because they have the capabilities.

However, when their act was created, National Defence was not named as an agency they could support, ironically. They were us, so there was no need to put defence in that legislation. I think some of the amendments happening in that bill will help remediate the legislative policy layer, if you will, to allow us to work together more actively. That's one part of your question. I really wanted to explain that we will move forward in cyber as a team as soon as we're able to.

To the other part of your question, as of the current day, in terms of day zero capabilities in cyber, we have limited cyber capabilities in the active cyberspace today that we could, without CSE, engage and use to support mission. I wouldn't want to give you the impression that we could provide extensive cyber capabilities that would be of concern to Canadians, but the ability for us to jam a radio, block a telephone, take an Internet site down, or block a service provider are things we are evolving quickly in order to support mission.

Mr. Randall Garrison: Are you authorized to do that now?

Mr. Len Bastien: Under the defence act, we would be authorized to bring those equities to bear. We are working with our colleagues in CSE to make sure that what we do develop and work with inside the government construct is transparent to the government.

This is new territory. For the government to give us a mandate to move into active cyber operations—offensive cyber, as you described it—was not taken lightly, and we're not reacting lightly inside our organization.

We will brief and we will be held to account for the constructs we put in place to engage in any kind of active cyber operations.

As I said earlier, we cannot unilaterally engage in those kinds of activities in the way we can engage in any kind of military activity without the oversight and request of the government. There's ultimately a command and control structure that is connected to the administration of the government before we could actively get going in that kind of activity. I hope that answers your question.

Mr. Randall Garrison: If you feel you're already authorized, what are the constraints that you're operating under? How have constraints been established to make sure that any potential offensive cyber-organization would not come into conflict with international law and would adhere to some of those basic principles of distinguishing between military and civilian targets and those kinds of principles?

Mr. Len Bastien: Thank you, sir.

Mr. Chair, for that answer I will defer to my colleague, Commodore Feltham, since he is a military officer and an operator who has experience and can speak better to that question.

Cmdre Richard Feltham: Thank you, Mr. Chair, for the opportunity to speak on this question.

As was mentioned earlier, the policy to conduct active cyber operations for the Canadian Armed Forces just came out in their recent defence policy. We're working with our international and government partners to develop this capability.

You asked the question, Mr. Chair, on how we ensure that the cyber operations active offensive as a component of active cyber adheres to the law of armed conflict. I can tell you that, just as in any military operation, kinetic or in cyberspace, we only conduct operations in the Canadian Armed Forces based on the government's mandate and in accordance with the law of armed conflict. This is what regulates us day in and day out, and there are no exceptions to that.

In terms of ongoing operations within the cyber realm, this is not my field, and I can't comment on that in any great detail, but I can assure you that from our perspective—and I've developed this capability with our partners—we stick to the mandates. We go on government missions and we operate within the law of armed conflict.

Mr. Randall Garrison: Are there any special reporting mechanisms to government that have been put in place because of the nature of cyber operations being covert?

● (1000)

Mr. Len Bastien: In our reporting structure, when we're employing the Canadian Armed Forces, it is through the chief of the defence staff. He does a report back to government on Canadian Forces operations. I would offer that it is better for his office to address exactly the semantics of how that feels and looks from a government perspective, but I can assure you that we report in to him. We'll leave it there.

Mr. Randall Garrison: Thank you, Mr. Chair.

The Chair: Okay. That ends the formal questions. We still have time left, so I'm going to predictably go around the track one more time. It will be five minutes, so it will be Liberals, then back to Conservatives, and then back to Mr. Garrison.

I will need to leave a little bit of time at the end. There are a couple of motions that I need to deal with, but we'll dispatch those when we get there.

I am going to turn the floor over to Mr. Rioux. You have the floor for up to five minutes. Share your time if you'd like.

[*Translation*]

Mr. Jean Rioux (Saint-Jean, Lib.): Thank you, Mr. Chair.

Mr. Bastien, I have a basic question for you. What are the major cyber-threats facing Canada? Are they in the main the same ones as other NATO countries are facing?

Mr. Len Bastien: Thank you for the question.

[*English*]

The threat vector vulnerabilities that we monitor change every day. Every day there are new vulnerabilities that are brought to bear, whether through industry or other governments, and those vulnerabilities are assessed.

A vulnerability is not a threat until it becomes exploited, so we are constantly reacting to what I would call “vulnerabilities”. With that, the same would exist for industry, for Canadians, and for NATO when those vulnerabilities come to our awareness. We work usually as a government, as a collection of government agencies, to bring the right get-well-plan and to shore up those vulnerabilities through patching and the evolution of technology to avoid the moment in time when a vulnerability becomes an exploit.

The way it works is that the good guys are out there trying to learn about vulnerabilities and protect themselves from the exploits. The bad guys are out there trying to figure out how to use a vulnerability to exploit, so it's a race. Our ability to stay in front of that comes back to our security posture and our compliancy with our own standards, whether within government or within National Defence. I would offer that NATO's agency responsible for their cyber would have the same perspective, as they're constantly reacting to the potential vulnerabilities that have come to our attention that we need to react to.

I hope it explains the environment a little bit to know that it's not a single event that happens. It's typically a series of vulnerabilities that have been exploited that you hear about in the news. Our ability to stay in front of those vulnerabilities and stay protected comes back to our ability to interoperate with our allies, to work closely with industry, even academia, as well as with our colleagues in the government. We're constantly reacting to new vulnerabilities.

[*Translation*]

Mr. Jean Rioux: I'm going to follow up on Mr. Garrison's questions and talk about CSIS.

We know that the Department of National Defence and CSIS are two distinct entities. I believe I understood from your answer earlier that you do not have a mandate to work with CSIS and that the law does not require that you work together. Did I misunderstand you?

Mr. Len Bastien: I'd like to clarify the nature of the relationship between these two entities.

[*English*]

The Communications Security Establishment has a very different mandate from CSIS. We work with both agencies. What I described was a relationship with CSE specific to cyber and cyber-active operations. That doesn't negate that we work with both those agencies in many other areas of intelligence. In terms of the cyber role, the cyber mandate I described, the relationship was with CSE. We have a very strong interoperating relationship with CSIS as well, but for different reasons.

The Chair: We have some time left, so I'm going to hand it over to Mr. Spengemann.

You have the floor.

Mr. Sven Spengemann: Thank you, Mr. Chair.

I have a general question that loops back to your exchange with my colleague Ms. Alleslev. You mentioned to her several tiers of information that were communicated under top secret and secret clearance. It's a policy decision whether this committee should have elevated levels of security clearance to get a full view of the material that's in front of it.

I'm wondering if you could tell the committee, from your perspective and specific to the area of cybersecurity and its rapidly evolving dynamics, what this committee would see if there were an elevated classification in security. In other words, how much more of a fine-grained conversation could we have?

I appreciate that this is a public meeting, but were we to be in a meeting that would allow an elevated security clearance for this body, how would our understanding improve?

● (1005)

Mr. Len Bastien: Some of the answer to that question will fall back into my own personal opinion, so I'll avoid that. However, I would offer to you in all sincerity today that I felt quite comfortable with the information I shared with you, in that a change in classification would not have significantly changed my testimony. I think you're getting a good perspective from today's interview. I hope you are.

Typically classification is more about timing than it is about the content of the information. We use classification to protect national interests—national security and national safety—and we do it because the information at any given time would be incredibly valuable or risky should it fall into the wrong hands. However, given time, that same information is no longer a threat and therefore should no longer be classified.

I think there's a tremendous amount of information available in an unclassified discussion about lessons learned and about our reaction to certain situations that will give you a very good perspective on how we operate day to day. When we start talking about active operations and about things we're going to do tomorrow, that level of classification is there for a reason. It is to protect equities that are important to Canadians, and that's where you may be running into a challenge.

In my realm, in today's discussion we didn't go there, so I'm hoping you're getting rich content that will help advise you in your decisions that are forthcoming.

The Chair: Thank you.

Go ahead, Mr. Bezan.

Mr. James Bezan: Thank you. I'm going to split my time with Mr. Paul-Hus.

In the opening testimony, we talked a little bit about smart defence within NATO and how you're doing that through cyber. The European Union recently stood up the permanent structured cooperation on security and defence, PESCO. How is that going to impact smart defence, especially in a cyber context? Does it make it stronger or better, or is it a competing factor?

Mr. Len Bastien: I'm going to open by saying that I'm not entirely familiar with the details of PESCO, so I may not be able to offer you a full, comprehensive answer to that question. I'll ask Commodore Feltham if he has anything to add. We may have to get back to you regarding the impacts that PESCO will have on the cyber-equities of NATO. I just don't have that today.

Cmdre Richard Feltham: I'm actually in exactly the same space, unfortunately, in terms of the impact of that. In a broad context, when we have more people discussing and sharing information on the cyber-threat, it's usually better. If there are shared equities that get pulled from one to the other, that might be a complication, but I'm not aware of any to this day, Mr. Chair.

Mr. James Bezan: Thank you.

[*Translation*]

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

I find today's discussion very enlightening, but also somewhat worrisome. Regarding defence and cyber-security, your role is to protect Canadian Forces and the defence infrastructure. Insofar as operations are concerned, that involves the CSE.

My question concerns NATO. Some of our troops are currently deployed; the Canadian Forces protect us. If we decided to attack Kaliningrad, for instance, and to shut down its power station, who would lead that attack? The Canadian Forces or CSE?

Mr. Len Bastien: Thank you for the question.

[*English*]

I will answer in English simply because this industry is really a lot easier to describe.

Let me just be clear. Any military operations are governed by the Canadian Armed Forces. Bringing CSE into an operational environment is under the authority of the Canadian Armed Forces. Their ability to bring their capabilities to bear for us right now is somewhat inhibited by legislation, because we're not defined as an agency they're allowed to use and operate with. We're looking to fix that with some of these legislative changes.

The scenario you described would be a military-led, integrated team approach using our equities and CSE's equities in concert. That would be in the future, once the legislative—

● (1010)

[*Translation*]

Mr. Pierre Paul-Hus: After this meeting, I am going to go to a meeting of the Standing Committee on Public Safety and National Security where we will discuss Bill C-59. We'll be meeting with the CSE Commissioner, as it happens.

That bill involves transferring CSE national defence-related powers to the Minister of Public Safety and Emergency Preparedness. The bill also contains provisions that will require the authorization of the Minister of Foreign Affairs to conduct an operation.

How do you see that?

[*English*]

Mr. Len Bastien: The impact of the proposed CSE Act is more relevant in its broad terms to their operations than to ours. We have dependencies on them to move into cyber operations and be able to work with them in a more integrated fashion than we can today in operations.

I want to leave you the perspective that we've done the work, we've done the exercises, and we've done simulated operations with them. We've been heavily integrated and invested with that agency to work together in cyber operations going forward, but that will be defined by the government, and I can't speak to the other areas of that.

[*Translation*]

Mr. Pierre Paul-Hus: Do similar concepts exist in most NATO countries? In other words, does their defence include cyber-security elements in addition to emergency preparedness elements? Do they all work together in an integrated fashion?

[*English*]

Mr. Len Bastien: As I said, we have terrific relationships with our allies. I can tell you that those I work with regularly don't all share the same construct of governance, of design of our governance, when it comes to where cyber capabilities rest inside of government. I can tell you how Canada is engaging, and I'm hoping to do that, but I can't speak—

[*Translation*]

Mr. Pierre Paul-Hus: As compared to the models in other countries, is Canada's model effective? Are there better models in the United Kingdom or the United States, for instance?

[*English*]

Mr. Len Bastien: The concept of whether we're good, better, or best among our allies is an opinion. It is what we have established in Canada. For us, our abilities and our current design and portfolios are deemed to be very effective in cyber-defence. It has worked very well in signals intelligence and in other areas and capabilities we've brought to bear for the Canadian Armed Forces. It's the construct we've chosen to propose to government that we will move out on cyber operations.

Commodore Feltham may have a better perspective globally of other militaries. Simply put, he has been deployed and is an operator, versus a civilian member of the defence team. I don't have that perspective.

Do you have anything, Commodore Feltham?

The Chair: I'm going to have to leave it there. You might be able to circle back, but I'm going to have to give the floor to Mr. Garrison.

The floor is yours.

Mr. Randall Garrison: Thanks very much, Mr. Chair.

I really appreciate the testimony we've had on cyber defence today, and I am reassured that we're doing our best in cyber-defence, but your testimony today identified that the legislation in Bill C-59 is really going to bring CSE in line with the authority to do active cyber that DND already sees itself as having.

In the legislation, section 31 says essentially that active cyber, after being authorized, can be carried out despite any act of Parliament or any act of a foreign state. This is a very broad grant of authority.

I'm wondering whether you consider that DND is already authorized to conduct active cyber-activities without regard to any act of Parliament or the act of any other state.

Mr. Len Bastien: Let me clarify the perception of our relationship with the Canadian Communications Security Establishment that I would like to leave you with.

We have abilities in technology that we have needed to operate in the past. They are of great value to us, but somewhat limited. Before we would invest to grow that arsenal, if you will, of cyber ordnance, we recognize that a lot of that capability exists inside CSE. Getting access to it and giving them the legislative mandate to come to our side and use those capabilities as part of the military construct is the gap. That's the incremental difference that we're looking for, and it's a very small part of that bill.

As for what the rest of the bill addresses and the changes, they are very relevant to the Canadian Communications Security Establishment and, I would offer, are not in my jurisdiction to comment on.

Rich, is there any part of that question you would like to...?

● (1015)

Cmdre Richard Feltham: Yes. Mr. Chair, I would just add one point.

Like many other government partners, we will work with the Communications Security Establishment to increase the capabilities of the Canadian Armed Forces, but I want to be perfectly clear. Any military operation that the Canadian Armed Forces engages in, whether in traditional military structures of naval, air forces, army, or in cyber, are government-mandated military operations conducted in accord with the law of armed conflict and the rules of engagement specifically authorized by the chief of the defence staff through the Government of Canada.

The answer to your question is that we would not operate cyber any differently from any other kinetic military structures outside of the government mandate. What CSE would do within their mandate is beyond my scope to comment on, sir.

Mr. Randall Garrison: It seems to me that some of the common practices that are referred to as "active" cyber operations are modern-day equivalents of things such as wearing the enemy's uniform, the kinds of things that we've tried to prohibit specifically in international conventions. I know that misuse of uniforms was prohibited in The Hague convention of 1907.

Within our NATO partnerships, have there been any activities you're aware of—and I know that it's not necessarily in your mandate—to try to draw some very specific lines around what would be acceptable in the use of active cyber operations?

Mr. Len Bastien: Let me open, and then I will ask Commodore Feltham to comment on potential policy gaps internationally in cyber engagement or the rules of engagement, if you will, for cyber.

I can tell you that in my experience we've realized the reality that every nation has a different set of legislative and policy constructs for their respective militaries to engage in cyber activities. Some nations fully endorse offensive cyber, while others are completely prohibitive. There's a real variation as you wander around the globe and look at different constructs. I think Canada is looking at its options. Our policy of "Strong, Secure, Engaged" has proposed a scope for cyber—an arc of fire, if you will—that is reasonable, and we've been given explicit direction to implement that.

Commodore Feltham, if there are any activities within NATO or other fora with regard to establishing policy around rules of engagement for cyber, I'd ask you to explain.

Cmdre Richard Feltham: If I have time, Mr. Chair, I'll continue.

The Chair: Yes, very briefly.

Cmdre Richard Feltham: Just to clarify one term, Mr. Chair, "active cyber" is a mixture of what we would consider active defence and what we would consider offence. It's the difference between standing on your castle wall waiting till the guys are coming in through your wall and then attacking them or seeing the guys come to your wall and attacking them there. That's active defence. The other is going to the other person's place to actively attack.

What's the intent? If my intent is to defend myself, I can still be active, but it's to defend my own equities. If my intent is to attack another person's networks, that's offensive. "Active" is a component of both. The NATO community and the broader communities at large are working to understand where those lines lie. If you read the output from the *Tallinn Manual*, for example, you'll see that there are ongoing efforts from the legal community and military forces within our alliance to understand that better.

Are there agreed-upon rules across all of the alliance and all allied nations? I don't think there are, but it's a growing and emerging conversation that is very rich.

The Chair: Thank you.

I know that one person wants to have a couple of minutes to ask a question, but given the time I have left and a couple of housekeeping items that I have to take care of, I can't really go there unless everybody else agrees. I don't have time to give a couple of minutes to everybody.

Did you have anything else, Mr. Garrison, that you wanted to add? Mr. Bezan? No?

I'd like to give Ms. Alleslev just a couple of minutes to finish off, and then we'll move to our motions.

Go ahead, Ms. Alleslev, for a couple of minutes.

Ms. Leona Alleslev: Thank you very much, team, and Mr. Chair.

I wanted to close out on the conversation around whether you felt comfortable having an unclassified conversation. There are many of us around this table who've had and have security clearances and therefore did not ask questions that we knew you wouldn't be able to answer. You commented that you're comfortable with the answers you gave; I think the level of conversation was therefore based on the questions we asked and that there perhaps are more classified levels of conversation that we have obviously not had today.

It's particularly in this space that we look at the overlap between our health and well-being domestically, in terms of both civilian and military infrastructures, and then that of our allies, in terms of what information we communicate between those two. I wonder if you could comment on that.

● (1020)

Mr. Len Bastien: I wouldn't want to have misrepresented the fact that in a classified environment with the right situation, with all the conditions met, a classified conversation in certain key areas would not be a richer dialogue between committee and us as witnesses. What I would simply offer is that in the line of questioning we received today, there were great questions that allowed me to talk about our business and to talk about our situation in the world and our relationships with our partners without compromising national security or safety.

Ms. Leona Alleslev: Thank you.

Mr. Len Bastien: You're right. Should the questions—

Ms. Leona Alleslev: Thank you. We didn't ask the questions that would have put you in a position of not being able to answer.

Mr. Len Bastien: No, so I should thank you for that, Mr. Chair.

Voices: Oh, oh!

The Chair: It's a circular argument.

Mr. Len Bastien: It is.

We come here to have a valuable exchange of dialogue so that we can engage with you and help you do the very valuable work that you do to help the department situate itself inside the government, so with that, I thank you.

I wouldn't want to leave you with the perspective that a classified conversation would yield different answers to the questions I received today. Indeed, if you had asked different questions, there would have been different answers, absolutely.

Ms. Leona Alleslev: I think that we're wrestling with it because we recognize, particularly in cyber, that it's far more complex and uncharted, both because of the nature of the changing warfare and because, at the moment, those who would deny us our sovereignty and call into question our domestic security are moving quite agilely and are not constrained to the same extent that we are. To understand that next level of conversation, we feel that we need to be able to have a secure conversation.

Mr. Len Bastien: Thank you.

The Chair: I had 10:30 a.m. in my mind, because we've just started in the mornings again. We're actually at 10:45 a.m. I'm just checking on something else here, motion-wise. Again, I'm happy to give everyone a fair amount of time. Ms. Romanado had a question.

We do have a little bit more time, and I'd like to give you an opportunity, Ms. Romanado. Go ahead. You have the floor.

Mrs. Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.): Thank you, Chair.

Thank you very much for your testimony. I had the great opportunity to visit MDA about two weeks ago and to visit their installation. I know that the Triton project is actually a new maritime command and control solution for both fixed and deployable systems, so we look forward to receiving that briefing.

We talked a little bit about the assets that we are deploying for NATO, specifically support. You mentioned 120 to 130 positions in direct support of NATO. I know that with “Strong, Secure, Engaged”, we're talking about a 3,500-person increase in military personnel.

Maybe you're not the person to answer this, but in terms of how many of those folks are going to be allocated towards cybersecurity and with respect to operability with our NATO allies, what kind of training programs are we developing for cyber for our men and women in uniform? Are we working with NATO to create those training programs, based on that incredibly fast-moving technology?

Mr. Len Bastien: Indeed, we will come back with as much information as is available to us with respect to the MDA project. They're probably quite excited about it and have more details than we would, on the periphery, watching that happen.

With respect to what we would refer to in our terms as force development for cyber and co-operation and collaboration with NATO, as Commodore Feltham indicated in his remarks, NATO has invested significantly in a centre of excellence—a cyber range, if you will.

Imagine a technical environment where you can test cyber ordnances, your reaction to an attack, and so on. These are very valuable entities that we, as a partner of NATO, will be able to exploit and take advantage of. We look forward to that.

With respect to the commitments of our policy, the policy as delivered by the government directs investments by the department over a 20-year period. Those funding and personnel commitments have not exactly dropped into our laps this year, so we are busy looking at the design of the implementation of this policy and what it's going to look and feel like over the 20 years of its term.

It's a little early for me to comment on how much of the resources committed in the policy will land in NATO. Suffice it to say that the policy also explicitly tells us that we will continue to invest in and support our relationships with our allies, including NATO, Five Eyes, NORAD, and the others.

Unfortunately, I can't give you an quantitative answer other than an explicit direction from government in the policy for us to continue investing in that area. Then, as we implement the policy in the coming years, it will become clearer to us how and where to make those investments.

As Rich said earlier, there's always more demand than there is supply in a give-and-take relationship with any entity. We want to be very smart about where we put our resources so that we get the most return on investment for us and for Canadians, ultimately.

● (1025)

Mrs. Sherry Romanado: In terms of our actual training programs, right now if someone is working as a cyber-operator, they would do their BMQ and then go off for their 16 weeks of training. Are we working to develop those training programs that are going to be meeting that forecast, that evolution of cyberwarfare? What are we doing in terms of recruiting the best that we need? We know this is an emerging field that we need to continue to invest in, so what are we doing in terms of the training and recruiting and getting that pipeline?

It's one thing to have NCMs, but we're going to need officers as well. What are we doing in terms of recruitment for that field?

Mr. Len Bastien: That's an excellent question, Mr. Chair. I'll ask Commodore Feltham to speak to that.

Cmdre Richard Feltham: Thank you, Mr. Chair.

As I mentioned earlier, the human resource demand in this occupation is extreme and very difficult. We don't take it lightly. I would say I spend the vast majority of my time trying to understand innovative ways to come to that answer.

The first tranche of operatives we put into cyber-occupation, as an example, we took from a proven commodity. They were people who were doing that work within our operation centre, and we moved them into the operator trade. We've developed internal training programs. We have standards to develop and train our operators. We got those standards in collaboration with our allies. We worked together to have standardized training that we can exchange with our other broader allies.

Also we recognize that within the civilian sector, there's a robust and rich opportunity to recruit young Canadians from colleges around our country, and we are working with a number of colleges to accredit their programs and to bring those people into our programs as fully fledged cyber-operators.

I would not want to leave you with the impression that this is another military occupation that we will handle like every other, because it's not. It demands a different view, a different focus, and an adaptive approach over time.

The answer I give you today is that I hope that it will adapt and evolve over time to meet the demands of that occupation. For example, in the coming weeks we're going to have an entire ideation session on how we can best use the reserve force within a cyber-occupation. We're looking at every and all means, and not just within our own structure. We are trying to leverage both industry and academia to bring ideas to us and to leverage those as well. I don't think we have all the answers—I know we don't—but we're working with all allies internationally and nationally to get the best advice within that structure.

Mr. Len Bastien: If I may follow up on that, earlier a colleague asked a similar question, and I wrote a note, which I want to contribute to the answer, around the reserve force and how exciting that is for us.

In my interactions with industry—we're significantly engaged in areas in which we are able to be—the discussion around cyber-talent is always a challenge, as it is for them as well. Given their industry base, they're able to pay some of the skilled people very well. It's very difficult for government to attract them to come over in the regular normal time as a public servant or as a regular force member. However, the interest in being a part-time cyber-operator for the Canadian Armed Forces is of great interest to industry and industry personnel whom I've engaged with.

As we learn and exploit how we're going to implement these new curriculums and these new criteria for being a cyber-operator, we're looking at creative ideas around using and leveraging the reserve force to get access to that industry talent, even if it's only on a part-time basis.

● (1030)

Mrs. Sherry Romanado: Thank you.

The Chair: Go ahead, Mr. Bezan.

Mr. James Bezan: Thank you.

To build upon what Mr. Fisher asked earlier about one of our frigates being deployed to NATO's Operation Reassurance as part of the maritime task force, we know that U.S. warships have been attacked through electronic warfare by the Russians. We talked earlier about how our troops in the enhanced forward presence in Latvia have undergone hybrid warfare attacks with some misinformation and slanderous media stories coming from the Kremlin-controlled news agencies Sputnik and RT.

Explain to me the difference between how we would provide cybersecurity to our troops stationed in Latvia or on one of our frigates in a NATO Operation Reassurance measure versus what we do in Operation Unifier with our troops in Ukraine. From a cybersecurity standpoint, do DND and the Canadian Armed Forces provide close personnel support in, say, Yavoriv, versus what they do with the guys who are outside of Riga, as done through Joint Operations Command of NATO?

Mr. Len Bastien: Again that's a very good question, in the sense of getting a perspective of what it would look and feel like to deploy as military personnel from a digital perspective.

As Rich said earlier, when we get ready to deploy our forces into these areas of the world, a threat assessment is done and a reaction to that assessment to mitigate those risks is established before we deploy. In the digital and cyber world, for this conversation, we provide the capabilities for those men and women in uniform to operate, to do the job that they need to do to succeed in operations. We give them capabilities that are secure and compliant. We do our best to stay ahead of the bad guys when it comes to exploits and vulnerabilities and we are constantly readjusting our position.

In some ways it will be the same approach when we deploy our men and women when it comes to cyber and digital capabilities, but it will always be adjusted to the threat of the environment they are going into.

To that end, I will offer Commodore Feltham, as an operator himself, the opportunity to elaborate on my statement.

Cmdre Richard Feltham: Mr. Chair, I can really only reiterate what I said earlier, which is that it's all based on threat assessment, so the broad answer to your question is that there is no difference in how we approach the problem. The specifics of what we will deploy to support any individual operation will vary based on that threat assessment. I couldn't speak to every ongoing operation in the Canadian Armed Forces today, but the path we take to prepare our troops to enable them to succeed in operations is essentially the same. We analyze the threat and prepare them against that threat.

Mr. James Bezan: Commodore Feltham, you're a navy guy. Now we're going to be putting Wi-Fi on all our frigates and we're talking about leisure time, and people are going to be doing their Facebook, Instagram, and whatever else. How does that impact your job from a cybersecurity standpoint? Does the civilian infrastructure that's now being utilized through a Canadian Armed Forces asset compromise cybersecurity in any way, shape, or form?

Cmdre Richard Feltham: You're asking me if it compromises cybersecurity. I know I wear a navy uniform, but I must say I haven't worked within the navy structure for a number of years, so I'm not aware of their analysis of the threat that this morale tool introduces. I wouldn't want to speak out of turn.

The navy has done an analysis of what Wi-Fi means to the security of their platforms and the morale advantage that it provides to people who will deploy for months on end through having access to communications with families back home and what that provides for them. In terms of a threat or a cyber-threat, I'm not aware of any because I'm not working in the navy lines.

Mr. Len Bastien: I would only want to interject to make sure that it was clear to the committee that the Wi-Fi capability supported by the navy on those platforms is not connected to the corporate network in any way, shape, or form. It provides access to the Internet for the men and women on board ship to have a bit of a work-life balance when they are off duty.

The corporate equities on board that ship still fall under the authorities of my organization to secure and maintain, and they are not involved in getting these men and women access to the Internet through corporate systems. These are independent systems that the navy has deemed a tolerable risk in order to enhance work-life balance. Further to that, you would have to ask the commander of the navy of his level of comfort with that.

● (1035)

The Chair: Gentlemen, thank you very much for coming. The ability of cyberwarfare and information warfare to influence outcomes is significant. We have seen it in Ukraine, we have seen it in Europe, and we have seen it in the United States. We haven't worked out the terms yet, but there is a will of the committee moving forward to drill down a bit more on cyber, and I suspect that we will probably see you sooner rather than later on this issue.

Thanks very much. I was going to suspend and let you go, but I'll never get everyone back in here, so I'm just going to ask you to bear with us. There are a couple of housekeeping motions that we need to get to the table here.

I'm going to call on Mr. Spengemann.

Mr. Sven Spengemann: Mr. Chair, thank you much. I think they are being circulated. Let me just read them back to back. There are two motions.

The first is as follows:

> That the Committee approve the hospitality expenses incurred during the trip to Brussels, Latvia and Ukraine from September 18-26, 2017.

The second motion reads:

> That the Committee approve the hospitality expenses for a dinner in Room 602, Parliamentary Restaurant on Monday, February 12, 2018 in honour of Ainars Latkovskis, Member of Parliament and Chairman of the Defence, Interior and Anti-corruption Commission, Saeima, Riga, Latvia.

The Chair: Is there any discussion on those topics? Apparently I can do them both at the same time.

(Motions agreed to)

The Chair: Gentlemen, thank you very much. We look forward to seeing you in the future.

The meeting is adjourned.