HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on National Defence

NDDN • NUMBER 038 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, November 20, 2014

Chair

The Honourable Peter Kent

Standing Committee on National Defence

Thursday, November 20, 2014

● (1535)

[*English*]

The Chair (Hon. Peter Kent (Thornhill, CPC)): Good afternoon, colleagues. As you know from the notification of the orders of the day, we are here pursuant to Standing Order 108(2) to continue our study of the defence of North America.

We have two witnesses today, one in each of the following hours. In this hour from the SecDev Group we have Rafal Rohozinski, a principal of the organization, to address the issue of cybersecurity. Thank you very much for being here.

Mr. Rohozinski, your opening remarks please.

Mr. Rafal Rohozinski (Principal, SecDev Group): Thank you very much.

Thank you to the members of the committee. It is truly a privilege to address you today on the topic of cybersecurity.

By way of background I am not just a principal of the SecDev Group, which is a Canadian company that works at the intersection of technology and security and has actively worked in an operational capacity in the cyber domain on behalf of the U.S. and U.K. governments in particular. I am also a senior fellow at the London-based International Institute for Strategic Studies, where together with colleagues from the government community we have addressed the more intricate policy implications of both cyber and how it crosses over with other forms of insecurity including hybrid warfare and transnational crime.

Let me start perhaps unconventionally by indulging you in a bit of a story. Last week when I was travelling to the Middle East I was woken up in the morning by an application on my iPhone. As I ate breakfast I watched Russian television streaming on my iPad. On the way to the airport I took an important phone call using an encrypted voice application called Silent Circle to speak securely with my colleagues in the Middle East. As I approached the airport my electronic boarding pass automatically popped up in another application to swiftly get me through security procedures.

What's unusual about this story? Perhaps nothing because everything I've described here one or all of you have experienced in your everyday lives. The unusual thing is that none of these technologies existed five years ago. That's the point. The speed and depth at which the digital world has colonized the physical world is astounding. Twenty-five years ago there were perhaps 14,000 people connected to the Internet. Today over a third of humanity is connected to broadband Internet and there are more cellphones on the planet than there are human beings. This has a significant and profound impact on all of our societies.

Our dependence on digital technologies and networks has expanded faster than our ability to design rules and regulations or adapt existing laws and practices to this new environment. We live in an era that we at SecDev have described as open empowerment, where the ability of individuals to act has scaled faster than the ability of institutions to adapt. The positive side of this empowerment has been perhaps the greatest leap forward in human knowledge ever. More people are empowered to make decisions over their lives through access to information and knowledge than at any other point in human history.

At the same time with great empowerment has come great risk, and these risks are not just those implicit to technical failure or manipulation in a malfeasant manner of information in the information systems on which we depend and which are evident in the kinds of stories that are making regular headlines telling of major breaches of privacy, data loss, data thefts, and other compromises of critical information and communication systems.

There are also important risks implicit to a silent rewriting of the social contract between individuals and states that have emerged as more and more of our everyday lives are now mediated through or assisted in the cyber domain. The risks implicit to these normative challenges are perhaps as complex, if not more so, than the technical challenge of dealing with vulnerabilities and insecurities to our critical digital infrastructure.

Perhaps to illustrate a point, currently Canadian workers who work in bricks and mortar institutions such as car plants or other factories can legally engage in labour action that may involve picketing their workplace. In other words, denying access to new non-union workers or clients to their place of work. But what if that place of work is not a bricks and mortar institution but rather a virtual business, maybe a website rather than a storefront? If workers in this environment decided to deny access to their place of work in cyberspace, say using a denial of service attack, this would be considered a criminal act.

The point here is not to equate a computer denial of service attack with a picket line but merely to point out that there are certain rights and norms that we have struggled decades to establish in physical space that do not have a comfortable or meaningful equivalent in the cyber domain.

Cybercrime also faces us with other challenges to our existing normative order. Criminality in cyberspace, whether directed at individuals or at states, leverages the globally contiguous nature of the cyber environment in order to create a jurisdictional nightmare for law enforcement agencies forced to pursue these cases. Put bluntly, cybercriminals can use the absence of a global convention on cybercrime and agreement among law enforcement agencies to effectively put their activities beyond the reach of national law enforcement. The situation is perhaps viewed best by way of analogy.

During the prohibition era in the U.S., most policing was organized on a local basis. Bootleggers and rum-runners used the absence of a unified legislation or convention across state or national borders to circumvent the reach of local law enforcement authorities. The result was the emergence of national policing in the U.S., and unfortunately doing the same for cybercrime would require a global agreement for which there is very little opportunity at present.

The cyber environment has significant impact for Canadian national security for other reasons. If Canada is a country that was forged by the iron rail, today Canada's economy is held together by the glass fibres of the digital web. Put simply, Canada is the first country of cyberspace because of our geography. Commerce, governance, as well as everyday life, are dependent on telecommunications and the Internet. In this respect cyberspace is a national strategic asset whose disruption or vulnerability to disruption represents a significant risk to national security far greater than that of other physical threats to economic and territorial integrity.

Here I would add that the risks and threats are not just to cyberspace, but what cyberspace enables, including critical infrastructure and important access to knowledge including genetic, biological, and other areas of science, which in themselves represent unique and important risks to our increasingly complex and technologically dependent societies.

Defending cyberspace is not an easy task. First and foremost this is a synthetic environment that was built for resilience and not for security. Unlike land, air, sea, or space, cyberspace requires constant and continuous attention at the technical, code, and regulatory levels to simply exist. Changes within any of these three levels can cause significant changes to the synthetic environment with cascading impacts for commerce, governance, and everyday life.

While it is sometimes said that cyberspace has no centre, I would argue this is not the case. Cyberspace has its physical manifestation in the switches, routers, and cables operated by the telecommunications industry. Ironically, telecommunications remains among the most regulated industries in Canada and among the G-7 countries, yet very little has been done to leverage the provisions of the existing Telecommunications Act to compel or incentivize operators of this infrastructure to take steps to limit the vulnerabilities that exist within this domain.

Quite simply, many of the critical vulnerabilities implicit to Canadian cyberspace could and should be addressed at the level of operators of the infrastructure where the patterns of malfeasance, the things that make malfeasance work, are best seen and addressed at scale. Thereafter better coordination and cooperation between and within agencies of government and the private sector would go a long way to building a greater resilience into Canadian cyberspace, increasing confidence, and minimizing the potential for catastrophic or black swan events.

I'll turn briefly to the military aspects of cyberspace and its importance for cybersecurity. The critical dependence that advanced industrial societies have on cyber infrastructure, including the way we've chosen to structure and gain efficiencies out of our national defence institutions means that cyberspace has become an active zone of experimentation and development of capabilities, both offensive and defensive. Whether we wish cyberspace to become the domain of military activity or not, the reality is that it will as it offers threat actors—be they states, transnational criminal organizations, terrorist organizations, or superpowered individuals—the ability to create and generate sustained effects. Put simply it offers them an opportunity to leapfrog generations of industrial warfare and to compete on a global scale in the ability to muster the use of force to further political effects.

Our modern military is leveraged on technology. A few years ago I had the privilege of running a senior workshop at the Center for Strategic Leadership at the U.S. Army War College. One of the questions that was asked to a highly selected group of individuals from across the defence and intelligence communities was whether we could rerun the invasion of Normandy today given our current force structure. The answer to the question was no, because we have done away with whole levels of staff positions and functions that are now made possible through technologically mediated processes. Quite simply, we don't have enough trained people to do all the tasks manually.

● (1540)

If this is the case today, in the future operating environment with increased reliance on automated technologies, the risks and vulnerabilities implicit through the technical environment will only increase.

What is also perhaps notable about the use of cyberspace and its military dimension is that the threshold for generating effects does not require the resources available to a state. Groups as disparate as the drug gangs of Latin America and the so-called Islamic State can generate significant effects in and through cyberspace in pursuit of their political agendas. I'll simply put one example here. Last year not the Islamic State but a group aligned with the Syrian government successfully hacked into the AP Twitter stream and put out a false message that the White House was under attack and President Obama had been injured, which caused a 150-point, $1.36-billion drop in the stock markets for a period of three minutes. This was a short-term effect, but this was still a strategic information effect, and I think what we see here is a road map for the future.

What is important perhaps to take away from this larger more complex discussion is that cyberspace operations as understood by many of our peer state and non-state actors are not limited to operations through the network domain but incorporate an understanding of leveraging the information domain as a means of generating effects. This concept is important given that for the most part our tendency in the west—and by this I mean also the Canadian Forces—has been to see information operations and computer network operations as two separate silos. Doing this, I would argue, is a mistake.

Finally, in closing, I'd like to make the observation that despite the vulnerabilities and insecurity that may emanate from an infrastructure that has so deeply and pervasively colonized our everyday lives, governance, and commerce, cyberspace benefits open societies. Therefore, it benefits our national security to maintain it as an open commons. Greater security is not served by building digital borders, fences, or enclaves; rather it is served by taking a more intelligent and intelligence-led approach to understanding the nature of the risks, threats, and opportunities that emanate in and through cyberspace and by developing capabilities and mechanisms within and outside the public sector to ensure resilience and the ability to act decisively in and through this domain in defence of our national interests.

I thank you for your attention and welcome your questions.

● (1545)

The Chair: Thank you very much, Mr. Rohozinski.

We'll now commence the first round of questioning with seven-minute slots.

Mr. Norlock, go ahead, please.

Mr. Rick Norlock (Northumberland—Quinte West, CPC): Thank you very much, Mr. Chair.

Thank you to the witness for attending today.

My first point is a little comment regarding my experience with those beautiful things called computers and malware and all those others things you buy. You pay $150 for some sort of antivirus software and you put it on and if you don't keep it up every week somebody finds a way of circumventing it. I take it from your testimony that no matter what we come up with today, maybe 10 days from now somebody will come out with some way of overriding or getting around the kind of net you put up to protect yourself. I'd like you to make a comment on that and work it into the following questions.

In Canada of course, we have Public Safety, which is the lead agency for our cybersecurity. I'd like you to comment on the extent to which you think it's appropriate to compare our cybersecurity with that, let's say, of the United States, which recently developed Cyber Command or USCYBERCOM as a centralized command for their cyber operations. If you could comment on those themes, I'd appreciate it.

Mr. Rafal Rohozinski: Sure. Thank you very much for the questions.

With respect to your first question, yes, I think we have to recognize the fact that one of the costs of openness is the fact that the environment itself will always provide a degree of insecurity. That's absolutely right. The problem, however, is that the nature of the kinds of threats that exist in malware code can be aggregated and seen when you look at them at scale. In other words, that which affects your computer that's difficult to detect is actually much better viewed by someone who's providing you your services and can see multiples of the same thing happening at the same time.

This is where I would come back to the comment that I made in my testimony, that we have not really leveraged where that sort of concentration point actually exists, the point of seeing the risk and threat that affects individuals. In Canada, 95% of what we call cyberspace is actually operated by a single operator, Bell Canada. It's through a variety of different mechanisms, but the reality is that there's a high concentration of it. There are telecom regulations acts, as they exist currently, to compel those operators to work in certain ways—interchange, etc. Security is not one of those things. In other words, we have not used the most valuable mechanism that we have already on the books as a way of being able to address what you might call the “95% problem” of a dirty ecosystem that is currently polluted by opportunistic cybercrime, for which we pay $150 to hopefully be able to defeat on our individual computers.

By way of background we, SecDev, participated in a study with Bell Canada that tried to look at the scale of what you might call malfeasant behaviour existing online. This study was done a couple of years ago now. We found that at any given time between 5% and 12% of all devices connected to the Internet belonged to a botnet. In other words, they were under the control of some form of malfeasance software, which was not intended by the operator of the system itself. This is a fairly significant problem. The fact that we haven't regulated or incentivized the telecommunications industry to provide that first line of defence, I think, is one of the critical failures that we've had in addressing cybersecurity.

With the question of—if I understand the question correctly—who should be leading on the cybersecurity portfolio, I think if I look across our colleagues in the Five Eyes, one thing has happened there that has not happened in Canada. In Canada, the issue of cybersecurity has not been elevated to a national security priority—in other words, something that works across the interagency or the intergovernment, as they call it in the U.S. In the U.S. there is an executive-level entity that looks after coordination of cybersecurity across the whole of government. Similarly, in the U.K. the mechanisms that bind together their version of public safety, their version of CSE, and industry are far stronger and far better developed than they are here at the moment.

I think, in answer to your question directly, we do need Public Safety Canada to be taking a lead in terms of the coordination of cybersecurity as it applies to aspects of public safety and security, meaning the interface between the public and the private sector. We equivalently do need to have an institution that provides those capabilities on the military side, which I don't think we currently have.

● (1550)

Mr. Rick Norlock: Carrying through with that, the Department of National Defence's network is adequate, but to what extent are the capabilities used by the Communications Security Establishment or CSEC adequate to ensure the protection of the Government of Canada's electronic information and information structures? You did separate them into two entities, public-private and military, which you now say we need. By that, I gather that there should be two entities within government, one to take care of the military and one to take care of public-private, or can they be housed under just one roof?

Mr. Rafal Rohozinski: I can't comment on the capabilities of CSEC, seeing as I'm not really speaking on its behalf nor am I an employee nor do I have privilege to be able to access it at that level. However, if I talk about it from an institutional point of view, I think CSEC has definitely taken a leading role in cybersecurity in Canada because, quite frankly, that's the institution where government has been able to bring together the expertise and know-how to do so. Whether that should continue to be the centre, going forward, I think is a very good question.

Again, I think, the past is prologue here. Air traffic control, at one point in time, was the responsibility of the Department of Defense in the U.S. Currently a civilian agency is responsible. I think there are capabilities that currently exist within CSEC that have to be migrated out into law enforcement and other government departments that have a responsibility for ensuring those components of cybersecurity that apply to very specific sectoral areas. I think overall, though, from an institutional point of view, there has to be an understanding and I think a recognition of the fact that cyberspace requires an emphasis equal to what we put to territorial security, economic security, and energy security. We should treat it in the same kind of way in terms of the kind of intergovernmental and interagency coordination that would allow us to have a coordinated policy.

The Chair: That's your time. Thank you very much, Mr. Rohozinski.

Mr. Chisholm, please.

● (1555)

Mr. Robert Chisholm (Dartmouth—Cole Harbour, NDP): Thank you very much, Mr. Chairman, and if I can stop talking, I will share some of my time with Mr. Brahmi.

I found your presentation and your brief interesting. I want to follow up on the whole level of the issue of coordination and cooperation that Mr. Norlock was talking about, but I want to do it this way. In July, the National Research Council suffered a major cyber-attack that included the infiltration of systems containing personal information. The response from the government was that they blamed China.

I want to ask you two questions. Could you give us some indication of how safe Canada's critical infrastructures are from cyber-attacks by state-sponsored actors? Also, could we be doing a much better job on the issue of coordination and cooperation?

Mr. Rafal Rohozinski: On the issue of vulnerability, I think the reality is that our systems are very vulnerable. The reality is that they're vulnerable for two reasons: first, because security was never at the heart of how these systems were engineered to begin with, and second, we haven't put in those kinds of regulatory demands to ensure that operators of critical infrastructure take security not just as a responsibility to their shareholders, as businesses, but also as part of their responsibility to Canada, quite frankly, or to national security. That, I think, is the principal failure we have.

Mr. Robert Chisholm: On the issue of better coordination in the public sector of agencies that are investigating our vulnerability, are we doing enough?

Mr. Rafal Rohozinski: Again, I think part of the problem is that currently the heart of the capabilities that the government has for doing attribution-type work lies in an institution that was never designed to do so—the CSE—hence my comment earlier on that I think there are capabilities that currently are, for all the right reasons, centralized within CSE, but that actually have to be migrated out. Either they have to be migrated out to other government departments or we should be looking at creating a civilianized, non-military, non-intelligence institution that would coordinate cybersecurity across the board.

Again, I would emphasize that we have much to lose here. We are not Estonia, where you can drive across the country in six hours, or Israel. We are Canada, where it takes six or seven hours to fly across the country. What we lose by losing critical infrastructure can be far more catastrophic, and therefore, this really does require a strong policy emphasis.

Mr. Robert Chisholm: A civilianized agency is not what I understand the other countries in the Five Eyes are doing. It's generally an intelligence-led activity.

Mr. Rafal Rohozinski: Yes and no. I would separate two things.

Yes, there has been, not just amongst the Five Eyes, but across, if I'm not mistaken.... We did a study for the strategic balance for the IISS, and about 90 countries are starting to develop the equivalent of what would be a cyber command, which means a military organization that effectively looks at cyberspace as a domain for operations and that trains, equips, and develops a doctrine for being able to conduct operations therein. Clearly that's happening in other Five Eyes countries.

However, within the U.K. and the U.S., you've also seen coordination amongst the civilian agencies, such as Homeland Security, for example, and the critical infrastructure protection office in the U.K., which have taken capabilities from GCHQ and NSA and moved them into civilian agencies that have responsibility for critical infrastructure, the financial sector, the energy sector, etc.

Mr. Robert Chisholm: Okay.

Thanks very much.

The Chair: You have three minutes remaining, Mr. Brahmi.

[*Translation*]

Mr. Tarik Brahmi (Saint-Jean, NDP): I would like to ask a question that is of great concern to the citizens of Saint-Jean-sur-Richelieu, where an attack was carried out by what is called a lone wolf.

Could you tell us about cybercrime and cyberterrorism in terms of the lone wolf? If we are not able to link a particular incident to a terrorist organization, how can we intervene?

Are there criteria for defining acts as analogous to terrorism because they took their inspiration from information on the Internet? If there are no such criteria, how can cyberspace be protected to prevent people with mental health issues from committing a terrorist act after getting information from terrorist organizations? People like that may have no link to, or knowledge of, terrorist organizations, but they may interpret certain messages in cyberspace as a call to commit terrorist acts.

● (1600)

[*English*]

Mr. Rafal Rohozinski: Excellent question, and I'll predicate my answer by saying that I'm testifying in front of a Senate committee on the issue of cyberterrorism on Monday. We have been involved in working with Public Safety Canada under the Kanishka program, specifically looking at social media, the Internet and radicalization, and what measures can be taken, both within the public sector as well as at the community level, in order to be able to detect and provide early intervention to individuals at risk of radicalization.

The longer answer, I would say, is that I think your observations are quite right, that as the Internet, or the population of the Internet, more and more reflects that of society at large, it will include the good, the bad, and the ugly—individuals who are predicated towards mobilization and others. That has certainly been exploited by groups like Daesh Islamic State.

I think the principle difference, I would say, between al Qaeda and Islamic State is that al Qaeda was a conspiracy. At some point in time the individual was always vetted by someone else who knew someone else. There was a physical contact. Daesh, or the so-called Islamic State, is much more like a brand. It provides an aspirational message and those who are interested in those aspirational messages will choose to act on their own. That's terribly difficult to be able to detect because, although technology allows us at one level to be able to identify individuals who access content that may cause radicalization, having that technology at the disposal of law enforcement without grounds effectively means that we are creating a system of surveillance that may actually be far worse or outweigh any benefits that we would have by identifying individuals who are at risk.

However—

The Chair: That's your time, Mr. Brahmi. We may pursue that with subsequent questioners.

Mr. Daniel, please.

Mr. Joe Daniel (Don Valley East, CPC): Thank you, Chair, and thank you, Mr. Rohozinski, for being here.

You talked about a variety of things. It's interesting to note that there are so many issues relating to cyber-attacks, etc. But going down to the most fundamental aspects of it, Internet protocols, can you just explain to this committee who writes them, how do they get implemented, etc? Those are the fundamental elements of communications across the cyber-network, which I don't think anybody really considered seriously when they were talking about the wider use of the Internet as we see it now. As you know, it came from a protocol between universities way back when, so can you just help us understand the fundamental aspect of that? Could you also address the hardware side, if you get a chance to do that?

Mr. Rafal Rohozinski: Sure. I'll give the short-form answer to it.

Effectively, the standards that currently define the interoperability between hardware using the Internet protocol came out of a governance structure that was initially put in place when the Internet globalized in 1995. That included both the creation of an entity, ICANN, that effectively regulated the address space, but it also included subcommittees that dealt with security, and for example, the engineering aspects of cyberspace itself.

Initially, in the first 15 years of the Internet, if you like, from 2000 until the mid-2000s, a lot of that was dominated by engineers, researchers, who may have worked for corporations but really were looking for writing protocols that would make it easier for devices to start working together. In the recent past, cyberspace has started to be seen as a strategic aspect by countries like China, Russia, and others. There's been a greater intervention both by corporations as well as government-sponsored engineering groups to define standards that worked in terms of their own favour.

Certainly, one aspect, as I said, since cyberspace is very much a synthetic domain, is understanding how the introduction of standards may change that domain in ways that are either consistent with our norms and values, or not consistent with our norms and values. That really should be part of the watch list of a cybersecurity institution that should exist at the government level.

● (1605)

Mr. Joe Daniel: Is that something your organization is actually participating in, in terms of making sure that protocols are secure and that the Internet becomes more secure?

Mr. Rafal Rohozinski: Certainly, one of the things that we have developed as a criterion when we work with other states who are seeking to develop national cybersecurity strategies, is to understand the role of standards, and participation in standards-making bodies as a way of ensuring that the technical aspects of cyberspace don't start going against either national interests or a common interest.

Mr. Joe Daniel: You mentioned something like 15% of computers are actually being activated remotely by some of these applications, etc. Is there some collusion between the hardware manufacturers that allows this to happen working with the Internet folks? Is there a dark world out there that actually allows this to happen? Certainly, encryption has not survived. Even up to 256-bit encryption for communications has been broken into in a matter of hours.

Mr. Rafal Rohozinski: I think the issue is more the ecosystem itself.

If you take a look at it, consumer protection laws that exist for the building of a device—for example, a car—compel the manufacturers to look at safety and security as the basic design of what they're building, whether it's seatbelts, airbags, or whatever.

That is not the case when you buy a piece of software. It was built for interoperability and not for security. I think that's the consequence of the fact that we essentially had a massive gold rush in building a global domain over the last 15 years, and security really took a back seat. I think that's going to change, but certainly that's not the environment in which we live.

Mr. Joe Daniel: Should we as a government be establishing standards for these sorts of issues to actually make cyberspace more safe?

Mr. Rafal Rohozinski: I think that is certainly one issue that needs to be considered, among others. I would say that the issue of dealing with basic insecurity and vulnerability of networks at its highest concentration point, which is the operation of networks themselves, is probably more important than the consumer level at this point, in terms of the effect that it would generate.

Mr. Joe Daniel: The intermingling of the defence industry with the Internet system, which seems to be very useful in many ways, has kind of happened without any supervision. What are your comments on that?

Mr. Rafal Rohozinski: I'm not sure if I understand the question. Perhaps you can rephrase it in a different way.

Mr. Joe Daniel: The defence industry has adopted the Internet as a way of communicating, but that seems to have happened without anyone really considering the security aspect in a big way.

I guess my follow-on question to that is this. Should we, as a government, be establishing a security department that will actually monitor and police what's taking place on the Internet?

Mr. Rafal Rohozinski: Perhaps I'd answer differently.

Certainly, if we take a look at the model that's been adopted for security in the U.S., which is emerging right now, we see there's certainly a sectoral approach in terms of the degree to which security has to be ensured for the survival or the needs of the sector itself. The financial sector, for example, has its own mechanisms for information-sharing and ensuring security among the institutions that are most vulnerable and actually play a critical role in the U.S. economy.

Similarly, initiatives have been made within the defence industrial base in the U.S., where the NSA does share classified signatures that give the defence industry a better chance of dealing with vulnerabilities in the cyber domain than other sectors.

From that point of view, yes, I do think there needs to be a more sectoral approach to cybersecurity, recognizing that there's a differentiated priority in terms of how we want to implement that.

Mr. Joe Daniel: I have one last question along the same sort of line.

Shouldn't we be developing a parallel Internet system that is secure and that doesn't use the protocols that exist that are not secure, so that we can have a very secure network for critical infrastructure and the defence industry?

Mr. Rafal Rohozinski: I would argue that any network that's designed for interoperability will always have a vulnerability. Whether it's designed to be isolated or not isolated, ultimately it's going to have the same basis of vulnerability. I think Stuxnet proved that rather effectively in Iran, where a completely isolated system still managed to be compromised through a vector.

For me, coming at it from the point of view of security, it's that we need to change our mentality about how we think of security. It shouldn't be the Maginot Line, how to keep threats out. Rather, it's how you actually detect threats that you know and implicitly understand will exist within your network, and shape and manipulate them so as to minimize their effectiveness.

● (1610)

The Chair: That is time.

Ms. Murray, go ahead, please.

Ms. Joyce Murray (Vancouver Quadra, Lib.): Thank you for this fascinating presentation and discussion.

Just to follow up on Mr. Daniel's question about cybersecurity strategy, you did say that our other Five Eyes partners have a more coordinated cybersecurity approach. Is that through a national cybersecurity strategy? Is that something you think Canada should work towards having?

Mr. Rafal Rohozinski: The answer is yes, and I think that is definitely something that Canada should work at having.

The problem with cybersecurity is that it isn't quite as easy to understand as health care, unemployment, or other things that the average voter will either have a position on or not. Cybersecurity tends to be a lot more abstract, which means that it really does take an act of will to force it up onto a national agenda, ensure that there are the adequate resources put against it, and in effect compel the degree of coordination that would be required. We are talking about creating a new institution.

But then again, when we see the importance of cyberspace to governance, to commerce, and to our national security, I think we are foolhardy not to do so.

Ms. Joyce Murray: Would you have a national cybersecurity strategy with some sectoral aspects within it, or would you have a military or defence cybersecurity strategy and a commercial or civilian cybersecurity strategy?

Mr. Rafal Rohozinski: That's a good question, and I would say this. You need to start small.

I think understanding the role of cyber within the military means you need to have some kind of doctrine around cyberspace operations that is consistent with the existing defence posture. However, because cyber goes across law enforcement, defence, and even domestic issues—for example, countering radicalization or dealing with criminality—it almost requires a wider discussion.

I'm almost a bit surprised that we haven't had a royal commission on cyberspace to look at the ways cyberspace touches all aspects of governance in Canada, because in some ways that's almost a natural place to start before we can start defining specifically how it would pertain to areas like national defence.

However, in the absence of that, I think looking at it sectorally is probably the most prudent way to start.

Ms. Joyce Murray: You said that none of these technologies you were talking about existed five years ago. Technologies expanded faster than the ability of laws to address them. We know the law that created a legal framework for CSE was written in 2001 and not a period or a comma has been changed since then.

I'd like you to comment on whether updating the laws governing CSEC would be an integral part of proper security strategy.

Mr. Rafal Rohozinski: Again, I think the answer is yes. It boils down to the fact that CSEC is—rightly so—the institution in which we have concentrated the capabilities and understanding of the cyber domain in government. However, CSEC is both constrained in some ways and maybe not the most appropriate institution to be looking at how those capabilities need to be migrated out across the whole of government.

So I would say, yes, with the focus being not just on CSEC but rather on what CSEC represents as a national asset for government to be able to deal with the challenges of cybersecurity across the board.

Ms. Joyce Murray: I have questions on two other areas. I'll be as quick as I can.

The Homeland Security agency's deputy director has declared that embedding privacy and civil liberties into the programs and activities of Homeland Security is essential to strengthening it and making it more effective. In other words, respect for privacy and effective security is not a zero-sum game. You actually have the better of both if you properly embed privacy into the organization. Would you agree with that approach?

Mr. Rafal Rohozinski: I would very strongly agree with that approach as, I think, the comments during my testimony would emphasize. We risk silently rewriting the social contract between individuals and states if we don't take into account the role of privacy and the right of the individual as we rebalance institutional values.

● (1615)

Ms. Joyce Murray: In other words, some proper addressing or updating of CSEC laws to improve the embedding of privacy would actually strengthen CSEC.

Mr. Rafal Rohozinski: That's correct, but here I might also make a small distinction that is quite important. There is surveillance for law-enforcement purposes, but there's also public health surveillance. Both rely, essentially, on the same kinds of methodologies, which means gathering data in order to be able to understand patterns of either behaviour or incidents, to allow intervention to happen.

We've grown to understand the role of public health surveillance and its importance to basic public health. We've understood the role of public health surveillance, in a law enforcement sense, as enabling us to understand individuals at risk of criminality far before they start entering into the criminal justice system. I think looking at those lessons to see how they apply to the policing of cyberspace is probably a far better lens than is simply viewing the world of law enforcement or state surveillance with post-Snowden revelation eyes. I think there's a danger of the pendulum going the other way.

Ms. Joyce Murray: Okay. Thank you for that.

Our other Five Eyes partners have this kind of coordination across agencies and we don't. Along with that, you just commented that these things are in silos. There has been a comment—and I agree, actually—that not having a parliamentary committee looking at all of the departments and agencies that deal with security and intelligence is partly why we have these silos.

In the countries that do have that—i.e., all of our Five Eyes partners—that committee of parliamentarians empowered to do that through security clearance can actually identify where there are gaps, duplications, and a lack of interoperability. It's like having the RCMP on the same channel as House of Commons security. That's part of why they have a coordinated place in the other countries and we don't, so there's a lot—

The Chair: Ms. Murray, I'm afraid you've talked out your time.

We're going to the second round now with five-minute slots beginning with Mr. Williamson.

Mr. John Williamson (New Brunswick Southwest, CPC): Thank you, Chair.

Thank you for being with us today. It's very interesting.

I'm going to follow up or question some of the points you made to get a little more background on them.

You mentioned that some of the threats could create and generate "sustained effects" on the country or society. Could you explain what that might entail or what you had in mind?

Mr. Rafal Rohozinski: It could mean anything as simple as the mass disruption of telecommunications networks; the manipulation of data in critical systems, for example, at Treasury Board or Bank of Canada; or the remote manipulation of SCADA or process control systems around either electricity delivery networks or things such as nuclear power plants. It's both near physical effects, in other words, where you're touching infrastructure, or it's the manipulation of information such as to make that information unreliable or to foster a failure of the systems through not being able to rely on the input being given.

Mr. John Williamson: Thank you.

What did you mean by, we've not put in place the regulatory demand? Again, I understand where you're coming from, but can you be more precise about what that might entail coming from government or Parliament? I have a sense of what you mean.

Mr. Rafal Rohozinski: I will give you an example. It'll be an artfully constructed one but I think one that will make the point.

All the banks in Canada use the same Internet providers for most of their network services. Whereas banks can see anything that happens within their infrastructure, they can't see what happens across infrastructure. That's visible at the level of the operator. Currently, if that operator were to turn to the banks and say he sees a vulnerability that is addressing all of them, chances are the banks would come back to the operator and ask why he didn't tell them 30 seconds ago when he knew about it, and therefore, they're going to hold him liable for their losses.

There is a perverse disincentive for the infrastructure operators to provide that information. I would argue that rewriting the current instruments of the Telecommunications Act to compel operators to share that information would, first of all, not expose them to liability and would, second, increase the usable information on the cybersecurity side that would be available to the downstream clients.

● (1620)

Mr. John Williamson: That's interesting. I think you make a good point but do we not risk.... I'm going to touch on where I think Mr. Daniel is going with the sectoral approach or even what I'm beginning to wonder, which is if a macro versus a micro approach is better. Let me give you a small example, the one you raised, with AP, I think you said, in highlighting the false news feed.

I would think, at the end of the day, we want to hope it's AP's responsibility to protect against those kinds of attacks. That organization has the most to lose by an attack: misinformation. People then question their data; they look elsewhere. Similarly, my concern would be if we hold another entity responsible for bank data, no one's really accountable for it. I haven't come to any conclusion, but should banks not be responsible for their security? If we keep elevating it, ultimately, no one might be responsible for control. The backdrop to all this is that to me, working in this environment you have to be nimble, you have to evolve, you have to recognize threats, you have to be able to assess, and it strikes me that, ultimately, government is the place where you're least going to find that kind of thinking or approach. Don't get me wrong, governments do some things very well.

The Chair: Mr. Williamson—

Mr. John Williamson: I probably only have 30 seconds, but this macro versus micro approach....

Mr. Rafal Rohozinski: I don't think the government should take responsibility, but I think the role of government is to set rules and those rules can either regulate or they can incentivize. In certain cases, creating incentives for information-sharing through very light regulation is probably a lot better than creating an institution to oversee it. I would say that both macro and micro are important.

The Chair: Thank you. That's time.

Mr. Chisholm, please.

Mr. Robert Chisholm: Thank you very much, Mr. Chairman.

I'll again share my time with Mr. Rafferty.

We've talked a bit about ISIL and their role in the cyber domain. There was apparently a conference recently hosted in Kuwait. Some of the Five Eyes were there. Canada wasn't. What is being done, or what should be done, to combat what ISIL is doing in the cyber domain?

Mr. Rafal Rohozinski: I'll give a two-part answer, partially answering a question that was asked previously.

This method of public health surveillance as a way of identifying individuals at risk I think actually does have applicability in cyberspace and could be applied at a community level without creating a liability for Canadian rights. That's certainly something we should be doing, because ISIL is only the tip of the iceberg in terms of this kind of self-radicalization threat that we face.

In terms of shutting down ISIL's ability to use the Internet, I think that would be a big mistake. It is a channel for being able to understand their actions and motivations, which yields far more intelligence value for us in terms of the organization than simply shutting them down. I say this partially because we are engaged as a company in support of doing exactly that kind of work—in other words, being able to understand the motivation and actions of actors such as ISIL in places like Syria and Iraq.

Mr. Robert Chisholm: So you're saying the role, then, is to do the assessment and detection work here, or online.

Mr. Rafal Rohozinski: Exactly right. This is a separate topic but maybe an important one.

The global Internet, because it reflects the majority of humanity right now, is probably the single most valuable intelligence tool we have. By that I don't mean intelligence in terms of state intelligence but in terms of open intelligence. Literally, it allows us to gain perspective on what previously would have been local water-cooler conversations, but at a distance—not by using the capabilities of a CSEC to listen in on the very specific conversations of two individuals but literally by being able to listen in to it in a crowd.

I think that aspect of it is something that is greatly under-appreciated. My colleagues in the intelligence community in the United States will openly say that 80% to 90% of useful intelligence is open source intelligence. It's not the stuff that we pay the institutions for, it's the stuff that literally exists and needs to be simply processed from the street.

● (1625)

Mr. Robert Chisholm: Interesting; very interesting.

The Chair: Mr. Rafferty, you have 90 seconds.

Mr. John Rafferty (Thunder Bay—Rainy River, NDP): Thank you, Chair.

Thank you for being here, Mr. Rohozinski. I just want to follow up on some of Ms. Murray's comments with regard to lawful access and privacy.

You have some experience with other national governments. Should international norms and laws be developed to govern the cyber domain? Very briefly, can you tell us what's been done and what your own personal thoughts on privacy are?

Mr. Rafal Rohozinski: I think we have a much greater risk at the moment in terms of what is happening within the commercial sector and the aggregation of data at scale than we do within the government institutions. This is an immensely challenging area because we have not only built an industry around it but we also benefit disproportionally from it. I mean, there is a utility function that each and every one of us gives up when we decide to give our credentials to Google, which allows us to more efficiently and effectively organize our everyday lives.

That again, I think, is something where the danger of silently rewriting the social contract...and not just between the institutions of governance and the individual. The responsibility of the third sector, the private sector, in it really needs to be explored in all of its depth, and it has not been to date. I think the Snowden revelations at least lifted the lid on the fact that this is an issue of a social contract, but the fact that it has been weighted so heavily on issues of responsibility of state institutions I think has partially obscured the fact that it requires a much broader examination.

The Chair: Thank you.

Our final five-minute slot goes to Mr. Bezan, please.

Mr. James Bezan (Selkirk—Interlake, CPC): Thank you, Mr. Chair.

Mr. Rohozinski, it's great to see you again. Last time we talked it was on the Iranian situation, on their cyber capabilities and some of the attacks they've already orchestrated on North American soil. I want to get that perspective: who are the threats?

As well, you might be familiar with a story that came out last week that earlier this year, in April, a U.S. destroyer, the USS *Donald Cook*, was disabled while on patrol in the Black Sea by an unarmed Russian bomber. The Voltaire Network reported that a Russian Su-24 buzzed the ship and "disabled all radars, control circuits, systems, information transmission, etc. on board the US destroyer. In other words, the all-powerful Aegis system...installed on NATO's most modern ships was shut down".

Is there legitimacy to the story that was reported? What other capabilities are we facing from a military standpoint?

Mr. Rafal Rohozinski: Again, I'd go back to what I said earlier. In my work with the International Institute for Strategic Studies this year, for the first year, the strategic balance, which is really the referential tome when we look at the capabilities of nation states and others in traditional military domains, has started to look at cyberspace as one of those domains. Perhaps most interesting in the research that's been done is the range of countries that now develop active cyber capabilities, offensive cyber capabilities.

Why? As I said earlier, it's because it allows them to leapfrog a whole generation of industrial warfare. It lowers the threshold for being able to compete at a military political level that previously required an investment in manned materiel technique that was really reserved only for the most advanced countries. The question really is not who is the threat; it's who's not the threat, because the threshold is so low. I think if we don't want to be the Zulus faced with a Gatling gun, we do have to wake up and recognize that an investment in cyber as a capability of national security and national defence is a critical requirement and something that we do have to spend the time and resources to develop.

On the question of the Aegis of the destroyer, I can't really comment on that. I'm aware of it but it may well be as much a fanciful part of the Russians' information operation strategy around Ukraine as anything else.

Mr. James Bezan: Even if it is hypothetical, would that be considered an act of war?

Mr. Rafal Rohozinski: That's a question and there has been quite a bit of work done in the last three years in terms of looking at how the existing laws of armed conflict can be updated to include the cyber dimension. I think there's a greater understanding now, especially post Ukraine and Crimea, that incorporating cyber into one of the trigger points for alliance-based responses is something that's required.

However, as we have seen and as I'm sure this committee will also be examining, hybrid war, in other words war that exists outside of the laws of armed conflict, exists outside of the threshold of what can be considered state to state, is certainly something where cyber has a huge and important role to play. Given the confluence of those two things, I think the challenge of creating norms around the use of cyber in the sub state-to-state warfare scenario is going to be extremely challenging.

● (1630)

Mr. James Bezan: The U.S. has set up Cyber Command. We have activities in NORAD—and we are talking about the defence of North America—but we also have a great relationship with NATO, and you already mentioned Estonia. They have the NATO Cooperative Cyber Defence Centre of Excellence base there. Can you talk about how important it is that Canada should be playing more of a role in cybersecurity in these multinational organizations?

Mr. Rafal Rohozinski: CCDCOE is not an operational structure of NATO. It is a research centre, so it actually has no capability apart from the research function that it forces. If the question is should Canada be creating a cyber command or at least looking at where cyber fits within the current force structure, I think the answer is unambiguously, yes. The challenge of course will be that we have three strong services and our own traditions of institutions and rearranging these to create a cyber-force will be a challenge institutionally, budgetarily, as well as in terms of simply the visionary leadership required to make it happen.

The Chair: On that challenging note, Mr. Rohozinski, we will end this hour and your testimony. I will say though on behalf of the committee we would welcome any afterthoughts or summaries or advice that you might still wish to correspond with us, but we thank you certainly for your presence here today.

Ms. Joyce Murray: There were more questions but we just ran out the clock.

Thank you.

The Chair: We'll now suspend as our next witnesses approach the table. We would like to make this transition nice and quick if possible.

● (1630)

(Pause)

● (1635)

The Chair: All right, colleagues, we will resume and continue with our study of the defence of North America.

From the Department of Fisheries and Oceans we have two witnesses with us here today: Nadia Bouffard, deputy commissioner of operations, Canadian Coast Guard; and with her Gregory Lick, director of operations support, Canadian Coast Guard.

Ms. Bouffard, your opening remarks please.

Ms. Nadia Bouffard (Deputy Commisioner, Operations, Canadian Coast Guard, Department of Fisheries and Oceans): Thank you, Mr. Chair.

[*Translation*]

Good afternoon, everyone.

[*English*]

My name is Nadia Bouffard. I'm the acting deputy commissioner of operations in the Canadian Coast Guard. I'm joined by Greg Lick, who is the director general of operations.

We wish to thank you for the opportunity to speak about the Canadian Coast Guard and its role in maritime security. The Canadian Coast Guard has a long and proud history of supporting our partners and allies and serving Canadians. For more than 50 years, the Canadian Coast Guard has been recognized across the country as a symbol of maritime service and safety. Our personnel operate in challenging circumstances, in the harshest of climates, and throughout many of the most remote corners of Canada. The distinct red and white hulled coast guard vessels are symbols of safety, sovereignty, and security.

Our mandate focuses on the safety of mariners at sea, and we deliver programs that are critical to the safe, economical, and efficient movement of ships in Canadian waters. To that end, our direct service includes: aids to navigation and waterways management, environmental response, icebreaking, marine communications and vessel traffic services, and of course, search and rescue. These services are delivered along the single longest coastline in the world and within major waterways, such as the Great Lakes, the St. Lawrence Seaway, the Mackenzie River, and Lake Winnipeg, to name just a few.

Although we have no explicit legislative mandate for security or law enforcement, I will explain today how we have a direct role in supporting our partners that do.

Our fleet is the backbone of the Canadian Coast Guard. The government recently invested $6.8 billion in renewing vessels and helicopters, and I am pleased to report that we are making significant progress on this front.

Of great interest to this committee, perhaps, we recently accepted the last of the midshore patrol vessels into service. These nine new midshore patrol vessels provide new tools to deliver our maritime security program on the Great Lakes and St. Lawrence Seaway and fisheries conservation protection on the Atlantic and Pacific coasts. We are renewing the fleet to maintain our significant vessel and helicopter capacity for the future.

Combined with our various vessels' tracking systems, the Canadian Coast Guard is well positioned to support Canada's security priorities. No single department or agency is responsible for maritime security in Canada. lt's important to recognize that the lead for maritime security always remains the department with the explicit security, intelligence, or enforcement mandate. These include, for example, the RCMP, Transport Canada, the Canada Border Services Agency, and Fisheries and Oceans Canada in terms of our conservation and protection officers, as well as the Department of National Defence.

The Coast Guard has a dual role in maritime security. We provide critical maritime information to security partners, and we help deliver on-water security activities. Coast Guard information is essential to the building of maritime domain awareness, which is the foundation of maritime security in Canada.

Canada uses a layered approach to establish maritime domain awareness. lt's the result of a coordinated effort among federal departments, allied nations, and other levels of government to collect, consolidate, and analyze information and intelligence to support maritime monitoring. Federal organizations use this information for a range of purposes, including marine safety, security, national defence, and environmental protection. For instance, the 96-hour, pre-arrival information report provides information for our security partners on vessel type, cargo, crew, last port of call, destination port, and flag.

Coast Guard vessel identification and tracking systems validate location information reported by vessels and monitor vessel movements within Canada's exclusive economic zone, its maritime approaches, and around the world. This information is collected from a number of sources, including radar, the automatic identification system, and the long-range identification and tracking system, as well as other vessel traffic management systems.

● (1640)

We also collect weather and geographic information as well as real-time reports on commercial vessels and pleasure craft observed by our own vessels.

The long-range identification and tracking system provides positional data on vessels of 300 tonnes or more, including Canadian-flagged vessels, international vessels destined for Canadian ports, and vessels transiting within 1,000 nautical miles of Canada's shores. Inside 50 nautical miles, Canada's Coast Guard automatic identification system tracks vessels of 300 tonnes or more.

These capabilities are critical within Canada's vast Arctic territory where few resources are readily available to monitor the maritime domain. The important role the Canadian Coast Guard plays in providing maritime information is further demonstrated through its presence within Canada's three marine security operations centres, or MSOCs as we call them. These centres are vital in the collection, analysis, and dissemination of maritime information and intelligence. Located on Canada's west coast and in the Great Lakes region, these centres co-locate five federal departments: Fisheries and Oceans Canada and the Canadian Coast Guard, the Department of National Defence, Transport Canada, Canada Border Services Agency, and the RCMP.

The Coast Guard brings great value to the marine security operations centres as it provides close to 80% of the maritime vessel traffic information that our partners require. In the north, the Canadian Coast Guard marine security operation centres monitor all traffic entering the Arctic, including the entire northern Canada vessel traffic services zone. From the centres' watch floors, the Coast Guard sends out reports of all known vessel activity in the Arctic and approaches twice a day.

Our marine security operations centres' personnel liaise regularly with various federal, territorial, and international organizations to maintain comprehensive awareness of activity in the Arctic. This includes but is not limited to liaising with the foreign affairs department; Environment Canada; the Public Health Agency of Canada; the governments of Nunavut, Northwest Territories, and Yukon; the government of Greenland; and the United States Coast Guard.

[*Translation*]

The Canadian Coast Guard plays a second important role in supporting Canadian security by providing marine platforms and support needed for law enforcement, as well as the ability to intervene on water. For this role, the Coast Guard provides ships, equipment, personnel and expertise to federal law enforcement and security organizations in order to provide more effective protection in Canada's navigable waters.

Our ships are routinely active in Canadian waters: along our coasts, in the Great Lakes, all along the St. Lawrence River and in the High Arctic. They usually support law enforcement activities in the course of their daily work and whenever they are needed.

A good example of our routine marine activities is the marine security enforcement team program, jointly operated by the Royal Canadian Mounted Police and the Coast Guard. This joint program ensures that specialized security investigation resources are present in the Great Lakes and St. Lawrence Seaway. The Coast Guard is responsible for the operation of the vessels, the RCMP for all law enforcement activities.

Because of their high visibility, their frequent patrols and their capacity for rapid intervention against potential threats, these teams provide a strong presence nationwide as a deterrent to illegal activities.

In 2012, the Coast Guard began the transition to the marine security enforcement team program, moving from the four original temporary vessels to new mid-shore patrol vessels. In contrast to the original modified vessels, these new vessels have greater range, higher speed and better ability to sail in difficult weather conditions at all times.

In addition, they can communicate securely with other Government of Canada vessels and with the national classified command and control networks. These new vessels were constructed specifically for marine security activities and they have enhanced the Coast Guard's overall capacity to provide effective support to marine law enforcement activities.

● (1645)

Canadian Coast Guard vessels also play an essential role in support of marine security priorities in the Arctic. Each year, from the end of June to the beginning of November, the Canadian Coast Guard deploys six icebreakers: one light icebreaker and a combination of five medium and heavy icebreakers in the Arctic.

Often the only visible Government of Canada presence in many parts of the region, these vessels strengthen Canada's sovereignty by providing essential services to our northern partners and communities.

That includes escorting commercial shipping—

The Chair: Excuse me.

[*English*]

Could you wrap up your opening remarks quickly, so we have adequate time for questions?

Ms. Nadia Bouffard: It will be my pleasure.

[*Translation*]

That includes escorting commercial and military shipping through sea ice to deliver essential supplies to residents of the North, a search and rescue capability, and a first-response role in incidents of pollution.

It also includes our platforms supporting scientific work, such as collecting scientific data at sea, hydrographic charting, mapping Canada's continental shelf and search work, such as the work that led to the discovery of one of the ships of the Franklin expedition.

Also in the Arctic, the Canadian Coast Guard ensures that our fleet continues to provide effective support in security and law enforcement.

This includes our participation in Arctic exercises such as Operation Nanook, in which we have been participating for a number of years, together with our partners from the Department of National Defence.

Similarly to the marine security enforcement team program and its recent transition to new mid-shore patrol vessels, the icebreaking capability of the Canadian Coast Guard will be considerably enhanced in 2022 with the arrival of the CCGS John G. Diefenbaker.

This will be the first polar icebreaker and it will replace the CCGS Louis S. St-Laurent as the flagship of Canada's Arctic fleet.

The CCGS John G. Diefenbaker will be able to serve in the Arctic for longer periods each year and in more difficult ice conditions than we do currently.

[*English*]

In closing, while the Canadian Coast Guard may not have a direct security mandate, legislated or not, we do make an important contribution to Canada's maritime security.

Thank you.

The Chair: Thank you, Deputy Commissioner.

We'll begin our first round of questioning, seven-minute slots, with Mr. Williamson, please.

Mr. John Williamson: Thank you, Chair.

Thank you, Ms. Bouffard and Mr. Lick, for being here today.

I, of course, put my head down at the wrong moment in your address. Did I understand correctly—and I apologize if you didn't say this—that the Coast Guard has no law enforcement mandate? Did I understand that correctly? I might have misunderstood you.

Ms. Nadia Bouffard: That's correct.

Mr. John Williamson: That's correct. It's interesting. I did not know that.

I'm from southern New Brunswick, and I will say that just in my neck of the woods, with some of the islands, we look through American islands to see other parts of our country. So it's not just in the north that the Coast Guard plays a role in terms of our sovereignty and border enforcement. It's even closer to home and often close to American ports as well.

This is a small question. In light of the lack of mandate with respect to law enforcement, there is from time to time a debate about whether or not our Coast Guard officials should be armed. Do you have any thoughts on that?

● (1650)

Ms. Nadia Bouffard: You're totally correct that our vessels and our crew are not armed, with the exception of two vessels on our east coast, stationed in St. John's, which are armed with, I believe it's a 50-millimetre calibre—

Mr. Gregory Lick (Director, Operations Support, Canadian Coast Guard, Department of Fisheries and Oceans): It's a 50-calibre machine gun as well as nine-millimetre handguns.

Ms. Nadia Bouffard: Thank you.

So those particular armed vessels operate in very specialized specific circumstances under the Coastal Fisheries Protection Act, the Fisheries Act, and the Criminal Code, and their activities are conducted within that context by our fishery officers and fishery protection officers under those pieces of legislation.

Mr. John Williamson: Do you have any thoughts on the broader idea? Is it necessary to look at that? Well, actually, let me back up.

Do the coast guards of our close allies—the United States, Britain, Australia—have a police mandate, law enforcement mandate?

Ms. Nadia Bouffard: The role of coast guards around the world and the scope of their authorities are different. The one we're typically aware of and knowledgeable about, as we see on television, is the U.S. Coast Guard for instance that is armed and has a much broader mandate.

The approach in Canada is to have a multidisciplinary approach with various departments involved. While we are not mandated to do law enforcement and security, we support the platform and those that do have those mandates. We will have armed RCMP officers on board our vessels to conduct security and law enforcement operations.

Greg, do you know the other countries? I'm familiar with the U.S., but not the others.

Mr. Gregory Lick: Madame Bouffard is correct in that regard. Every coast guard around the world is very different, and they all have very different roles and mandates. Certainly, as Madame Bouffard has said, we don't have a security mandate but there were very clear and very good examples of where we support our partners like the RCMP on the Great Lakes and the St. Lawrence Seaway with our MSET vessels. That's probably the best example of a joint operation with us.

The other examples are more along the lines of ad hoc security operations where we will carry the security partner to where the particular interdiction would occur.

Mr. John Williamson: That's interesting.

Did you have any thoughts or comments on the broader question of having arms throughout the Coast Guard and not just on the two points you referenced in St. John's, but throughout the fleet?

Ms. Nadia Bouffard: We have studied this in the past and have not been provided any direction to change our current approach, so we are currently delivering the mandate as we are directed to do.

Mr. John Williamson: I thought you might say that.

The Chair: A very brief question please, Mr. Williamson.

Mr. John Williamson: I have to be very brief. There is so much stuff.

I know you mentioned it but you didn't get the chance to go through some of the assets that are based in the north, the Arctic.

Ms. Nadia Bouffard: First of all, they're not based in the north.

Mr. John Williamson: That's fair enough.

Ms. Nadia Bouffard: They operate there for a good chunk of the year, from June to November. I mentioned in my opening statement that we have a combination of six icebreakers of various sizes that will break ice and provide services and be available for various services such as environmental response or SAR operations throughout this period.

Greg, do you want to give the details on those icebreakers?

Mr. Gregory Lick: ×Certainly.

As Madame Bouffard said, we deploy six icebreakers in the north. In addition to those we supply those normal activities of icebreaking and resupply to remote communities, and so on. We also have a couple of vessels that primarily aid navigation on the Mackenzie River. We supply security services not primarily, obviously, but we are there primarily for aids to navigation and search and rescue purposes and monitoring that particular waterway.

I think the other asset you can determine as an asset or something else is the marine security operations centre, which monitors the Arctic. It is one of our other key elements of security support. In this case the Coast Guard in MSOC East is the one that monitors the Arctic for us and supplies the main awareness to our partners, in particular on the marine side of the Arctic.

● (1655)

The Chair: Thank you, Mr. Lick.

Mr. Chisholm, you have seven minutes.

Mr. Robert Chisholm: Thank you very much, Mr. Chairman.

I want to ask a bunch of questions. If I may, I'll ask them one after the other and then give you a chance to respond.

I have a couple of things. The first is that you're part of the 17 departments that are responsible for marine security, which should be no small feat, but there is apparently a marine security working group. I'd like you to give me an indication of how often the working group meets and maybe some idea of when it last met and what were some of the things on its agenda.

The next one is on the territorial issues around the Northwest Passage and the other territorial issues around the Arctic. I would think they must create some interesting tensions between Canada and the U.S. I'd like you to speak a bit about that in terms of the added challenges that situation causes for both the Northwest Passage and other areas in the north.

I'm curious. The AIS and I think also the LRIT system track vessels of 300 gross tonnes and greater. What about vessels under 300 gross tonnes? Are they not a security threat? It sounds like they would therefore go undetected. I wonder if you would comment on that.

Also, in regard to the assets in the north, there has recently been a decision on the west coast to defer the construction of the new heavy-duty icebreaker that's meant to replace the *Louis*. When I think out another seven or eight years, I wonder what that means. When are we looking at decommissioning the *Louis St-Laurent*? What does that do in terms of the Coast Guard's capacity to be able to fulfill its function of icebreaking for security purposes in the north?

Again on assets, there is the Parliamentary Budget Officer's recent report on the Arctic offshore patrol vessels. They were of course promised in 2007, and I believe $3.1 billion was the budget. He suggested that not only are we not going to be able to produce six to eight vessels but now it may be four, and if we wait any longer, it's going to be three. This has implications in terms of the icebreaking capacities of those particular vessels. I wondered if you could comment on that in terms of your assets, or the assets in the north. They are not "your" assets, because they have been assigned to the navy.

I guess that's my last question. Again on that issue, the AOPS, how is that going to work? The Coast Guard has the expertise in the north with regard to staffing these vessels and conducting these icebreaking and surveillance activities with your ships in the north. How is that going to happen operationally with the fact that the navy has responsibility for these however many AOPS vessels, three, four, five, or whatever? How is that going to happen?

If I may, I'd like to ask for your comments.

● (1700)

The Chair: The deputy commissioner has two and a half minutes to answer those questions.

Mr. Robert Chisholm: I've seen her work. She can do that.

Voices: Oh, oh!

Ms. Nadia Bouffard: All right, I'll try, and hopefully Greg will help me out.

Let me start with your last question, very quickly. We are not procurement experts, so we'll try to respond and if we can get back to you with details, we will.

Mr. Robert Chisholm: Thank you.

Ms. Nadia Bouffard: I'm going to let Greg speak about the marine security working group, and I will jump very quickly to the Canada-U.S. relations. I think that's going to answer some of your questions.

Our relationship with the U.S. and the U.S. Coast Guard in conducting our mandate is very close and collaborative and very productive, whether it's in the north or anywhere else, whether it's environmental responses or security. This is demonstrated through a number of groups, meetings, treaties, agreements, and MOUs we have with the U.S. I could give you a couple of examples, but given the time, I won't get into those examples. Suffice it to say that we have a long-standing relationship with the U.S. Coast Guard. We meet regularly and we pick up the phone regularly from Ottawa to the regions. On operations, we work very closely together. There is no difficulty in that relationship. You have to have those kinds of relationships in operations, close relationships.

You asked why 300 tonnes and what happens with the balance of vessels that are smaller. I believe the rule that originally created the limit at 300 gross tonnage came from the International Maritime Organization, and its role and mandate was really focused on safety and risks associated with the safety of mariners and environmental protection.

The Chair: We're out of time.

You may, Mr. Chisholm, wish to follow up on answers to your other questions in your next slot.

Mr. Robert Chisholm: She can just provide that in writing.

The Chair: Well, we can do it in writing or whatever.

But for now, go ahead, Mr. Norlock, please.

Mr. Rick Norlock: Thank you very much, Mr. Chair.

Thank you to the witnesses for attending today.

Since we are studying the defence of North America, how closely and in what areas does the Canadian Coast Guard cooperate with the Canadian Armed Forces with respect to the defence of North America?

Ms. Nadia Bouffard: Here's another example of a very close seamless relationship with the Canadian Armed Forces. We of course have a very close relationship, a partner relationship, with them on search and rescue. I co-chair a SAR committee with Major-General Coates. We do operations in support of them and in collaboration with them.

Maybe you could give the details, Greg, in terms of some of the stuff we do with them.

Mr. Gregory Lick: I think I would add to what Madame Bouffard has said. Certainly in the search and rescue area, our key area where we actually work together is in the joint rescue coordination centres in Halifax, Trenton, and Victoria, where we are actually co-located with Canadian Armed Forces personnel and manage the SAR system from there and all the taskings from there. That's one of the critical areas for search and rescue and our ability to respond effectively to search and rescue.

I think the other area I would note would be the exercising we do, both in the north and around the country. We do numerous exercises with the Canadian Armed Forces, primarily in the search and rescue area, which is our top mandate or top priority. We also do maritime security exercises as well. That usually involves helicopter support with the Canadian Armed Forces, our vessels, and various emergency response teams, which would be primarily from the RCMP, but we all work together in responding to or interdicting certain vessels that we may become aware of through our maritime domain awareness.

Those are the primary areas where I would say we concentrate our efforts in terms of cooperation.

● (1705)

Mr. Rick Norlock: Thank you very much.

Since we're talking about that area, the marine security enforcement team program is a joint RCMP and Canadian Coast Guard project. As you mentioned, that was established in 2005, and it enhances marine security in the Great Lakes and St. Lawrence area, in particular. Can you tell me what sort of interdictions this enforcement team would be targeting? Are there security threats to Canada that MSET would be confronting? Then, what kind of resources and assets does the Coast Guard have to meet that responsibility?

Ms. Nadia Bouffard: With regard to the assets, we spoke in our opening statement about the renewed vessels going into the St. Lawrence Seaway and the Great Lakes, with greater capacity to support our partners, such as the RCMP.

I'm not sure about the first question with respect to the specifics of MSET's security role.

Mr. Rick Norlock: I know they have a specific job.

Ms. Nadia Bouffard: Yes.

Mr. Rick Norlock: You, along with the RCMP, are targeting certain entities or certain threats on the Great Lakes and the St. Lawrence. I'm asking you about the kinds of threats you have encountered since 2005, some of the operations you've been in, and some of the successes, or challenges for that matter.

Ms. Nadia Bouffard: Do you want to try that?

Mr. Gregory Lick: Yes.

Without getting into the details of all the actual interdictions that have occurred, I would say that most of the interdictions with personnel, vessels on the water, and so on, have primarily been around Criminal Code actions. I certainly don't have all the details of those types of interdictions, but they've primarily been around the Criminal Code.

Those could be anything from something as simple as alcohol on boats up to something like smuggling or anything like that. Some of the incidents have occurred and are out in the public domain, such as incidents of smuggling in the Cornwall area.

Mr. Rick Norlock: You're referring to illegal and illicit cigarettes, right?

Mr. Gregory Lick: It could be something like that. Certainly smuggling is something—

Mr. Rick Norlock: Don't be afraid to say what it is; I think we all read the newspapers.

The other thing, of course—and this leads to a previous question—is that we know that many of the firearms used in Canada illegally are exported from the United States into Canada. “Smuggled” is the right word to use. I'm wondering if that forms part of the MSET duty.

Ms. Nadia Bouffard: I don't know. But I would say that with respect to specific interdictions and enforcement regarding those interdictions, really the RCMP would be the better organization to pose those specific questions to. They would have the answers.

Mr. Rick Norlock: Thank you.

Some of the areas that have been previously.... You talked about the new assets you have that permit you to do your job much better. We do have the longest coastline in the world, and we have one of the smallest populations. I guess my kudos would be that we do a darn good job of protecting those people who utilize the coastline for everything from commercial to pleasure to other occupations.

Since we are talking about the defence of North America, I just wonder what kind of interoperability you have with the Canadian Armed Forces, the RCMP, and other entities that are meant to keep us safe, and also with the U.S. entities of the same sorts.

Ms. Nadia Bouffard: Those are all good questions.

Mr. Gregory Lick: With respect to interoperability.... We can take them one at a time, but they all have very similar themes in terms of what we're working on.

I would say that one of the best examples with respect to the Canadian Armed Forces in terms of interoperability is one of the systems that is part of a project we're actually in the middle of developing and installing on board both the Canadian Coast Guard, particularly the larger vessels, and some of the Royal Canadian Navy vessels, termed IMIC3.

It provides an unclassified view for those particular vessels as well as certain operation centres in both the Canadian Armed Forces and the Canadian Coast Guard. It provides that national maritime picture of what's out there, in an unclassified format, so that both the ships and the shore side can actually see. That is providing, as we complete the project, a better sense from both the navy and ourselves so that we both have that common understanding, that common picture of what's out there that could be a threat.

● (1710)

The Chair: That's all of your time.

Ms. Murray, go ahead for seven minutes, please.

Ms. Joyce Murray: Thank you for being here to help us understand the Coast Guard's role.

In previous testimony we've asked a lot about the threats to the Arctic as we think about the defence of North America. I would say 95% of the witnesses answered that the threats are not military threats, they are threats that have to do with melting ice due to climate change, increased vessel traffic, the security of people so the search and rescue aspect, the potential for pollution and spills, sovereignty, and so on. So that's a very important aspect of what you do with your icebreakers and other measures.

According to the Auditor General's office, the fall 2014 report of the Commissioner of the Environment and Sustainable Development, there are no real performance measures for Arctic icebreaking services nor measures for when users requested service but it wasn't provided. Are those measures something that the Coast Guard is planning to put in place?

Ms. Nadia Bouffard: We received the commissioner's report and we are assessing it. We will be looking at what improvements can be made to Coast Guard services in the north.

You are correct that the qualification of the risk is not one of security in the north, it's everything else that we've talked about, including environmental, population, providing services, search and rescue—

Ms. Joyce Murray: Excuse me, I have about four questions so I hope the answer for all of them will not be that you're considering the report.

Here's another concern. According to the commissioner the Coast Guard believes that it has the resources to address current traffic levels even though there were deficiencies in response at times and so on. But according to the commissioner the Coast Guard noted that it does not have sufficient resources to respond to an increase in demand for services and we know that it's happening due to the ice melt. Does the lack of resources to respond tie into lapsed funding? What has been the total of lapsed funding for the Coast Guard since 2006? The lapse is what I would call planned clawbacks.

Ms. Nadia Bouffard: I don't have that figure with me, but I will start by saying that the increased traffic qualification perhaps is overstated today. There's no doubt that at some point we're going to have to look at what assets we have to serve and address the increased risk associated with increased traffic.

For the last two or three years, traffic in the north has gone from 250 to 350 voyages, compared to millions of voyages in the south. It's not a huge increase. There is no doubt though that with increased activity in the north that may increase in the future.

Ms. Joyce Murray: Thank you. So that's a 50% increase, very roughly, in—

Ms. Nadia Bouffard: That's in a very large area.

Ms. Joyce Murray: Yes, and a 50% increase is significant. I would like a written response to the question of lapsed funding since 2006, please.

Ms. Nadia Bouffard: I would be happy to provide it.

Ms. Joyce Murray: In terms of the services you provide, the icebreakers are important. Your two most capable icebreakers are scheduled to be decommissioned in five to seven years but they will be replaced by one. It seems as though you are planning for a reduced ability to provide support through icebreakers. Has there been an analysis of the risk you're addressing with the icebreakers and is it related to reduced risk, which would be strange given the traffic increase? Or is that a resources issue as well, replacing two with one?

● (1715)

Ms. Nadia Bouffard: I'm going to answer that generally, and then I'll ask Greg to provide some details.

Replacement of fleet is also supplemented by maintaining the current fleet in operation until we have the new icebreakers coming in. We don't consider the replacement of icebreakers coming in, like the polar, for instance, as reducing our capacity and our assets and our service.

I mentioned in our opening statement that the polar that we are building is going to be bigger and better and provide longer time service in the north.

Ms. Joyce Murray: Thank you.

That does bring up another question that I wanted to address, which is in terms of icebreaker deployment time. Since 2011 the Coast Guard has decreased by 33 ship days the total time that it planned to deploy icebreakers in the Arctic. In addition, in two of the last four years, the Coast Guard operated one less icebreaker than intended due to maintenance issues—so it had old icebreakers—and it didn't meet its planned deployment time. If we already have missing planned deployment times, reduced deployment times, maintenance issues, and replacing two with one, can you explain how the Coast Guard will meet the security and defence needs in the north? Or is this a matter of inadequate resources to do the job you're being asked to do?

Ms. Nadia Bouffard: Greg here is responsible for setting up our annual plans every year in terms of what actually goes out, so I think he's best placed to provide you with an explanation of how we determine what's appropriate in terms of service.

The Chair: A very brief answer please.

Ms. Joyce Murray: All right, I had another question I was going to insert, but go ahead with your answer to that.

Mr. Gregory Lick: Thank you very much for the question.

Yes, the Auditor General, through the Commissioner of the Environment and Sustainable Development, did note those particular statistics that you outlined there. I think it's very important though to say that we are meeting our level of service in the Arctic at this point in time, at least within a few days here and there, or a few hours here and there. That's the important statistic to recognize here I think.

In terms of the number of vessels deployed to the Arctic, like a car we also have to look at maintaining those assets. These assets don't require a two-hour time in the garage type of thing. I think everybody can understand that. It requires months and months to maintain them. In the case where we are looking at vessels of the age and condition that ours are at this point in time, what we needed to do, and Madame Bouffard outlined it in her opening remarks, is extend their life to the point where we're able to renew their capability with a fleet renewal plan.

The Chair: Thank you, that's time.

Mr. Bezan, please.

Mr. James Bezan: Thank you, Mr. Chair. I want to welcome you both to the committee and thank you for being here. I have spent a lot of time on the Arctic, and it is a concern. As Canadians we all love the Arctic and it's an area that is undergoing some new opportunities and challenges tied to the situation up there. I had the opportunity to be on the *Amundsen* in Hudson Bay a few years ago and appreciate the great work that it's doing up there in mapping and environmental research, as well as having that presence pulling into Churchill and allowing people there to see the Coast Guard in their backyard.

Now we have touched on the replacement of the *Louis S. St-Laurent*. Can you talk about the new heavy icebreaker that's coming online to replace it and what capabilities it has versus what we currently have, and how that works into the protection of our international waterways and protection of our sovereignty? Also, could you elaborate on how this new icebreaker compares to those of other Arctic nations?

● (1720)

Ms. Nadia Bouffard: I'll start very generally, but Greg has the expertise with respect to the vessels. My understanding of the new polar icebreaker we're expecting by 2022 is that it will have the capability of spending longer periods of time up north. It is stronger and it has more capacity in terms of icebreaking. Those two combinations will provide a longer season of icebreaking and other services that the icebreaker will provide in the north.

Mr. Gregory Lick: Further to that, in order to get that longer season, both at the start of the season and at the end of the season... and we're talking about three months in total, about a month and a half at either end. That's the time period we're looking at in terms of a mission for that particular vessel. That requires a higher ice class in order for the vessel to actually operate in different areas and farther out than our present fleet can. That's another aspect that's important for the vessel to be able to go farther out into our Arctic domain.

In terms of your question on marine security, or the surveillance aspect of it, one thing we were very good at doing in this particular case was working with all of the marine security partners. Because of the idea—as we have outlined all the way through our testimony here—of the support element that our Coast Guard performs within our mandate, we worked with all our security partners, whether it was RCMP or whether it was Canadian Armed Forces, to outline what their requirements were for this type of vessel in the Arctic. Just as an example of one of the ideas, a very complex operation centre is on board the vessel, which will supply the partners with the communications ability, the surveillance capability, that they need and that they had outlined for us in terms of the requirements on the vessel.

That's how we built capability into the vessel.

Mr. James Bezan: Thank you.

We have also been building up at Nanisivik a new berthing and refuelling facility. How will that enable the Coast Guard to do more in the Arctic than we are currently doing?

Ms. Nadia Bouffard: I'm sorry, I missed the first part of your question.

Mr. James Bezan: In Nanisivik there's a new refuelling and replenishment facility, which was established predominantly for the navy but will also be used by the Coast Guard. How will that facility enable the Coast Guard to do more than what they currently are doing in the Arctic?

Mr. Gregory Lick: Essentially it provides us with exactly what you would think. It provides us with a refuelling capability in the Arctic. Normally we have done it in the past through barges, through ship-to-ship transfers. This provides just another capability or a solution for the Arctic in terms of refuelling our vessels.

Mr. James Bezan: One thing that you didn't touch on in your response, Mr. Lick, was with regard to the new icebreaker that's going into construction. How does it compare with other icebreaking capabilities of other nations from a coast guard standpoint?

Mr. Gregory Lick: I could compare it with our present fleet, which might give you a good sense of what we're comparing it with. There are comparisons with a number of other icebreakers around the world, but sometimes, because of the age of the vessels and when they were built, some of the classifications are a little bit difficult to compare.

Essentially, however, just roughly, our current *Louis S. St. Laurent* is a polar class 4, approximately, and what we're looking at with the polar icebreaker—this is something I will confirm with the committee—is a polar class 2. That gives you a sense of the difference between our current fleet and others. Certainly when we're comparing it with, say, the U.S. Coast Guard's breakers that are presently there, the *Healy*, the *Polar Star*, and so on, it will have higher capability than those particular vessels to get into areas, as I said, that we can't get into now or certainly go into very rarely; or we can go into them longer.

The Chair: Thank you.

Mr. Chisholm, please, you have five minutes.

Mr. Robert Chisholm: Thank you.

The *Louis S. St-Laurent* was commissioned in 1969, I believe. I think it was recently suggested that it would be decommissioned in four to six years. But I understand you're going to have to maintain it, because the new one, the new polar, won't be coming online until 2022. What will it cost to extend and how long will you be able to extend the *Louis S. St-Laurent*?

Then I want to go back to my question on the AOPS in terms of vessels. Will you be training the people who will be operating these vessels in the Arctic? Or will you be operating them yourselves?

My final question has to do with the Bell helicopters and when we can expect those to be available.

● (1725)

Ms. Nadia Bouffard: I'll start very generally and I'll ask Greg to supplement. The Coast Guard is planning to spend about $360.4 million over 10 years on a vessel life extension and mid-life modernization program. So that's not just on the polar; it's on all our fleet. This program was announced in February 2012 and consists of a set of interim measures to extend the life of Canadian Coast Guard vessels. It includes existing icebreakers, to ensure the continuity in service delivery of its current fleet, and anticipation of new vessels that are coming down the pipe. To date, we've spent about $30 million in terms of work that has been completed.

Mr. Robert Chisholm: Excuse me. Sorry. I appreciate that, but that doesn't deal with my specific question and we don't have much time, so maybe I'll ask Mr. Lick.

Ms. Nadia Bouffard: Greg could give you the details about the polar, if we have it. As I said at the beginning, we're not the vessel procurement experts from the Coast Guard.

Mr. Gregory Lick: Certainly what I would say is that we've committed to ensure that the CCGS *Louis S. St-Laurent* and the rest of the fleet is in...and we put money into it in order to extend their lives until they're renewed. I don't have the number with me, but I think we can commit to getting that back to you.

Mr. Robert Chisholm: And the AOPS; how are you going to...?

Mr. Gregory Lick: The AOPS project is obviously a project on which we've been working closely with the Royal Canadian Navy. I would say in particular that we've had recent exchanges in the Arctic, where we have Royal Canadian Navy navigation officers who come on board our vessels and work with our officers aboard in terms of gaining expertise in icebreaking, ice knowledge, ice observation, and all the elements they will need to safely navigate in the Arctic.

Mr. Robert Chisholm: The last question was on the Bell helicopters. I had a meeting last spring with the public works folks, and there was some question about the capacity of these helicopters to do what the Coast Guard wants them to do. I wondered if you could just tell me sort of where that's at.

Mr. Gregory Lick: Certainly with respect to the current light helicopter contract that was announced earlier on in the year, we are currently in a contract with Bell Helicopter in Montreal to produce the 15 light helicopters that we contracted for. They're in production. They absolutely meet our requirements in terms of the capabilities we asked for in the bid process, and we're confident that they'll be delivered on time and on budget. We have no issues with respect to that contract.

Mr. Robert Chisholm: Are there other helicopters involved in that particular tender?

Mr. Gregory Lick: No, I think you would have seen that, following the contracting, there was a separate process to look at our medium helicopters. That process is ongoing, and that announcement has not yet been made.

Mr. Robert Chisholm: Okay.

So the capacity in the north now, as far as you're concerned, to be able to meet search and rescue needs is that you have the assets you need.

Ms. Nadia Bouffard: The answer is yes, but as I said earlier, if traffic increases over time, at some point in the future we're going to have to look at it. But yes, currently we feel that we have.

Mr. Robert Chisholm: How much of an increase would that be; is there a threshold?

Ms. Nadia Bouffard: That's a good question.

Mr. Robert Chisholm: You talked to Ms. Murray about 50% not being anything in particular to worry about, the 250 to 350. So what —

Ms. Nadia Bouffard: That's something we're going to have to look at in the future, but at the current moment we feel we have what we need.

The Chair: I will exercise the chair's prerogative to ask just a couple of final questions. You touched on it, and at our last meeting Vice-Admiral Norman spoke to the changes and considerations with regard to crewing aboard Coast Guard vessels in the future. You've addressed that somewhat here today, but are the facilities on the existing and new icebreakers being designed, in terms of the temporary renovations or refits on the current vessels and on the new one, to accommodate a permanent presence by Royal Canadian Navy personnel?

● (1730)

Mr. Gregory Lick: Mr. Chair, I think I understand your question. In terms of the requirements for the new icebreakers when they eventually come—and the government does intend to fund them—we would look at it with our partners. So as part of that, when we develop our requirements, like the navy does, we consult with the partners on what their requirements might be. In terms of the polar, as an example—and I talked about that earlier—we did talk to our various marine security partners in this case and asked them what their requirements are. To be honest, I don't have that kind of detail in front of me, but we can get back to you in terms of the polar characteristics, maybe with respect to what berths are available on board.

The Chair: But certainly the Department of National Defence, more specifically the navy, seems to consider the Coast Guard as the first responder increasingly in the future, and there will have to be, built on your current work with the RCMP in southern waters, certainly an increased presence aboard your vessels by Royal Canadian Navy personnel.

Mr. Gregory Lick: I do remember the number now off the top of my head. Certainly with the polar, it has a capacity for approximately 100 personnel on board. In fact, the crew is only about half of that. That extra berth availability on board is meant for a variety of missions, whether it's for scientific or security missions or environmental response. It could be a whole range of missions. Certainly there is extra capacity on board to handle those types of missions.

The Chair: Thank you very much, both of you, Deputy Commissioner Bouffard and Director Lick, for being with us today. We look forward to continued updates as the new vessels approach launch.

I would just remind members that our next meeting is scheduled to hear the minister taking questions with regard to the supplementary estimates. We will advise you of the location of that meeting. The clerk assures me that it will be in Centre Block. We'll see you on Tuesday.

This meeting is adjourned.