HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on National Defence

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

EVIDENCE

Thursday, March 29, 2018

Chair

Mr. Stephen Fuhr

Standing Committee on National Defence

Thursday, March 29, 2018

● (0845)

[*English*]

The Chair (Mr. Stephen Fuhr (Kelowna—Lake Country, Lib.)): Good morning. I'd like to welcome everybody to the defence committee this morning to our final meeting discussing Canada's relationship with NATO. It's been a long study, but it's an important topic. I'm really pleased to see our last witnesses come before the committee today.

First, from NATO, we have Jamie Shea, deputy assistant secretary general, emerging security challenges. As an individual we have Madeleine Moon, U.K. member of Parliament for Bridgend, from London. As an individual we have Rafal Rohozinski, consulting senior fellow, future conflict and cyber security, International Institute for Strategic Studies.

Thank you, all, for coming today. We'll start with Jamie Shea.

Sir, you have the floor for your initial opening comments.

[*Translation*]

Dr. Jamie Shea (Deputy Assistant Secretary General, Emerging Security Challenges Division, North Atlantic Treaty Organization): Mr. Chair, let me begin by thanking you for inviting me to take part in this committee meeting. Although I am not in the room with you and am participating by video conference, I am very honoured to have the opportunity to address you.

Before I begin my preliminary remarks, I want to express special thanks the High Commission of Canada in the United Kingdom for facilitating this communication today. I am not at NATO headquarters in Brussels, but in London, at the High Commission of Canada in the United Kingdom.

I am speaking French simply to show you that I am fully prepared to respond in English or French to any questions addressed to me during the question period. However, since I can speak English twice as fast as I speak French, I hope you will not mind if I deliver my opening remarks in English.

[*English*]

First of all, if I've understood this correctly, Mr. Chair, your focus today is on cyber issues, cyber defence, and cybersecurity. That's where I'll begin, but I'd just like to say before I start that as somebody who's been around NATO for a very long time, my division, emerging security challenges, deals with a broad portfolio of issues, including cyber issues, but also counter-terrorism, nuclear policy, and strategic forecasting.

If afterwards the members of the committee want to enlarge the discussion to other aspects of NATO's current postural policies, please, I'd be more than happy to stray off the reservoir—or the reservation, if you like—and intervene on that too.

On cyber, you could of course spend many a happy hour talking about this, because it's such a complicated, fast-moving topic. Let me at least briefly try to give you a sense of where NATO stands. For us, cyber represents three very key strategic challenges. The first one, to paraphrase an American sociologist, Clay Shirky, is “here comes everybody”.

Cyber for the first time allows virtually anybody in the world to become a strategic actor—and for a very small investment compared with what states used to have to invest to develop significant capabilities. Cyber allows anybody to attack anything from anywhere at any time. It totally obliterates the traditional security refuge of geography, of being behind borders and declarations of neutrality.

For states or for organizations like NATO, for the first time we have to defend everything all the time, whereas security policy, as you know, for most centuries allowed you to define a particular adversary and particular strategic access and to focus most of your resources on certain nevralgic points. Now you have to make difficult decisions over priorities, whether that's critical infrastructure, the civilian sector, the banking sector, or telecommunications and, as the threats from cyber keep shifting, from one sector to the other. You need an enormous agility to be able to keep up with the changing threat landscape, particularly when a company like Symantec identifies upwards of two million pieces of new malware on the market every year.

The second issue, of course, is that cyber obliterates the old distinction between being at peace and being at war. It condemns us to live in a kind of permanent grey zone, neither peace nor war, where everything is contested and where we are subject to attacks, major or minor, every day of the week. Most of these attacks are below the traditional NATO article 5 threshold, which used to be clearly identified in terms of tanks crossing a defined frontier.

Cyber is in that sort of grey zone where we sometimes find it difficult to determine what is an armed attack or its equivalent, or what is a hostile attack and what is simply a nuisance. Therefore, there's a difficulty in knowing how to respond, because on the one hand you want your response to have an impact, and on the other hand you want to avoid an escalation into a crisis that probably goes beyond where you would like to be.

There are issues of how to classify attacks, how to attribute attacks and how quickly to do so, how much evidence you need before you can make attributions, and what the appropriate response is. Is it diplomatic? Is it economic? Could it even be military? NATO certainly has said, back at our summit in Wales in 2014, that at a certain threshold a cyber-attack indeed could be considered the equivalent of an armed aggression and therefore provoke the activation of article 5 and a NATO response. However, what that threshold would be is something that we have kept ambiguous, because we believe that ambiguity serves the purpose of deterrence.

● (0850)

The third and final opening strategic point about cyber is that it clearly cannot be dealt with by using the tools that you traditionally have within your own organization. When it comes to traditional collective defence—and Canada is participating in that, of course, in leading the multinational division in Latvia at the moment—we have within our own organization the tanks, the aircraft, and the artillery we need, even if sometimes we would like it to be more modern or more ready.

When it comes to cyber, we find that in order to be effective we have to depend on others, the private sector, for instance, which is responsible for 90% of the networks where most of the innovation and much of the cyber-intelligence come from. In the cyber-field, you're only as good as your ability to form those partnerships, to persuade other people to help you out, and to build a true ecosystem for handling the challenge.

Those are three introductory messages.

Very briefly, what is NATO doing? There are four areas. I'm more than happy, of course, to go into these with all of the members of the committee in as much detail as would be helpful to you.

Number one, we of course need to defend our own networks. It sounds simple. It's the starting point, but in a complex organization like NATO, it isn't so simple. We have 55 different sites to protect. We have 35 different IT systems. Some are new and some are legacy systems. Of course, when you combine the old and the new in the cyber-world, you have many more interfaces and therefore many more vulnerabilities and attack surfaces. We have built up, over the last few years, a comprehensive NATO cyber-incident response capability—we call it NCIRC—situated within SHAPE in Mons, that provides our civilian and military networks 24-7 coverage.

A second part of this is bringing the intelligence community, which has forward strategic warning of cyber-attacks, together with the technical community. In the cyber domain, particularly for incident management, it's very important to make sure that what you are seeing corresponds to what you are hearing. In other words, the intelligence piece corresponds to what you are actually seeing in the networks, because the one could, of course, alert the other. We therefore have a cyber-threat analysis cell that brings these communities together.

Mr. Chair, as you know from the time that you and the members of the committee visited NATO headquarters in Brussels, we have established a joint intelligence and security division precisely to bring more of the national intelligence feature into NATO so that we can have better situational awareness and better correlation of the data we are receiving.

Of course, also in this field, as you know—and this is true of all of us—part of the protective task is identifying your critical dependencies. You are often amazed to discover that just when you thought that you had mapped out your cyber-ecosystem, identified all of your critical networks, and brought them up to the same level of protection, there is some new supply chain risk from some other system that you realize is connected to yours, and you don't know exactly what the level of security is there. That constant mapping is important, too.

The second level of our efforts is assistance to allies. We really want to be the heart of a number of cyber-defence services that could help our allies become more resilient at the national level and learn from each other's technologies, people, processes, education methods, and experiences so that we can increasingly benchmark standards in an objective way by allowing allies to assess themselves voluntarily and then compare the results with others.

This is in the form of a cyber-defence pledge that is now in its second year. Indeed, I am hoping that, in the next couple of days, Canada's submission, its self-assessment for the second cycle, will arrive at NATO headquarters. Of course, we'll compare that with what Canada told us just a year ago. I know, from your own national activities over the past few months, there's been a surge of effort in this area. Therefore, I'm sure you can add many good new things to report to us.

● (0855)

The pledge, as I said, allows for comprehensive benchmarking: it allows NATO to have a comprehensive overview of the strengths or weaknesses in the cyber realm of our allies, and therefore to help with feedback and advice; and it encourages nations to both devote more resources to cyber by identifying key NATO priorities and to also join themselves up more at the national level over the various ministries and different departments. Many allies have told us that the pledge was the first comprehensive stock-taking that they were asked to carry out.

Very briefly, before I stop, there are two final elements. The third is where perhaps we might get some questions and discussion, because it's the most ambitious and the most demanding. At our summit in Warsaw in 2016, we declared cyber as an operational domain. In other words, we have to fit the virtual world and cyber together with the four traditional areas of crisis management and conflict: air, sea, land, and space. We have to fit cyber as the fifth domain and therefore understand the implications of conflict in the cyber space and which instruments and doctrine we need to be able to deal with that on the assumption that all future conflicts will probably, or inevitably, have a cyber dimension. Therefore, how does cyber fit with nuclear deterrence, conventional defence, and missile defence, into NATO's posture? What can it do, what can it not do, and what kinds of new capabilities do we need?

You've probably seen, Mr. President and members of the committee, that we've agreed now to establish a cyber operations centre and to incorporate into NATO's posture voluntary national cyber contributions that individual allies who have these capabilities would be willing to make available to us. That work is ongoing.

My last point is that we in NATO of course want to be political in the cyber domain, and not simply technical military, because as with every other area of NATO engagement, we see our security as depending upon political initiatives, arms control initiatives, confidence-building measures, and agreed restraints, and not just in the development of new weaponry. Therefore, we are very engaged—even if we're not negotiating—in the whole domain of international law as it applies to cyberspace, and how we can work with the EU, the United Nations, the OECD, and other institutions.

If your committee is interested in this, I would refer you to the two Tallinn manuals that our centre of excellence has produced on the international law governing cyberspace, which are helping to drive this intellectual debate forward.

I will stop there, but again, I hope we can have good, productive discussion with the committee in the direction you wish to follow afterwards.

Thank you again for the privilege to be able to speak to you this morning.

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

MP Moon, the floor is yours.

● (0900)

Ms. Madeleine Moon (Member of Parliament for Bridgend, United Kingdom, As an Individual): Thank you.

I can't say that I'm going to be as erudite, as flowing, as Mr. Shea was, particularly in French. I can give you a bit of Welsh, but my French is fairly limited.

Thank you again for inviting me to appear before the Standing Committee on National Defence. I want to start briefly by recognizing the critical role that Canada has played in setting the NATO alliance and the Parliamentary Assembly.

It could be argued that in fact the alliance started when Canada agreed to send more than one million people to serve in the Second World War, including over 14,000 who joined the allies in Normandy on June 24, 1944.

Across the NATO alliance, we do remember the work of Escott Reid, Lester B. Pearson, and Louis St. Laurent, who floated the idea of a temporary military alliance in the north Atlantic region to ensure the stability of democracy and freedom in western Europe, in the face of the communist threat. The North Atlantic Treaty was signed on April, 4, 1949, and included article 2, which became known as the “Canadian article”. The enthusiasm and commitment of Canadian Senator Wishart McLea Robertson and British MP Sir Geoffrey de Freitas initiated the first gathering of parliamentarians in July 1955 to create the NATO conference of parliamentarians, the forerunner of today's NATO Parliamentary Assembly. Senator Robertson was elected as the first president of the new assembly in 1955, and was the first of many important Canadian presidents, vice presidents, chairs, vice-chairs, and rapporteurs who served the alliance and the assembly.

I want to look at today's pressures. I plan to focus on the role NATO plays in the maritime and space domains, and in advancing a women, peace, and security agenda. I've prepared, on behalf of the defence security committee, reports on the maritime and space domains. I will be speaking to those.

Maritime is first, because NATO in many ways was primarily a maritime alliance. The transatlantic link is vital to all member states, but has long been neglected. I think it's been said that you cannot win a war in the Atlantic, but you can certainly lose one there. Control of the sea is vital for communication and freedom of movement, both of which are crucial aspects of NATO's operational efficiency. Alliance naval forces guarantee NATO's strategic defence and are central to the promotion and protection of political, economic, and diplomatic interests.

However, member states' navies, on the whole, have been shrinking in size, largely due, as in most fields, to the increasing cost and sophistication of vessels. This has had two major effects: allied navies have shrunk and the capability gaps have increased. A ship, no matter how sophisticated, can only be in one place at one time. The effect of this trend is that the U.S. is now the only member state with truly full spectrum capability.

Why is the maritime environment so crucial at both a local and global level? Currently 95% of trade is conducted on sea routes, 80% of hydrocarbons are transported by sea, and 95% of Internet traffic goes through undersea cables. A closer look shows that 80% of the maritime trade passes through eight choke points, three of which are crucial to NATO in the Mediterranean, the Black Sea, and the Red Sea.

The figures show that freedom of the seas is a driver of global economic interests. However, it is worth much more than this. Free seas are also a global norm and can be a tool to use in reinforcing international order.

With 80% of the world's population living within 60 miles of the coast, and 75% of the world's major cities being littoral, plus the use of sea lanes growing at 4.7% a year, the maritime domain is only becoming more critical to the alliance.

Threats at sea are increasing. I'll cite just one example. As the Arctic Ocean becomes navigable, the bastion concept is being reinforced with increased numbers of Russian submarines present. The threat to the GIUK gap and our undersea cables is growing. All aspects of naval capability serve as an essential enabler of deterrence and as demonstrators of political will and power.

● (0905)

Naval assets also provide the capacity to manage crises by providing expeditionary capabilities, sea control and denial, and logistical support to amphibious operations, including the enforcement of embargoes and no-fly zones, and the provision of humanitarian assistance. Naval forces also often offer the easiest and quickest route to providing co-operative security by working in partnership on capability building, training, joint exercises and, less directly, through naval diplomacy.

Here I will just put in a quick mention of port security, which we must raise our game on.

I want to move on to the new frontier of space. It's complicated but increasingly important area. Over the last few years, space has become a key pillar of NATO defence. Space is increasingly at the forefront of the security policy and planning debate, and a key area of global geopolitics.

The cost of operating in space is high, and as such the agenda lends itself to collaboration, rather than competition, among the alliance. This is perhaps reflected as a push for some kind of space code of conduct. As far as NATO is concerned, the alliance has no official space policy, but has released an allied joint doctrine for air and space operations. This is an area that NATO should now be looking to consolidate.

The current picture in space is complex. Satellite constellations are now vital for the efficient functioning of modern infrastructure, both military and civilian. Indeed, one challenge is the indistinguishability of military and civil spacecraft. It's estimated that 40% of all satellites are military, but that's not to say that civilian craft can't also be used for military functions.

Over the last two decades, both the breadth and depth of possibilities have expanded. A flood of new actors, both national and commercial, is making the three principal geocentric orbits congested and dirty. In part this is due to almost every country now having a satellite, or a stake in space. We've now got approximately 1,100 satellites in orbit; some are saying there are as many as 1,500. On top of this, in recent years new and dynamic commercial actors have ignited a second space race. Costs, although still high, are falling, and this is opening the space arena to many more participants and many more potential threats and problems.

Finally, as the North Atlantic Treaty was being signed, women were leaving the many vital roles they had played in the armed forces during the Second World War. The important role of women in peace and security did not return to the main political agenda for some time. In 2000, the United Nations Security Council Resolution 1325 encouraged member states to involve women and integrate a gender perspective in multilateral security initiatives such as peace settlements, peace missions, disarmament, demobilisation, and reintegration programs.

Additional resolutions now include a focus on sexual violence in the context of armed conflict, and recognizing sexual violence as a serious violation of human rights and international law. Recognition of women's roles in post-conflict recovery and actively integrating them in peace-building, peacekeeping, and aid management, is growing.

More recently, the agenda has expanded from a focus on women and girls to include the impact of conflict on gender relations, recognizing that sexual violence in conflict affects men and boys and those secondarily traumatized as forced witnesses of sexual violence against family members. It also emphasizes the positive role that men and boys play in promoting gender equality during reconstruction efforts. We now recognize that efforts to build peace must benefit both men and women equally.

NATO has taken on all these objectives and subsequent resolutions at different levels of the alliance's structures and activities. The 2013 Parliamentary Assembly report recorded nine strategies deployed by Parliaments of NATO member countries that contribute to the promotion, implementation, and monitoring of the women, peace and security agenda. In four areas there was a commitment to change—the areas of gender-balanced Parliamentary leadership; legislative initiatives; influence and oversight through debates, questions, and reports; and civil society engagement.

● (0910)

This update was published in 2015. The Committee on the Civil Dimension of Security will be sending out another survey this year. The results will be presented in Halifax by Clare Hutchinson, the NATO representative for women, peace, and security, who will be with us to talk about the results.

I'll end on that positive note. Canada has been a key member of the alliance since its inception, and I have many Canadian colleagues.

I look forward to answering your questions.

The Chair: Thank you very much, MP Moon.

Mr. Rohozinski, the floor is yours.

Mr. Rafal Rohozinski (Consulting Senior Fellow, Future Conflict and Cyber Security, International Institute for Strategic Studies, As an Individual): Thank you very much. It's an honour and a privilege to be in front of the committee in person this morning.

I'd like to predicate my brief comments with a few remarks on position I take on these issues—in other words, where I'm coming from—and the importance of addressing this as a core issue both for Canada's relationship with NATO and Canada's national security.

My remarks this morning will be informed by essentially four activities that I've been involved in over the last 10 years.

First of all, for the last 10 years I've been one of the co-convenors of a Track 1.5 process with the Russian Internet Security Council that has dealt with the issue of cyber-norms and cybersecurity. Initially started as a NATO process 10 years ago, it has continued since then as an engagement activity, year on year, that has created a focal point for at least being able to understand the normative aspects of the use of cyberspace in security.

Second, I'm also a co-convenor, along with American and U.K. colleagues, of a Track 1.5 dialogue around the military use of cyberspace between the U.S., the Russian Federation, and the People's Republic of China.

Third, I'm citizen adviser to the United Nations counterterrorism executive directorate on combatting violent extremism and terrorist use of cyberspace, which brings together industry partners and nation-states around these issues.

Finally, I'm an expert to the World Bank digital economy working group, which is attempting to quantify the economic impact of information and communication technologies worldwide.

Why all this is important is simply the following. As Mr. Shea pointed out, NATO has declared cyber to be an operational domain for NATO countries, and yet this is the domain in which we have the least experience in understanding the levers of escalation and de-escalation. It is also a domain that has come into being at a time of the greatest tensions and degradation of channels of communication between NATO countries and its potential peer partners.

In my remarks, I want to cover two separate areas. The first area is simply understanding the impact of the cyber-environment on national security writ large. Absent understanding of this impact, it's difficult to be able to separate where we have issues that are purely domestic from those that can be influenced or otherwise made more serious by external partners. I also want to talk about the dangerous entanglement between cyber and security at a technical level and a social one—in other words, its social and political impact. I then want to briefly turn to the impact that this now has on NATO's position vis-à-vis cyber in terms of an alliance from our own preparedness point of view and also our relations with potential peer competitors in this field.

The first thing to recognize is that the foundation upon which we have built the global economy and the Canadian economy is largely made of sand. Currently, by projections of the World Bank, 26% of the global GDP will be dependent upon the digital economy by 2025. Of the $107 trillion GDP globally, $1 trillion is being spent on cybersecurity. Why is this the case? From statistics released by the Council of Economic Advisers at the White House in the last week, an amount between $57 billion and $106 billion is attributed to cybercrime losses each year in the U.S. This is occurring because the infrastructure of the Internet at a basic level was built for resilience rather than for security. At its basic, there is less security built into either the technology or the regulatory environment than there would be if I were building a car. To build a car, I have to put in a seat belt. If I'm building the equivalent in cyberspace, I'm effectively putting in an ejection seat.

Let me give you three statistics that indicate just what kind of magnitude we are facing in terms of ill-preparedness in dealing with fundamental issues of security on the Internet to begin with. These are three 90% statistics that you can keep in mind. The statistics are a bit dated, at about 12 months old, but still useful.

First, 90% of malware, code that is meant to do malicious harm on the Internet, uses a single channel to communicate, known as the DNS, and yet more than two-thirds of the Fortune 100 have no perspective on this channel in their security posture. Ask yourself, if 90% of the threat can be seen through one channel, why is it that only one third of the most valuable companies in North America have perspective on that channel?

Second, 90% of all industries are planning to implement the Internet of things as part of their infrastructure, and yet more than 80% of them have absolutely no confidence that the security measures they have in place will give them a perspective on the security coming out of the Internet of things. The reason for this is that our ability to understand what is considered to be bad traffic, malfeasant traffic, on the Internet of things has simply not been developed. It does not yet exist. This is an industry gap problem where the technology is moving faster than the regulation that exists.

● (0915)

The third 90%, which is the most important one, is that 90% of all cybersecurity breaches use the human vector. In other words, they are not dependent on a fault in the technology, but they use human behaviour and human weakness as a way to get in. If you ask any engineer, you cannot engineer a security solution against a human problem. This is a regulatory problem where we have not developed the rules commensurate with the importance of the infrastructure that we currently have and on which our economy depends.

Also, there has been a dangerous entanglement between cyber-capabilities and their social impacts. Quite frankly, in the last five or six years, two-thirds of humanity has gone online to the Internet, globally. Of those, almost all of them are also users of social media. In fact, for many countries, such as Burma/Myanmar, Bangladesh, and others, the first contact that individuals have had with the Internet has been through Facebook. Moreover, more than 50% of this online population is under the age of 25. These are first-time voters.

Last year, we were asked to do a study for the UN in Bangladesh looking at terrorist use of the Internet, and what we found was quite predictable. There are terrorist communities that use the Internet, that speak violent, terrible things, that spread propaganda, but ultimately these groups are quite small.

What we did find, however, on a much larger scale, is that mainstream political parties are now using the Internet and social media as a focus group. They're effectively putting out messages and seeing whether these accrete some form of popular support. What that has meant is that there has been a gradual mainstreaming of extremism across the political spectrum. If that sounds familiar, it should, because the very same kinds of patterns have impacted Canadian politics and also the politics of countries such as our neighbours south of the border.

Why this is important is that, if we focus on the impact of the Internet simply from the point of view of the meddling of international states, we miss a very, very important aspect of how the Internet is changing politics within our own countries, absent any kind of foreign interference.

I'll just leave you with a couple facts.

From testimony given to the U.S. Senate intelligence committee, we know that combined campaigns of Hilary Clinton and Donald Trump spent $81 million on Facebook advertising during their campaigns. That is money that was spent on Facebook ads, absent political action committees. The same testimony indicated that the Russian Internet research bureau, out of St. Petersburg, spent approximately $46,000 on Facebook ads. Even if we inflate that figure up to $1.5 million, say, we're talking about a very, very different percentage of money. Unless we're prepared to attribute the fact that the Russians are much cleverer about political messaging than U.S.-based political operatives are, who are trying to get their constituents elected, we have to be very careful in the way we look at foreign interferences or meddling being a decisive factor in international relations. That's not to say this didn't happen.

How does all of this relate to NATO's position vis-à-vis cyber? First of all, it's important to recognize that the vulnerabilities I have just described are vulnerabilities that we all share, and have have very little to do with an external threat but a lot more to do with a threat that was ascribed in a Pogo cartoon in 1936, which simply stated, “We have met the enemy, and he is us.” Unless and until we're able to shore up our own domestic regulatory environment, being able to deal with the potential impact of a volatile external actor becomes more and more difficult.

Moreover, the problems of defending cyberspace, which I described in the three 90 per cents, essentially hit every single NATO country. The additional challenge we have is that NATO's interoperability and the development of appropriate doctrines on the military side to address how we deal with these vulnerabilities are simply underdeveloped, and yet they're occurring at a moment when we have a period of grand confrontation with a particular peer actor.

It's important to recognize that Russia is only among what IISS has identified as 140 countries currently developing cyber capabilities. This means that the spectrum of threat is much, much larger than a single country in itself. Moreover, it's also important to recognize that, since 1997, the Russian Federation has been one of few states that have used the UN mechanism to try to define a pathway for addressing stability in cyberspace through a treaty-based approach that addresses issues both above LOAC—law of armed conflict—and below LOAC.

● (0920)

Why is this important to deal with right now? Although I don't have recommendations for the committee on what we should do, there are certainly clear things that we should not be doing. These include, for one, not degrading the operation of confidence-building measures that give us an opportunity to discuss the impact of a cyber on interstate relations between NATO and among NATO countries writ large, and, two, not cutting off channels for engagement to be able to discuss these issues and find common ground.

This is important for a number of reasons, but perhaps one of them is most important for us to consider. The Russian Federation, which is the object of most of our concerns in the cyber domain, has very clearly linked the escalatory ladder between cyber and nuclear. For them, this is an area where they see the threat to national security spanning two critical domains.

We spent many years prior to and after 1989 creating confidence-building measures in the nuclear security chain. Nunn-Lugar is one manifestation of legislation in the U.S. They put in place multiple points of discussion, multiple breakwaters, if you like, for us to be able to deal with this issue. Those are now being rolled back, and they're not being replaced by anything.

Moreover, we have not had an active channel to discuss cyber issues with the Russians for a number of years, either bilaterally, or, more importantly, within a multilateral session. If there is one thing we should not be doing, it is engaging in an escalatory ladder without thinking through our end game. What is it that we are trying to achieve? What constitutes deterrence in cyberspace, and is there such a thing if we've been unable to define, from a strategic point of view, what cyber means for us?

The most important thing is that absent a policy, we should not be entering into a game of chicken with a nuclear power without a strategy and a map for what we want, as a country and as an alliance.

Thank you.

The Chair: Thank you very much for that. It was fascinating, and I hope there are some good questions to pull out more of that information.

I'm going to give the floor, for seven minutes, to MP Robillard.

The floor is yours.

[*Translation*]

Mr. Yves Robillard (Marc-Aurèle-Fortin, Lib.): Thank you, Mr. Chair.

My question is for Mr. Rohozinski.

In your article entitled “The Internet has made nuclear war unthinkable—again”, you explain that the nuclear world and the digital world are increasingly interrelated. Could you please elaborate on the links between cyberspace and nuclear weapons?

[*English*]

Mr. Rafal Rohozinski: The question pertains to this entanglement between the nuclear and cyber domains, as it pertains to the development of new classes of both nuclear weapons, as well as the actors that are involved. This isn't a physics lesson, but one of the characteristics of nuclear weapons, particularly thermonuclear ones, is their ability to generate an electromagnetic pulse.

Electromagnetic pulse weapons are weapons that have been optimized for that, and have the characteristic of being able to affect any electrical system that is not adequately protected. What that means for countries and economies that are now increasingly dependent upon the digital economy and digital technologies is that deterrence is not just defined by the ability to deter an actor who can create mass damage in the physical domain. We can threaten hundreds of cities with nuclear weapons, but a single nuclear weapon generating an electromagnetic pulse can create mass effects that would bring chaos across a wide range of infrastructure.

That means that the threshold for countries to effectively join an elite club and be able to hold the world's digital economy to ransom has become much, much less. North Korea doesn't have to pursue the creation of thousands of nuclear weapons in order to threaten the world. It needs a few nuclear weapons that are able to create this kind of effect.

Second, and perhaps more importantly from the perspective of NATO-Russia relations, both the Russian Federation and the United States are now modernizing their nuclear capabilities. That includes replacing decades-old command and control systems that previously operated in a much more robust analogue way. There are concerns that this modernization means that we are going to be implementing technologies that are, first of all, much more susceptible to effects that can be generated through nuclear weapons designed to effect an electromagnetic pulse, and, secondly, that one of the ways of effecting deterrence may no longer be simply nuclear, but may be cyber itself. In other words, a cyber-attack against the command and control infrastructure may be a better way of being able to deal with it than necessarily doing a one-for-one missile cap.

This entanglement is something that is now starting to come to the fore. It certainly came to the fore in the case of North Korea, but I would also caution that with the modernization of nuclear arsenals on both sides, this entanglement will only grow.

● (0925)

[*Translation*]

Mr. Yves Robillard: Thank you.

The next question if for Mr. Shea.

As deputy assistant secretary general of NATO's emerging security challenges division, please tell us what kinds of threats NATO countries are facing from hybrid warfare, and cyber warfare in particular.

Could you also tell us also how prepared NATO is to deal with the threat of hybrid warfare?

Dr. Jamie Shea: Thank you very much for that question.

The threat of hybrid warfare, as I said, is that it erases the traditional distinction between war and peace, and leads us into a world where everything is constantly contested, where domestic security is becoming as strategically important as the traditional defence of our borders. I am referring to the security of populations and critical infrastructures, the ability of our societies to function well, and the ability of people to lead their lives normally without being subject to threats.

In hybrid warfare, the focal point of defence shifts in a sense from our territory or borders to our populations. It even affect what is on the minds of our citizens. How do they perceive reality? What messages seem most credible to them? What confidence do they have in their leaders' abilities? In the past, NATO's role was fairly simple: it was simply to physically defend our borders. It now has a dual role. It must first defend our borders, which is still important, in particular with the growth of Russian forces in Eastern Europe. That is why you currently have nearly 500 Canadian soldiers deployed in Latvia. At the same time, we must become increasingly competent in analyzing threats to the smooth functioning of our societies.

What do we have to do? We are currently pursuing six avenues.

The first thing is intelligence. How can we better anticipate and detect this kind of hybrid threat and make a distinction between a spontaneous attack and a deliberately orchestrated attack? How can we more quickly and more accurately identify and define threats in order to respond? If we spend months talking just to conclude that something that walks like a duck and talks like a duck is in fact a duck, we will be overtaken by the speed of events. So the first thing is to improve our anticipatory intelligence capabilities.

The second is crisis management. Can we make decisions quickly, in real time? Intelligence is very important, but do we have a series of special intervention measures planned in the event of crisis? How can we expand the tool box of measures we can take? As I said, there are diplomatic measures. For example, you learned this week of the expulsion of more than 100 Russian diplomats by various countries to protest the use of chemical weapons in Salisbury, England. So economic measures are needed, as well as a whole series of other measures that allow for a flexible response. At NATO, if we stick to the wording of article 5 of the treaty, we do of course have to wait for an actual war to be declared before we respond. So we need to increase the flexibility of our response options.

Third is strategic communication. Can we more effectively identify fake news and information operations and respond to them?

Next is the resilience of our infrastructures. How can we make our nuclear plants, electrical systems, and communications systems more resistant? That is also very important.

Finally, how can we be more effective in cyberspace and how can we learn from our partners? Take a country like Ukraine, which is an important partner to NATO. A lot hybrid tactics are used against that country. We have to help Ukraine, but at the same time learn from its experiences in order to prevent the same thing from happening to us.

● (0930)

[*English*]

The Chair: Thank you very much.

MP Bezan.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Mr. Chair, I want to thank our witnesses for appearing today and for sharing their knowledge and experience on this important issue and how it's affecting NATO and, in particular, how us here in Canada.

I know we're all captivated by the cyber content, cyber warfare, and hybrid warfare that seems to be evolving, especially since Russia's invasion of Ukraine. We're seeing technological advances, both in NATO countries and Russia, China, and others, in traditional weaponry like tanks, jets, ships, and nukes. Things are modernizing, and everybody seems to be moving in lockstep.

From some of the reading I've done, I'm a little concerned that our near peer adversaries may actually have the upper hand because of their technological advancements, such as in the world of cyber, cruise missiles, hypersonic missiles, electromagnetic pulse weaponry, and direct energy weapons.

Can we dive down more into where NATO nations are versus where we see the Russians, the Chinese, the Iranians, and even North Korean in terms of how they're advancing with their weapons and how that's keeping us off balance?

I'll go first to Mr. Rohozinski, and then to our guest by video conference.

Mr. Rafal Rohozinski: It's a broad question, but I'll give you a small slice of it, which I think pertains specifically to the cyber-environment itself.

One of the interesting paradoxes is that some of the more successful employments of code-based attacks—if you want to call them that—against critical infrastructure over the last three years have effectively been the repackaging of NSA attack code that was stolen during the Shadow Brokers incident. For example, there was the takedown of the systems at Maersk's major maritime operations. It was repackaged code that was effectively employed.

I think one of the things we've seen from a perspective of looking at how Russia and other countries employ information operations is this. Let's focus on how Russia has done so. One of the things we've seen is that their ability to develop techniques, tradecraft, and process around employment of a cyber-operation has been quite significant. In other words, there's been an intentionality in what they've tried to do.

From a technical point of view, their sophistication really hasn't been anything different—larger or smaller—than what we've had. I think there's a reason why the Russians have done this. I think it's partially due to the fact that they feel there's a certain existential threat that has occurred as a result of NATO's growing resolve around Russia's claims along its borders. I think it's a hardening of Russian positions in general. Does it necessarily reflect a capability that is more sophisticated than what we have from a technological point of view? My answer would be no.

Mr. James Bezan: The technical and tactical advantage that NATO nations have had over Russia, China and others, has narrowed, has it not?

Mr. Rafal Rohozinski: No, I don't think so. On the technical level, I'd say that the United States especially still is the paramount cyber-power in the world. I think that's quite undisputed.

In terms of the level of scope or openness to be able to experiment in the operational domain, I think the Russians have been much more promiscuous, so to speak. As a result, their ability to generate effects has been more evident, perhaps, than ours. That's not to say that NATO member countries haven't individually been able to mount very successful cyber-operations, both publicly known and less publicly known, but they've been different in political intent from those that have been run by the Russian Federation, hence why I think we spend a lot more attention focused on that.

Mr. James Bezan: Mr. Shea.

Dr. Jamie Shea: First of all, yes, of course there is a diffusion of technology for a number of reasons. The first reason is that 30 years ago most of the advances came from the military industrial complex, as President Eisenhower would have called it. You remember the invention of the Internet, or Teflon from the space program.

Today, much of military know-how is coming from the civilian sector. Cyber is an example of that, as are artificial intelligence and social media. Also, of course, civilian technology is far more widespread around the world. More and more countries invest in it, naturally, for their economies. In terms of the military technology, I think we just have to recognize that fact.

The second fact is that many countries around the world have spent a lot of money on developing their own domestic R and D and military capabilities. Brazil now produces submarines and first-class aircraft. I saw a couple of days ago that even Saudi Arabia is intending now to start up its own autonomous defence industry. There are more and more countries below the level of the great powers, if you like, who are now selling advanced military equipment and know-how to each other. Brazil sells to South Korea. South Korea sells to Israel. There is going to be a diffusion in the world.

The other thing, of course, is that countries such as China—let's be frank—are investing in certain areas far more than we are. For example, in artificial intelligence, it's investing about four times what the United States is investing at the moment. China now has the world's biggest and fastest supercomputer, and to date China graduates about eight times more engineering Ph.D.'s from its universities than the United States.

That's not to say that they're all 10 feet tall, of course not: they have their weaknesses as well. That is something that we learned from the Cold War, where we systematically overestimated the Soviet Union for many years. But it does mean that we need to take our own science and technology much more seriously.

You've seen R and D levels decline in many NATO countries. You've even seen people openly criticizing the value of science, scientific evidence, and scientific knowledge. There's the idea that came out in the U.K. Brexit campaign, which was that we don't want to hear from experts any longer—we're tired of that. I think we also need to pay more attention to our own science and technology base.

In NATO, of course, we also need to look more intensively at the impact that artificial intelligence, bioengineering, and new drones and so on are having on our defence posture, and not just to raise our awareness—the ambassadors, for example, had an away day on artificial intelligence last week—but also to look at how these are going to affect the future.

By the way, if I may continue for just one second, don't forget also that the new technologies not only influence the conventional battlefield, such as artificial intelligence, but it may also mean more hybrid warfare as well. They play both in the external aspect, which I was talking about, and in an internal aspect. You can do a lot of things with it that you can't do with a tank, and that's why we need to look at these very seriously.

My own sense is that the free societies, provided they pay attention to this, will generally have the superior technology in the long run.

● (0935)

The Chair: MP Garrison, you're next.

Mr. Randall Garrison (Esquimalt—Saanich—Sooke, NDP): Thank you very much, Mr. Chair.

Thank you to all the witnesses for appearing here today.

I want to start my questions with Madeleine Moon, whom I had the pleasure of meeting at a NATO Parliamentary Assembly in Washington a couple of years ago. We took advantage of the opportunity of long bus rides between venues to exchange views at that time.

I am going to ask you questions in the context of your being a member of the NATO Parliamentary Assembly's defence committee. First is my concern about the lowered threshold for use of nuclear weapons. We've certainly seen that in sabre rattling in North Korea. We've seen it in the deployment of tactical nuclear weapons. I'm wondering whether you have seen a renewed commitment or emphasis on NATO's commitment to create the conditions for a world free of nuclear weapons, either in the Parliamentary Assembly or in NATO's work itself.

Ms. Madeleine Moon: If you're looking for a world free of nuclear weapons, the U.K. is a good place to start. We have been working toward it, along with other allies within NATO, for some considerable time. However, it takes more than two to tango. You need people to agree that it's a good idea.

Part of the problem we have is that some countries, like North Korea, are emerging and developing their skills. We have tried to contain others, such as Iran, that have been working on developing their skills. We're very unsure about where Russia is going with its talk of creating new capability.

There is an increased tension about whether or not we are moving toward a different nuclear risk in the world today. We also have indications from Russia that commitment to non-use of first strike is not as strong as it used to be. As such, I think we have to be aware that we have to protect ourselves and that nuclear weapons are part of our arsenal. We're very clear that NATO is a defensive alliance and that there will be no first strike. But we also have to look at emerging economies and emerging threats where nuclear capability is being developed and try our best to make sure that this technology is limited and does not spread into areas where tension and conflict would be more likely to create a problem with the actual use of such weapons without agreements about non-use of first strike.

● (0940)

Mr. Randall Garrison: Of course, the U.S. Nuclear Posture Review was just published. It appears to repudiate the first strike. I've asked others how that relates to NATO's policy on deterrence, which would seem to exclude the first use of nuclear weapons. I'm not sure how it works when one of the key NATO allies seems to have abandoned that position.

Ms. Madeleine Moon: NATO's position remains NATO's position. As many of the American senators have said to you and to me, President Trump says what President Trump says, but the louder voice is what the alliance says.

Mr. Randall Garrison: Thank you.

I know I have limited time.

I want to turn to women, peace and security, and the work I know you have been doing in the Parliamentary Assembly and its defence committee. Of course, I think we were all pleased to see a NATO representative for women, peace and security.

My concern, which I know others share, is that once a representative is appointed, others believe it's her job to advance these goals, and they sometimes forget that it's part of everyone's mandate to do that. I wonder if you have any reflections on the impact of the creation of this position.

Ms. Madeleine Moon: You always need champions in any field. You need somebody who is going to drive the agenda.

Importantly, women, peace and security has almost morphed into gender, peace and security. There is a recognition now that gender is an issue not only in military activity and war but also within our politics, and how our politics are driven, as well as in who is in our military and who is going to be serving us and representing the values of our nations. It's happening on lots of different levels.

I hope that having someone who is going to focus on that agenda will mean that agenda will drive faster. You have to remember that in any alliance you are only able to go as fast as your slowest member. In some countries the issue of equality is not as advanced as it is in others. How we see women in the world, the military, and politics, and how we protect civilians—because the majority of civilians in any war zone are women, children, and the elderly—are critical questions we have to address.

Mr. Randall Garrison: Last night we elected the executive of our Canadian NATO Parliamentary Association. We re-elected one of the members of our committee, Leona Alleslev; another member of our committee, Cheryl Gallant; and one my colleagues, Rachel Blaney, as members of our executive.

I'm wondering whether you've seen change over time, because many argue that until you get to about 30% of women participating in organizations, it doesn't really change the culture. Have you seen a change in the NATO Parliamentary Assembly, in the number of women participating, and in particular on the defence committee?

Ms. Madeleine Moon: That's an interesting question. Here in the U.K. we are really struggling with the new phenomenon for women in politics, when, particularly in social media, the threats against women politicians are growing. It is now seen as perfectly acceptable to leave a social message suggesting that a woman politician will be raped or murdered. There are really quite nasty threats made against them.

What is interesting in the Parliamentary Assembly, and it's one of the reasons that it's such a pleasure to serve there, is that the discussion and conversation is at a different level. In fact, there's an urgent desire to hear from women politicians and to hear a different perspective. I think that's important because women do bring a different perspective, a different understanding, but they also bring an opportunity for the countries they represent to hear how that country is seeing their women. I think that's one of the great values. The opportunity to hear how women are projected in the society of each of the alliance members is as critical as the work we're doing to protect women in war zones.

● (0945)

Mr. Randall Garrison: Thank you very much.

The Chair: Thank you.

We have MP Gerretsen.

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

Ms. Moon, I wanted to ask you a couple of questions about NATO, and the general understanding of NATO among the U.K. population.

I see from reading up a bit on your history that you were a mayor, and councillor before that as well, and I think you have a unique connection at that grassroots level. You get to hear what a lot of people are talking about. I'm wondering if you can provide some insight into, first of all, what the general perception is of NATO amongst the population in the U.K. Do people know what NATO is, what it effectively does, how it plays a role in the defence of the U.K.? Is that generally understood? We seem to be struggling with that problem in Canada and we don't know if it's an educational thing or a geographic thing. I'm curious to get some of your insight on that.

Ms. Madeleine Moon: Actually, we have just set up a working group looking at how we go back out across the alliance and explain the nature of NATO and the alliance, what it is, what it does, and what the alliance actually stands for. I'm also an ex-schoolteacher, so I am very passionate about going into schools and talking to schoolchildren about politics, and why they should engage in politics. On a regular basis, I also have a series of talks I give about NATO. It is really quite scary how many of our under-25s have no concept even of what our air force does, what our navy does, never mind what the NATO alliance does.

Mr. Mark Gerretsen: Exactly.

Ms. Madeleine Moon: That is extremely worrying.

Mr. Mark Gerretsen: Is there any kind of educational program under way or being talked about in the U.K. to help promote that? I'm sure you can imagine how much more our population is disconnected from understanding NATO, given that we're so far away from the actual operations that NATO is regularly engaged in. I would be surprised if 5% of the population even knew what NATO was in Canada if you were to randomly start walking down the street talking to people about this. I'm curious if you've done any programs that we can model ourselves after.

Ms. Madeleine Moon: No, we don't have any programs, nor do we have anything in our educational system where children, as part of their studies, examine NATO and see where it came from. That is why I wanted to start with that. Knowing where you came from is very important to see where you're going and why you're doing what you do. It is a major problem and we are addressing it within the Parliamentary Assembly.

Mr. Mark Gerretsen: Can you explain how you're addressing it?

Ms. Madeleine Moon: We're looking at the issues that we need to focus on, going back into our educational systems. As individual members, we go into our constituencies and our wards and talk about defence and security, and I have to tell you, there's nobody in Bridgend who doesn't know I do defence. There's nobody in Bridgend who doesn't know that they're going to hear from me on a regular basis about what threats the country is facing, what the risks are, and why we're doing what we're doing.

I recently had the army presentation team in my constituency. I have the RAF presentation team coming in soon. I am passionate about going out there and talking about defence and security. There's a huge risk that many of our voices are being drowned out by those who would like to see defence and security as something that is done, dusted, and gone away, and since Britain is so isolated and still a little island off of the coast of Europe, we're perfectly secure.

Canada can think that it's perfectly secure it's on the other side of the Atlantic. You wake up when citizens in your country are attacked by chemical weapons. We have to recognize that risks can be anything at anytime.

● (0950)

Mr. Mark Gerretsen: I just have one follow up question on the discussion that you were having with MP Garrison about the state of nuclear weapons and the different actors in the world.

Do you think it is realistic to assume that we can live in a world that is free of all nuclear weapons?

Ms. Madeleine Moon: You always need something you aspire to, and it has to be greater than yourself and be greater than mankind, so yes, I think it's something we have to aspire to and want. As for wether we achieve it, I think humankind isn't quite there yet.

Mr. Mark Gerretsen: Okay. Thank you for that.

Mr. Rohozinski, I'm going back to your opening remarks and your comments about social media, the changes in our world, and how these relate to nuclear weapons. It got me thinking about the Cuban missile crisis and how that might have been handled so much differently in the world we live in today.

I'm curious what threats you see from social media and the fact that we live in a world where information is so freely available to flow around. What kind of impact does that have on the security and use of nuclear weapons?

Mr. Rafal Rohozinski: I think there are two separate questions there, but I can address them. I think that part of it is answering the question you had asked Ms. Moon about whether we can live in a world absent of nuclear weapons and how that links to NATO.

I think, in particular, the U.S. declaration of the development of a new generation of nuclear weapons that are dial adjustable—in other words, are more usable, in that yields can be adjusted—sends a very poor message to the rest of the world, in the sense that these weapons can now be used in a contained manner.

Similarly, my earlier statement about the fact that weapons can be designed to maximize the electromagnetic pulse means that small powers that may aspire to create a very limited nuclear capability suddenly have an incentive to do so because it would allow them to hold much larger countries at risk. The issue is not mass destruction of society, but the mass effects that can be generated through the use of these weapons.

Moreover, if you link the two things, the ability to use sub-yield nuclear weapons to take out limited nuclear capabilities means that the whole thought and architecture of nuclear exchange has become something other than this escalation ladder that we had with MAD. How does this relate to social media? I think part of the problem is that we're now living through a “Jerry Springerization” of politics, with the highly dangerous ability to seize the moment and to be able to drive political agendas around through Twitter.

Politics by Twitter means that you don't have the mechanisms to be able to engage and deal with escalation ladders in a reasonable manner. This comes back to my opening statement. We can confront peer countries that we feel we have a difference with, over things like territorial integrity or international adventurism. However, as we are doing this, we need to have mechanisms to be able to engage in confidence-building measures in areas where we have shared security interests, like the digital economy, existential matters, etc.—these things that we need. Make sure that first, we have a game plan when we escalate and, second, always talk even when you're fighting.

Thank you.

Mr. Mark Gerretsen: Don't make eye contact with them; then they can't cut you off.

The Chair: Well, I can. I'm just trying to do it gracefully.

We're going to move to five-minute questions now.

MP Alleslev, you have the floor.

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

The level of conversation today is simply outstanding, and I can't thank you enough for being here.

I'd like to move to areas of focus, particularly to Mr. Shea and Mr. Rohozinski. You gave us a distinct perspective on what not to do and some of the things that NATO is prioritizing within NATO. Of course, we're looking to give advice to government. It's a highly complex area. There are so many moving pieces. What should our top three areas of focus be in this domain? How do we make sure we're working smarter, not harder?

Mr. Rohozinski, perhaps.

● (0955)

Mr. Rafal Rohozinski: Rapidly, I think that on the NATO level, one of the things that has made NATO an exceptionally effective alliance in its past is the focus on interoperability and inter-operation.

In terms of the cyber domain, although there's been a declaration of cyber as an operational domain, I think that has been very much lagging.

In terms of defence of NATO systems, which I think Mr. Shea knows an awful lot about, there are definitely capability gaps there where I think leadership at a national level has to happen.

However, NATO is more than a military alliance; it's also a political alliance. I think, on that level, Canada's taking leadership in recognizing the fact that NATO needs a political strategy around cyber as a destabilizing environment is also really important.

Cutting off points of engagement and closing down mechanisms is not the way to go. I think Canada needs to show leadership on the fact that we can talk even when we have differences, recognizing the fact that the absence of a predictable escalation ladder in this particular area is something that creates volatility and danger for us all.

I'll let Mr. Shea answer the other two.

Ms. Leona Alleslev: That ties in with what you were saying.

Go ahead.

Dr. Jamie Shea: I don't disagree at all with what Mr. Rohozinski just said.

My top three, very briefly—because I know we have to be brief—are these.

We need to invest at a national level. NATO is only as good as the sum total of the capabilities its members provide. Apart from some AWACS aircraft—and Canada now is rejoining that program, which we're very pleased about—NATO depends exactly on its ability to generate national capabilities.

I'm very pleased, of course, that Canada is increasing its defence budget significantly. I mentioned the $750 million Canadian over the next few years going into upgrading cyber-defence, for a proposed Canadian centre for cyber security and a national cybercrime coordination unit. These are good examples. Of course, we need resilience to be built at that national level.

NATO could help the defence planning process. It could help to guide nations to where their investments would probably be the most cost-effective. We can learn from each other. We can give countries realistic targets, of course, but we very much need the 2% mark of GDP to be reached over the next few years progressively, because of all the challenges we face, whether from the east, the south, or this homeland front that we've been talking about today. Those are three strategic fronts where NATO needs to deliver, and we need that 2% to be able generate the suite of capabilities we're going to need.

The second thing is NATO-EU. Although Canada is not a member of the European Union, 22 NATO countries are. When it comes particularly to this hybrid thing, the co-operation between the two institutions is key. The EU has things—the R and D money, the new European defence fund of 5.5 billion euros that's being set up to promote more research and development, and the way in which the EU works to regulate the environment. Think of the general directive on data protection that is now coming in, and the efforts to protect critical infrastructure. The EU has many of the assets, frankly, that we lack, but NATO has things, of course, particularly in the military field, that the EU lacks. Getting these two organizations not just to talk about working together and not just to organize seminars in Brussels, but also to really pool their efforts is going to be key.

Finally, exercising is important. These challenges today, as I say, present us with some difficult issues. How do you do attribution? When do you do attribution? How do you classify a hybrid attack? How do you respond? Frankly, like everything else in life, we need to rehearse, rehearse, rehearse, not just military exercises—we have lots of those—but also political exercises on crisis consultation and try to work out which measure suits which situation best. The more we train, as with anything else in life, the more we'll be able to identify and deal with the real thing if it ever happens to us.

Ms. Leona Alleslev: Thank you very much.

The Chair: Go ahead, MP Gallant.

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): Thank you, Mr. Chairman.

Mr. Rohozinski, it took parliamentarians, people like you with experience who go to think tanks, as well as academia and those in the commercial sector to convince NATO that cyber had to be another domain. Given that it took a decade to get that through, what should we be looking at as the next operational domain?

● (1000)

Mr. Rafal Rohozinski: I think, to be honest, cyber is much wider than the way we've defined it right now. The emergence of autonomous, AI-based systems leads us into areas that I think start becoming really, really crucial to understand, simply because of the fact that the decision cycles over how these systems are going to operate will impact on us.

The fact that we've started to erode the kind of silos between chemical biological warfare, nuclear warfare, conventional warfare, and hybrid warfare means that on the policy end, much more so than on the domain definition end, we have a lot of work to do.

We talked previously about military civil policy. I think that's something we somehow forgot in terms of how it relates on interstate relations over the last decade and a half, having sort of lived in the aftermath of the end of the Cold War and saying, “Well, we solved that problem with the chemical weapons treaty. We solved that problem with START and nuclear treaties.”

I think there is a lot of work to be done, not so much in terms of defining domains that may be disruptive, but simply allowing our own rule set or our own institutions—from the UN down to domestic policy, which really needs to be addressed. The impact on cyber, on chemical, and on nuclear is now starting to become entwined, and that's the challenge for us.

Mrs. Cheryl Gallant: Mr. Shea, do you have anything to add?

Dr. Jamie Shea: If you'll give me the opportunity very briefly, I agree that one of the key things is to re-establish red lines. I honestly believe, in my personal view, that the reason chemical weapons were used in the U.K. is that we didn't do more to stop their use in Syria. We didn't follow our own red lines and therefore we've allowed the Chemical Weapons Convention to fritter away.

You've spoken a lot about nuclear, and we cannot allow nuclear norms to fritter away. If we don't respond energetically to cyber-attacks, particularly for really destructive things like WannaCry and NotPetya, we then communicate a message that this is now acceptable, that it's high gain and low risk, if you like. We need to turn it around and once again make these violations of international norms, not just in a genocide area but the use of these new weapons, high risk in terms of the response—it's going to be counter-productive, you're going to lose more than you gain, and low gain. That's going to take time, but I think that's key.

I think the second area—and I agree with Mr. Rohozinski here—is that when new things come along, like artificial intelligence or autonomous weapons systems, we need to be all over them early, and much more quickly. That means asking if there are advanced uses in these issues that we could develop to make our defence better. For example, quantum computing can provide a lot of the solutions to cyber defence, so it could be a good thing.

We know from experience that these new technologies have their good side, like the Internet, and their dark side, and we need to be quicker at how we try to stop the dark side.

Mr. Rohozinski, I think, is totally right to point out that, with autonomous weapons systems that could be used totally outside of the human decision-making loop, we need to now start thinking what kind of arms control norms and what kind of standards we need and how to get people on board, so that we establish a red line against the illegitimate use of these things.

Finally, I don't believe there is going to be a new domain as such, but I think one thing we need to think about is how the existing domains and people who work in those domains can help with cyber defence, and how the cyber people can help to reinforce our ability in the existing domains.

Mr. Rohozinski, I think, quite rightly pointed to the problem of more and more weapon systems now running on Windows 2.0, and the vulnerabilities that could come from that.

Those are the three points I'd like to make in response to an extremely interesting question.

Mrs. Cheryl Gallant: Okay.

With respect to cryptocurrencies, I know that governments are focusing on how to tax them, but from our perspective we see them as potential threats. It could be the way terrorists or other belligerents are moving money and funding, and you always follow the finances when tracking down people like that.

Now, we're seeing some movement in the United States with securities regulation, but from a national security standpoint, and more globally from a NATO standpoint, what should we be doing as parliamentarians, as legislators, to get this follow-the-dollar ability under control?

Dr. Jamie Shea: Well, I—

The Chair: I'm sorry, I'm going to have to cut it off there because we're just over time, and that answer is going to take us further over time.

I'm going to have to yield the floor to MP Sheehan.

Mr. Terry Sheehan (Sault Ste. Marie, Lib.): Thank you very much, Mr. Chair.

I appreciate the opportunity to ask a few questions here. This is a very important subject, and I'd like to commend the committee for undertaking such a great study. I've been here a couple of times, and it's very important.

To our witnesses, that was great testimony. I appreciate it very much.

I'm going to ask a first question. I've been talking about NATO a lot, and perhaps our witnesses from London—a third party, another country—could comment. How is the Canadian-American relation in NATO? Would you suggest that it's good, bad?

● (1005)

Ms. Madeleine Moon: That's a difficult question for me to answer. We view Canadians very differently from Americans. We see Canadians as more British, if you can say that.

Some hon. members: Oh, oh!

Ms. Madeleine Moon: I think the Commonwealth joins us much more closely. We have a stronger common background. We're close to the Americans militarily, but amongst our general population, the ease of relationship is not there. Especially when we see what is happening with the Twitter communications coming out of America now, it's creating a distance.

Having said that, the English language is always a unifier, a bond, and our past history, particularly the support that we've given to each other during the First and Second World Wars, remains a critical point of importance for us.

In terms of the future threats, can I stress the importance of greater honesty and transparency with our own populations? I say this because there is a growing cynicism that is being fed by others on social media. We need to have a resilience amongst our population that isn't there at the moment. We need to give them the decency and the integrity they deserve, and help them to understand what the threats are and the values we're defending. We need to do more of that before we go on to look at the next capability threat. The biggest capability threat that we face is undermining the values of democracy by not being as honest and straight with our population about what the threats are out there and what we're trying to do to tackle them.

Mr. Terry Sheehan: Understood.

Dr. Jamie Shea: First of all, my sense is that Canada is now showing again that it provides muscle to NATO, by rejoining the AWACS program and taking the lead in having Canadian troops back in Europe now—although after the Cold War we didn't know this would be needed again. You've answered the call by taking the lead of the multinational battalion—and the most complicated as well—in Latvia. This shows that Canada is sharing the burden, increasing its defence budget. That means you speak with a loud voice in NATO today. You've shown that it's not just words, but actions, like your commitment to Afghanistan, or the Balkans in the past. That's key.

Secondly, Canada stands for norms. I mentioned in my remarks the criticality of not just producing more weapons, but also producing norms and good ideas. Canada has always been in the forefront of propounding norms, since the days I used to work with people like Michael Ignatieff and Lloyd Axworthy. There's a lot of work to be done.

I totally agree with everything that's been said about women, peace and security; the great role of Ambassador Hutchison; and Security Council Resolution 1325. However, I would hope that Canada would go beyond that and also propound in NATO other types of norms that we should be developing, particularly in the arms control and cyber domains. You have a leadership role in the G7, which could be an appropriate venue as well.

Finally, from the point of view of my own country, you have signed a trade agreement with the European Union. Unfortunately, we don't yet have the trade agreement with the United States that we hoped for. You've shown that a major North American country can sign one. In my country, when we talk about Brexit, we always talk about Canada plus, or Canada plus plus.

I agree with Madeleine: lead the way on multilateralism, the liberal rules-based international order. You have a great deal of authority on that, and that's a message everybody needs to hear.

Mr. Terry Sheehan: Thank you.

The Chair: MP Yurdiga.

Mr. David Yurdiga (Fort McMurray—Cold Lake, CPC): Thank you, Mr. Chair. I'd like to welcome our guests here today. Their testimony is very important. I learned a lot of things today, so thank you very much for that.

We are all very concerned about cybersecurity, hybrid warfare, and the nuclear capabilities of some rogue nations. That's very concerning.

My first question will focus on NATO security, classified information and general information. Do all NATO members have the same access to all intelligence information? If not, who determines what level of access each individual member receives?

Mr. Rohozinski.

● (1010)

Mr. Rafal Rohozinski: I would suggest that the question's probably better addressed to Mr. Shea since he represents NATO.

Mr. David Yurdiga: Mr. Shea.

Dr. Jamie Shea: Okay. First of all, no.

There are lots of bilateral intelligence sharing arrangements. You know of the Five Eyes, of course, because Canada's part of that, and it has played, traditionally, a large role. We have in NATO today, with this joint intelligence and security division that has been in existence for just over a year, a concerted effort now to increase intelligence sharing in NATO by forming many panels. We're thereby linking, for the first time, civilian intelligence with military intelligence and therefore encouraging allies to share more. We now have a system called BICES—another terrible NATO acronym for you—which is a distinct agency that allows all allies and partners in the European Union to file the intelligence reports they're willing to share with allies. They can choose the level of classification, and they can choose whom they want these to go to. That's a voluntary effort, but by being voluntary it encourages more intelligence sharing than if we had tried to have a one-size-fits-all approach.

The situation is progressively developing, but it's always, always, always going to be a basic privilege and a right of any country that originates intelligence to determine with whom and what it wants to share. NATO could be a hub to facilitate this, but we can't change that fundamental national right.

Mr. David Yurdiga: Thank you.

Mr. Rafal Rohozinski: The additional comment I would make is that intelligence sharing is based upon knowing what intelligence is actually meaningful to the domain. I think that one challenge we have in cyber is actually knowing what is meaningful and actionable intelligence that you can work on.

Indicators of compromise, which are now being shared among NATO countries, both at the commercial level and the classified level, are one thing, but how do you share information on, for example, traffic emerging on social media that may have a direct impact as part of a hybrid impact against a NATO member country? Is there a justification for surveillance of social media traffic as a joint national defence or joint defence strategy? These are policy questions where we have quite huge gaps.

In fact, maybe as a closing answer or statement on this, I think you have an issue here as parliamentarians. Cyberspace is having an impact across the board on our society, which is disproportionate to how we see the size of the problem right now. We have a mechanism in Canada known as a royal commission that generally allows us to deal with things that are of a larger scale than simply a departmental responsibility. I've given testimony to several different committees of parliamentarians and the Senate. I've done work with individual government departments. In each case the stovepiping in how decision-making is being done means that there isn't a holistic approach to our being able to understand, as Canadians, and you as parliamentarians, how we need to approach this in a more overall manner where the impact is on domestic policy, where the impact is on our state policy, where the impact may be more narrowly focused on national defence. My encouragement to you as parliamentarians is to understand that this is a whole-of-society issue that requires debate and, like Ms. Moon has said, that we have to be forthright in understanding where the issues are and forthright in being able to identify them.

Thank you.

Mr. David Yurdiga: Thank you.

How much time do I have left?

The Chair: You have about a minute.

Mr. David Yurdiga: Okay. Excellent.

There's something I'm trying to figure out. We have the NATO body and we have the Parliamentary Assembly. What body determines what's relevant to each NATO member? Obviously, not every NATO member's involved in a specific task. Is there a body that actually determines what is relevant to which NATO member, and that one won't get that because it's not relevant to them? Is there a body that makes that sort of determination?

Mr. Rafal Rohozinski: I'll give you a very indirect answer. We have difficulty with that even domestically. There is no mechanism that compels, for example, banks to share information among themselves of threats they may share in common. There's no thing to compel telecommunication carriers, for example, to inform downstream organizations, whether those are banks or governments, of things that may be actually affecting them on an intelligence "sharing" level vis-à-vis cyber. This is a cascading problem that scales up to NATO.

I think the honest answer is no, there isn't a mechanism. There are mechanisms that we are trying to adopt, but there isn't a solution to this problem. That's one of the challenges.

Mr. David Yurdiga: Thank you.

The Chair: That's pretty much your time then, unless you can squeeze out a question and an answer in three seconds.

● (1015)

Mr. David Yurdiga: You can give up my three seconds.

The Chair: MP Alleslev.

Ms. Leona Alleslev: Thank you very much.

I would like to take your comments a bit further, Madeleine, on how we can ensure that we're communicating with our society. This study is about why Canada matters to NATO, and why NATO matters to Canada. Of course, as parliamentarians, we need to go back to our ridings and have these conversations. I hope an occasion will arise at some point when you will be able to speak to Canadians in a constituency. From a U.K. perspective, and of course as a founding member of NATO, how would you communicate why it should matter to Canada, and why it does matter or should matter to NATO that Canada is a member?

Ms. Madeleine Moon: There are so many places this can go. I am thinking about this in terms of an earlier question. You start with your borders. Where am I in the world? What are the boundaries around my country? Who are the neighbours? Then you move on to consider, what are the threats out there in the wider world and how might they come to our borders? What are the defences we have to protect ourselves with?

You can say such things as part of what we call the "Little Britain" view, but then you have to say, well, who do we need to be our friends? Who will stand by us? Britain's history stretches a long way back, and I think the Falklands was the one time we fought alone. Perhaps Jamie can think of another example. The rest of our history has been fought as part of alliances. In today's world it is very hard to stand alone. You have to stand not just with people who will fight with you as a country, but also those who share your values, who won't actually hollow-out your society by weakening those values with compromises, by allowing chemical weapons, for example, by seeing the mass rounding up of women and use of them as sex slaves. That's the sort of world you want to be allied to and working with.

We also have to explain to our populations that this world hasn't gone away. It didn't end in 1945. The world is still very dangerous. Some of the dangers are new and different, but the need for us to be resilient and ever-vigilant is still there, and no matter where you are in the world the risks are out there.

Canada faces two ways. You face into the Pacific and you face into the Atlantic. Now you're also facing into that opening up of new terrain of the Arctic. Boy, are you in dangerous waters. I hope your people will then understand why NATO is as important to you as it is to the little islands off the coast of Europe that are Great Britain.

Ms. Leona Alleslev: Well, thank you very much. To take it to the next step, can you give us a take on the fact that not all points in history are equal. Would you say that we're at a point where the temperature is rising, staying the same, or going down?

Ms. Madeleine Moon: I would definitely say it's rising, and I would say it's been rising for a while. I've been attacked for some time as being a Cold War warrior who is wanting to take us back in time. However, I think we have turned a blind eye for a long time to the risks that are coming our way. I think Jamie is right: The decisions that we've made over these chemical weapons, in particular, have allowed problems to grow. We have to wake up and stop being as complacent as we'd like to be about our security and the defence alliances that we're in, and also tell our populations that the world is a more dangerous place and they're heading towards us—

Ms. Leona Alleslev: As your Sir Richard Barrons says, we need to see the world as it is, not as we would hope it to be.

Ms. Madeleine Moon: Indeed.

Ms. Leona Alleslev: Mr. Shea, I would ask you to expand just a bit more on your commentary around international law, and perhaps the gaps in the cyber domain there. What do we need to do domestically in that area?

● (1020)

The Chair: Unfortunately, I'm going to have to yield the floor to MP Garrison, for the last formal question.

Ms. Leona Alleslev: Okay.

Thank you very much.

Mr. Randall Garrison: I'm going to ask a question of Mr. Shea. I will be in touch with him off-line about a particularly jarring remark in his opening presentation; I don't want to focus on that now.

You mentioned the concept of red lines for things like chemical weapons, and you talked about a role for Canada in advancing some norms on arms control.

Could you say a bit more about both the role of NATO in establishing some red lines with the new nuclear threats that we have with tactical weapons, and the idea of NATO pursuing some more activity in the area of arms control?

Dr. Jamie Shea: First of all, on the jarring remarks, forgive me—there was nothing intended to be jarring, but I'd be happy to address those off-line, sir.

Secondly, when we look at some of the new challenges—and we've spoken a lot today about cyber, but the Salisbury attack also shows that chemical weapons are still being used—we can certainly look at what we could do in the alliance, working together to increase our national resilience in dealing with chemical weapons if they should ever be used again.

There's clearly a need, for example, to be able to detect the type of weapon very early on, analyze exactly what it's all about, and therefore share the expertise among NATO laboratories. As you saw with polonium-210 when it was used in London in 2006, it can spread all around the place to a number of different sites, so tracking methodology is particularly important for protecting our civil populations. Of course, training intervention forces and those types of things would be important. Looking at medicine and so on—at what could be effective—is an area that we sort of gave up on after the Cold War, for obvious reasons. Certainly, one good example is to try to use NATO to regenerate certain core competencies, both at the national level and the NATO level.

In the nuclear and cyber realms there's also a lot of good work to be done. You'll remember the nuclear safety initiative that President Obama begun to track these materials around. Again, chemical weapons were smuggled over borders. That's clear, otherwise they could not have been used in London, so how can we work together on effective ways of identifying these things when they cross borders, including the intelligence-sharing piece as well, and working with countries and partners to ensure that they keep these things—when they have them—under safe lock and key?

In the cyber area, there are the CSBMs, How can we have international agreements that prevent cyber attacks against critical infrastructure like hospitals, power grids, and the things that our populations can depend upon? The U.S. and China, for example, have made an agreement that tries to outlaw these kinds of attacks, and so could we work to make that more of an international understanding?

There's a lot of good work to be done in this area. I was just suggesting politely and very humbly that a country like Canada, which has a good intellectual and diplomatic tradition, would be in a good position to take the lead in NATO as well.

Thank you.

The Chair: I'd like to thank all three of you for participating in our discussion today.

As I mentioned at the beginning, it's our last formal meeting on this particular topic. Now we're going to be talking about drafting instructions and recommendations to the Government of Canada on how we can make things better.

This conversation started some months ago. Obviously, after the last U.S. presidential election there was a lot of talk about NATO. The conversations seemed to shift to burden sharing and expenditures almost exclusively, which are important. Most people would agree those are important, but participation, capabilities, and all sorts of other things matter too. It's important that those things are considered, and it's a more complex conversation than just talking about who's spending what on NATO. We have a lot of work to do.

I want to thank you again for your participation in this conversation. We're going to suspend right now so we can get to work.

Thank you very much.

[*Proceedings continue in camera*]