HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

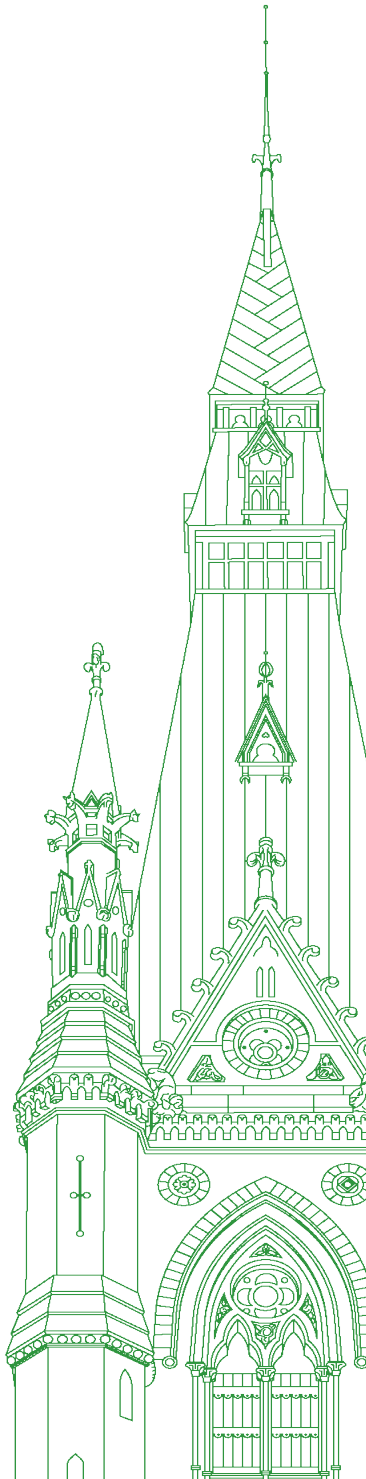
Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 037

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Thursday, October 6, 2022



Chair: Mr. Ron McKinnon

Standing Committee on Public Safety and National Security

Thursday, October 6, 2022

● (1100)

[*English*]

The Chair (Mr. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.)): Welcome to meeting number 37 of the House of Commons Standing Committee on Public Safety and National Security.

We will start by acknowledging that we are meeting on the traditional unceded territory of the Algonquin people.

Today's meeting is taking place in a hybrid format, pursuant to the House order of November 25, 2021. Members are attending in person in the room and remotely using the Zoom application.

Pursuant to Standing Order 108(2) and the motions adopted by the committee on Thursday, March 3, 2022, the committee is resuming its study on the assessment of Canada's security posture in relation to Russia.

With us this morning we have, from the Department of National Defence, General Wayne Eyre, chief of the defence staff, Canadian Armed Forces; Vice-Admiral Auchterlonie, commander of the Canadian Joint Operations Command; and Major-General Michael Wright, commander, Canadian Forces Intelligence Command and chief of defence intelligence. From the Communications Security Establishment, we have Ms. Caroline Xavier, chief; and Mr. Sami Khoury, head of the Canadian centre for cybersecurity.

Thank you all for joining us today. We look forward to your remarks.

General Eyre, I welcome you to make your opening statement for five minutes, give or take. We won't be too hard on you.

General Wayne D. Eyre (Chief of the Defence Staff, Canadian Armed Forces, Department of National Defence): Mr. Chair, thank you for this opportunity to discuss our geopolitical security environment, specifically the threat Russia poses to Canada.

I am happy to be here with Vice-Admiral Auchterlonie, who is the operational commander of our international and domestic operations, as well as Major-General Wright, who commands our intelligence enterprise. I'm also very happy to be here with my colleagues from CSC, Caroline Xavier and Sami Khoury, as you introduced.

We once again find ourselves in a chaotic and dangerous world where those with power, namely, Russia and China, are determined to remake the world order to suit their own ends and where the rights and freedoms of smaller, less powerful states are discarded. We are also witnessing violations of the sanctity of territorial sovereignty and of responsible dialogue about the use of nuclear weapons.

Russia and China do not differentiate between peace and war.

[*Translation*]

In seeking to achieve their national objectives they will use all elements of national power, often acting just below the threshold of large-scale, violent conflict—but, as we have seen in Ukraine, they are all too willing to cross that threshold.

Their aim is not just regime survival, but regime expansion.

[*English*]

In this context, they consider themselves to be at war with the west.

Their greatest threat comes not from external adversaries but from their own populations, so they strive to destroy the social cohesion of liberal democracies and the credibility of our own institutions to ensure that our model of government is seen as a failure.

We are seeing an example of this information war in real time, where the Ukrainians are winning the battle between truth and lies in the west, but the Russian narrative dominates in many other parts of the world.

Will we have an international order based on rules or one based on might? This contest of which order will prevail will certainly define the rest of our time in uniform and, indeed, the rest of our lives.

[*Translation*]

Many of our allies and partners are clear-eyed about the threat to our future.

We must be, too.

The stakes are high.

We must not allow authoritarian powers to change the world order to suit their purposes.

● (1105)

[*English*]

We must be strong. We must work with our partners and allies in a united front, and in doing so, deter miscalculation, adventurism and great power war.

Regarding our own national security, the distance and geographic isolation that Canada has enjoyed for so long is no longer a viable defensive strategy. Canada and the United States agreed in 2021 to invest in a long-needed modernization of NORAD, but Russia has also made significant investments, including in long-range aviation and the capability of the cruise missiles that its planes carry.

Russia also has the capability to threaten Canada via other domains, by sea but also in the cyber and space domains, where it is capable of threatening our networks, critical infrastructure, communications and economy.

[*Translation*]

Finally, there is the nuclear threat, repeated in a not so thinly veiled manner numerous times recently.

Right now, we do not believe that Russia plans to use strategic nuclear weapons against Canada. However, given the unfolding crisis in Ukraine and the potential for escalation, we must remain vigilant.

[*English*]

The Russian threat is very clear. Fortunately, so are the actions that we must take to meet that threat. As we prepare for the possibility of open conflict in traditional domains, we must also develop our capacity for confrontation in the cyber, space and cognitive domains.

We must integrate our capabilities across all domains. We must develop an integrated approach to national security that combines military responses with diplomatic, economic and information actions at the local, regional, national and multinational levels.

[*Translation*]

We must maintain an intellectual advantage, generating diverse policy options and ideas via an ongoing dialogue among allies, agencies, industries, academia and governments. This will be critical to sustaining our strategic edge.

[*English*]

We must not be naive about the threats in the world. Adversaries view compromise as weakness to be exploited. They only respect and respond to strength.

The rules-based international order, which has underpinned world stability and indeed our national prosperity for generations, is faltering. It needs to be defended. The gravity of these times should be apparent to all.

Thank you. We look forward to your questions.

The Chair: Thank you, General.

I would now invite Ms. Xavier to make an opening statement.

Ms. Caroline Xavier (Chief, Communications Security Establishment): Hello and *bonjour*. Thank you, Mr. Chair and members of the committee, for the invitation to appear today to discuss Canada's security posture in relation to Russia.

My name is Caroline Xavier. My pronouns are she, her and *elle*. I am the new chief of the Communications Security Establishment, known as CSE.

I am joined today by Sami Khoury, head of CSE's Canadian Centre for Cyber Security, which you have heard referred to as the cyber centre.

I'm pleased to join you. I too would just like to take a moment to acknowledge the land from which I'm joining you today, which is the traditional unceded territory of the Algonquin Anishinabe nation.

[*Translation*]

Today, I'd like to provide the committee with a brief update on CSE's role in Canada's cyber security posture as it relates to Russia, and some of the recent work that CSE has done to protect Canadians from related threats.

[*English*]

CSE, reporting to the Minister of National Defence, is one of Canada's key security and intelligence agencies. The Communications Security Establishment Act, or the CSE Act, sets out five aspects of our mandate: cybersecurity and information assurance, foreign intelligence, defensive cyber operations, active cyber operations, and technical and operation assistance. As part of this mandate, CSE is the country's lead technical authority for cybersecurity.

[*Translation*]

The Canadian Centre for Cyber Security, more commonly referred to as the Cyber Centre, is a branch within CSE and a single point of expertise on technical and operational cyber security matters.

[*English*]

I will now provide a brief breakdown of the key findings regarding the current cyber-threat landscape particularly as it relates to Russia. I should note that CSE has issued four bulletins about Russian-backed activities this year focused on threats to cybersecurity and on disinformation.

● (1110)

[*Translation*]

To set the stage, I'd like to highlight some of the current cyber threat challenges Canada faces. We identified these in our national cyber threat assessment, which I would encourage you to read if you'd like to have a better understanding of the current threat landscape.

[*English*]

In that assessment, we highlighted that cybercrime is the most prevalent and most pervasive threat to Canadians and Canadian businesses. Cybercriminals trying to probe Canadian systems have been found in Russia, China and Iran, among others. These actors use various techniques, such as ransomware, theft of personal data and online fraud. Critical infrastructure operators and large enterprises are some of the most lucrative targets.

While cybercrime is the most likely threat to impact the average Canadian, the state-sponsored cyber programs of China, North Korea, Iran and Russia pose the greatest strategic threat to Canada. Foreign cyber-threat activities, including Russian-backed actors, are attempting to target Canadian critical infrastructure operators as well as their operational and information technology.

[*Translation*]

Russia has significant cyber abilities and a demonstrated history of using them irresponsibly. This has included the SolarWinds cyber compromise, disruptions of COVID-19 vaccine development, threats to Georgia's democratic process and the NotPetya malware.

[*English*]

Besides Russian-backed challenges to Canadian cybersecurity, as I have noted, Russian disinformation campaigns also threaten Canada and Canadians. In July of this year, CSE noted that it had continued to observe numerous Russian-backed online disinformation campaigns aimed at supporting Russia's brutal and unjustifiable invasion of Ukraine.

[*Translation*]

Now that I've gone over some of the key trends and threats, I'd like to provide an overview of how CSE's mandate helps us address these challenges.

CSE has unique technical and operational capabilities, which allow us to respond to the various types of threats Canada faces, such as the threat of hostile state actors.

[*English*]

CSE's foreign signals intelligence program provides sophisticated capabilities that allow us to access, process, decrypt and report on current and emerging cyber-threats. We then use this information to brief and disseminate to government.

[*Translation*]

The foreign intelligence CSE collects allows us to pass that information to not only critical infrastructure owners and operators in Canada, but also to our allied and NATO partners, as well as Ukraine.

[*English*]

Having this information ahead of any materialized threat allows them to proactively protect and defend their systems. The CSE Act further enables us to provide technical and operational assistance to federal law enforcement, security and defence partners, including the Department of National Defence, our Canadian Armed Forces, the RCMP and the Canadian Security Intelligence Service, or CSIS. This means that CSE is authorized to assist the CAF in support of government-authorized military missions, such as Operation Unifier. This includes intelligence sharing and cybersecurity.

[*Translation*]

One of CSE's main roles is to inform the government of the activities of foreign entities which threaten Canada or its allies. This may include foreign-based cyber threats, espionage, terrorism and even disinformation campaigns.

[*English*]

For example, since the Russian invasion of Ukraine began, we have observed numerous Russian-backed disinformation campaigns online that are designed to discredit and spread disinformation about NATO allies, as well as false narratives about Canada's involvement in the Russia-Ukraine conflict.

[*Translation*]

For example, controlled media outlets were directed to include doctored images of Canadian forces members on the front line and false claims about Canadian forces committing war crimes.

[*English*]

We shared this information on Twitter as part of the Government of Canada's efforts to help inform Canadians on how to help stop the spread of and protect themselves from disinformation.

We will continue to work closely with our Five Eyes partners, as well as harness all of our expertise to confidently ensure Canada's resiliency against threats in terms of cybersecurity or disinformation.

[*Translation*]

Although Russian cyber threat disinformation actors are becoming increasingly more sophisticated, I can assure you that we are working tirelessly to raise Canada's cyber security bar and protect all Canadians from these emerging threats.

[*English*]

We have the necessary expertise in place to monitor, detect and investigate potential threats. We are developing further capabilities and capacities to take active measures to protect, deter and defend against them.

● (1115)

[*Translation*]

We also continue to publish advice and guidance for Canadians and Canadian businesses to improve their cyber security practices.

[*English*]

We will continue to collaborate closely with our Five Eyes and NATO allies to protect the critical infrastructure, economies and democratic systems of our country.

With that, I will be pleased to have the opportunity to answer any questions you might have.

[*Translation*]

Thank you.

[*English*]

The Chair: Thank you, Ms. Xavier.

We'll start our round of questions with Ms. Dancho.

Please go ahead for six minutes.

Ms. Raquel Dancho (Kildonan—St. Paul, CPC): Thank you, Mr. Chair.

Thank you very much to the witnesses for being here. It is an honour to have them here.

General Eyre, it is an honour to meet you in person. Thank you for everything you and your colleagues are doing to keep Canadians safe. I have a number of questions for you.

I've been reviewing some of the media that you've been doing in recent months. I'm quite concerned by some of the things you've been sharing with Canadians on the state of our military and our military preparedness.

In May 2022, you mentioned, “Given the deteriorating world situation, we need the defence industry to go onto a wartime footing and increase their production lines.” You went on to say, “We're facing a security situation in the world that is as dangerous, or more dangerous, than the end of the Cold War.” You also said, “Canada is not nearly as secure as it once was.”

Our understanding throughout the study we've been having is that since the conclusion of the Cold War, our infrastructure and defence capabilities that went along with our NORAD infrastructure have been neglected, as has our Canadian military, perhaps.

Can you comment on that, given the context of what you're saying about how we may be in a more dangerous situation than during the Cold War?

Gen Wayne D. Eyre: Mr. Chair, I think that the comments the member attributes to me are reflected in my opening statement as well about the urgency of the security situation that we are currently facing. I am concerned that as the threats to the world security situation increase and as the threats at home increase, our readiness is going down within the Canadian Armed Forces.

That is the reason we have embarked on what we're calling reconstitution. Reconstitution is a military operation that is used after a large-scale operation to rebuild, re-arm and re-equip.

The pandemic has not been kind to the Canadian Armed Forces, as our numbers have shrunk. We're embarking on a priority effort to get our numbers back up in recruiting and retention so that we can provide that readiness.

Readiness is more than just people. Readiness is also based on training, equipment and sustainment. We're working in those other three areas as well to make sure that we can provide the readiness that is essential so that we can respond at scale and speed to the needs of Canadians. We have lots of work to do in front of us.

Ms. Raquel Dancho: Thank you, General.

You were also quoted in the Toronto Star today that the rebuilding process needs to occur on an accelerated timeline and that the shortcomings that you've discussed today are preventing the Canadian Armed Forces more specifically, “from being in the position it needs to (be) in order to excel as a modern and combat-ready military force". Further, you went on to say that ultimately these personnel shortages are “jeopardizing the readiness and long-term health of Canada's defence capabilities.”

Can you outline for the committee and add on to that on how serious is this? How serious does the federal government need to be taking these investments that clearly are critical to our national security?

Gen Wayne D. Eyre: Mr. Chair, this is a challenge that not only every western military is facing, but we're facing it here at home as well with labour challenges and real challenges in the workforce. That's reflected in our own numbers. I am very worried about our numbers. That's why we're putting as the priority effort the reconstitution of our military.

What we're doing about it specifically is looking at our recruiting system. We've staffed our recruiting system to 100%. We are streamlining the recruiting system. We've brought in a retention strategy. There are many more things that we continue to work on to ensure that the quality of service that our members experience is what it needs to be.

Let's face it, nobody joins the military to get rich. What we offer is something transcendent. It's the ability to serve your country. We have to make sure that the quality of service is extended to such aspects as financial security for our members and their families; quality equipment, so they can work on modern equipment; quality infrastructure that they can have; and meaningful employment, and that means meaningful overseas deployments as well as meaningful employment here in Canada.

● (1120)

Ms. Raquel Dancho: Thank you, General.

Can you comment on the importance of reaching our 2% spending commitments for NATO? Is that a relevant number? Should we be trying to reach that quickly, or at an accelerated rate, as you've said?

Gen Wayne D. Eyre: Mr. Chair, it's not my position to talk about the specifics of our defence spending and any arbitrary target.

I will tell you that the military we have today is not the military that we need for the threats that are appearing in the future. We need to continue to look at and assess those threats, and make sure we have the capabilities to address those emerging threats.

Ms. Raquel Dancho: General, with my last minute, would you say that Canada is prepared for any eventuality in terms of defending itself?

Gen Wayne D. Eyre: Mr. Chair, “any eventuality” is a pretty broad characterization of the security environment. We have to deal in probabilities, because the imagination could run wild.

Ms. Raquel Dancho: I was just going to say that when the war in Ukraine and the Russian invasion first broke out, I had brought this question to our Minister of Defence, Minister Anand. I asked if Canada was prepared for the threats that Russia is making not only to Ukraine but to the world and those who help defend Ukraine. She responded that Canada is prepared for any eventuality. Given your comments and what we've learned during this study, I am very concerned that this is not the case.

With my concluding few seconds, can you comment on what needs to be done today and in the coming months to ensure we are prepared for the most likely, or any eventuality?

Gen Wayne D. Eyre: Mr. Chair, as I say, we need to rebuild our readiness so that we can respond with a sufficient number of forces at the speed required. That is what we are focused on right now, those four elements of readiness that I talked about.

Ms. Raquel Dancho: Thank you very much, sir.

The Chair: Thank you, Ms. Dancho.

We go now to Mr. Chiang for six minutes, please.

Mr. Paul Chiang (Markham—Unionville, Lib.): Thank you, Mr. Chair. Good morning.

I would like to thank all the witnesses for taking time to be here today.

My question is for General Eyre.

The director of the CIA, William Burns, has recently stated that while the CIA has not seen any practical evidence that Putin is moving closer to the use of tactical nuclear weapons, what we have to do is take it very seriously and watch for signs of actual preparation.

What would these preparations look like in Russia, and what should the response be from Canada if this does happen?

Gen Wayne D. Eyre: Mr. Chair, this is something we watch closely as well. We have to be concerned about the possibility of escalation. That being said, we cannot allow nuclear coercion to stop us from doing the right thing. Others are watching, and it will become a model for the future.

In terms of the details, I'll turn it over to General Wright to provide additional context.

Major-General Michael Wright (Commander, Canadian Forces Intelligence Command and Chief of Defence Intelligence, Department of National Defence): Mr. Chair, I would absolutely agree with the director of the CIA that Russia has the capability. What the Five Eyes alliance and our NATO allies are laser-focused on is whether the intent exists.

In terms of the question regarding indicators, this is obviously something the Five Eyes alliance is laser-focused on. We do closely track indicators and warnings. However, because of the sensitivity of those, I don't think we can discuss that in this forum.

Mr. Paul Chiang: Thank you so much.

What do we know about politicians within Russia calling for the removal of Putin from office and the accusation that some have made of high treason against him? Is Canada tracking these internal developments in any way?

Gen Wayne D. Eyre: I'll first turn to General Wright again to address that one.

MGen Michael Wright: Mr. Chair, we closely track all aspects of the conflict with Russia, and we have since the days before the invasion, when Vladimir Putin was blatantly lying that it was only a military exercise. We have been trying to ascertain both his intentions and also the strength of the Russian state and the support for him.

What I would say is that Vladimir Putin has spent over 20 years consolidating power in the state around him and a very small group of advisers.

Ms. Caroline Xavier: If I may, Mr. Chair, there is only thing I would add.

CSE being the national foreign intelligence signals intelligence program, we provide intelligence so that senior decision-makers are able to get some of that insight into the activities, the motivations, as well as the capabilities and the intentions of some of those foreign adversaries, including some of the ones you mentioned.

That's about the extent of what we can discuss this morning.

Mr. Paul Chiang: Thank you so much.

As this war progresses in Russia and in Ukraine, and as Russia seemingly becomes more desperate to annex certain regions of Ukraine and claim victories in the region, do you believe the cyber-threats to Canada from Russia increase, decrease or remain the same, and why would that be?

● (1125)

Ms. Caroline Xavier: Mr. Chair, can I just get the question repeated again?

Mr. Paul Chiang: Of course.

As this war progresses, and Russia seemingly becomes more desperate to annex certain regions of Ukraine and claim victories in the region, do you believe the cyber-threats to Canada from Russia increase, decrease or remain the same?

Ms. Caroline Xavier: Thank you for the question, Mr. Chair.

What we have seen is that there have been ongoing threats from Russia with regard to their cyber capabilities, and they've demonstrated a willingness to use them. Since early January or mid-January, we've put out several bulletins, and we're putting out information about the Russian threats and vulnerabilities that they like to typically exploit, along with advice and guidance on how to mitigate them.

We have put out in our “National Cyber Threat Assessment” what our views are with regard to hostile state actors, Russia being one of them. As a result, we are concerned about whether or not the opportunities could present themselves. What we also assess, however, is that they would not be perhaps directing some of those cyber-threats directly to us in terms of our critical infrastructure, given that we are not directly implicated in the conflict. However, we continue to monitor and investigate, and identify whether or not we need to provide advice for the actions that need to be taken.

Mr. Paul Chiang: Thank you so much.

Again, this question is for Ms. Xavier.

When you speak about hostile state actors, would you think that Russia is involved in any way in the conflict that's going on between Azerbaijan and Armenia now?

Ms. Caroline Xavier: I can't comment in terms of things that are not at a level that I can discuss in this unclassified environment; however, as I mentioned, we continue to closely work with our allies and monitor what is going on in the global world with regard to hostile state actors.

As we stated in our “National Cyber Threat Assessment”, we do see that Russia is one of those actors that have the sophisticated ability to be able to use their cyber programs. As a result, we are quite concerned, and it's an area where we work with our allies in identifying what the threats may be, put out necessary advice and provide intelligence to decision-makers to be able to take the necessary actions.

Mr. Paul Chiang: Thank you so much.

The Chair: Thank you, Mr. Chiang.

[*Translation*]

Ms. Michaud, you have the floor for six minutes.

Ms. Kristina Michaud (Avignon—La Mitis—Matane—Matapédia, BQ): Thank you, Mr. Chair.

I thank the witnesses for being with us today. I appreciate it.

My first question is for Ms. Xavier.

Ms. Xavier, I have read a *Journal de Montréal* article published in May 2022. In it, there are a number of figures on the Communications Security Establishment. According to the article, since the Russian invasion, the number of cyber-attacks has jumped 16% worldwide. In 2021, ransomware attacks shot up 151% over 2020, also worldwide. Canada alone experienced 235 known attacks.

For the benefit of committee members, could you explain why all this information is not known?

You said that this was the tip of the iceberg, but not all attacks are reported. Why aren't they all reported? Should we be doing more to encourage organizations under attack to report it?

As I understand it, there's nothing binding at this time. However, it could certainly be useful for any organization that might be a victim of an attack.

What do you think?

Ms. Caroline Xavier: Thank you for the question.

Of course, we'd like Canada to be immune from cyber-threats. Our agency's goal is to try to ensure that all organizations and all Canadians are aware that they need to be mindful of how they manage their data.

As you mentioned, we're seeing an increase in ransomware attacks. That's why we're working very closely with industry, various levels of government and Canadians. We're looking to educate them and raise awareness.

We're also working closely with organizations that report having been victims of cyber-attacks. However, as you said, many organizations don't report it. Nevertheless, we continue to discuss it openly with industry.

We do a lot of outreach and awareness sessions to let people know that we're there to provide the support they need. We also put out a lot of advisories to explain the risks so that they can protect themselves and prevent possible attacks.

We're concerned about this, obviously. But Canada isn't the only country suffering from the fact that many organizations don't want to disclose the attacks they are experiencing. We discuss this with all our allies around the world, and we continue to tell organizations that it's important to contact us. We know how to be discreet, and how to work with them to help them find the solution to their problem.

● (1130)

Ms. Kristina Michaud: Thank you, Ms. Xavier.

General Eyre, thank you for your opening remarks. I thought you were very forthcoming. It's refreshing to have people come in and give us the straight goods, even if some of the things you say can be scary at times. In particular, I'm referring to what you said about countries like Russia and China being willing to do anything to serve their own interests.

If I'm not mistaken, you said that you were not concerned that Canada would be the target of a nuclear attack by Russia. However, some of the experts we've had at committee didn't hesitate to compare nuclear weapons to cyber-weapons.

If you don't fear a nuclear attack, are you afraid of cyber-attacks, which could have very significant consequences for Canada?

Gen Wayne D. Eyre: Thank you very much for the question.

Exact comparisons are difficult between the two threats, cyber-attacks and nuclear attacks, but both pose a threat to our country and we must be prepared to respond.

I'd like to turn the floor over to Major General Wright of Canadian Forces Intelligence Command for his comments.

MGen Michael Wright: Thank you.

Russia is certainly able to launch cyber-attacks and target critical structures in Canada. It's also important to remember that Russia views North America as a target. It doesn't distinguish between the United States and Canada.

On the specific topic of cyber-attacks, our expert here is the chief of CSE.

Ms. Kristina Michaud: Thank you, Major General Wright.

That's very interesting, what you're saying about North America being a single target. I understand that North America is not in the same situation as Ukraine right now. Still, there might be cause for concern over retaliation for the economic sanctions both Canada and the United States have imposed on Russia, among the things.

Do you feel we're well prepared at this time to deal with cyber-attacks, should any occur?

Gen Wayne D. Eyre: Thank you for the question.

It's always difficult to prepare for a nuclear attack. We need to keep working with our colleagues at North American Aerospace Defense Command, or NORAD, so that they can send us a warning in the event of an attack.

Actually, it's hard to prepare for the consequences of an attack like that. I believe that we must continue to build our national resilience against all types of disasters—

[*English*]

Mr. Tony Van Bynen (Newmarket—Aurora, Lib.): On a point of order, Mr. Chair, I'm not getting translation.

The Chair: Thank you, Mr. Van Bynen. We'll check on that.

● (1135)

Mr. Tony Van Bynen: Okay. I can hear you in English now.

The Chair: Well, I'm speaking English right now, so....

General, if you could start your answer from the beginning, we'll make allowances for the time.

[*Translation*]

Gen Wayne D. Eyre: As I was saying, it's hard to prepare for a nuclear attack because there are huge consequences.

I believe that we must continue to build our national resilience to respond to the various types of disasters.

At the same time, we must continue to work closely with our American colleagues at NORAD. We believe it's critical that we receive NORAD warnings in the event of an attack on our continent.

[*English*]

The Chair: Madam Michaud, I think you have one more minute.

[*Translation*]

Ms. Kristina Michaud: I'd like to ask one last quick question.

We're right to worry about the threats that Russia poses right now.

However, considering that over 80% of Russian forces are currently invading Ukraine, can we afford to be less worried about Russia's ability to attack in any way shape or form, be it another country or North America?

We shouldn't underestimate what Russia can do.

Wouldn't you agree?

Gen Wayne D. Eyre: That's an excellent observation. I must say, however, that while Russia has deployed most of its land forces, it still has many other forces. You're right, we mustn't forget the air force, the naval force and the strategic force. So, the threat is still there.

The Chair: Thank you, Ms. Michaud.

[*English*]

We'll go now to Mr. MacGregor for six minutes, please.

Mr. Alistair MacGregor (Cowichan—Malahat—Langford, NDP): Thank you very much, Mr. Chair.

Thank you, witnesses, for being here. I know how valuable your time is, and our committee sincerely appreciates your being here today.

General Eyre, I'd like to start with you.

One thing we have been witnessing with Ukraine is what is possible when you have a determined fighting force combined with western training and western equipment. I think we've all been quite astonished at the capabilities of the Ukrainian military.

At the same time, I think we've also had the opportunity to learn more about Russian military capabilities, their fighting doctrine, the morale of their troops, etc. We know from public news sources that they have suffered some serious setbacks in the last month.

I know Canada and all of its NATO allies are paying attention to this conflict. In general terms, what have we learned about Russian military capability from this conflict, and how is NATO doctrine evolving from that assessment?

Gen Wayne D. Eyre: Mr. Chair, I thank the member for the question.

I'll say a few things and then give Vice-Admiral Auchterlonie, who monitors this on a daily basis, the chance to make a few comments.

I will say that the will to win that we see within the Ukrainian forces is probably the key determinant of their success.

We were very happy to see Ukrainian forces embracing what we call mission command—empowerment at the lowest levels to be able to go off and improvise, take advantage of the local situation and create success. We're not seeing that on the Russian side. They have very much the old Soviet mentality of a top-down, centrally driven command style. That is one of the big observations.

We've seen failures on the Russian side—failures at the strategic level to connect ends, ways and means. Their political ends have not matched their military ways and means. We've seen a disconnect there in that they've constantly had to readjust what those ends are going to be. Even now we're doubtful whether their maximalist ends are achievable.

We've seen challenges as well throughout their force, whether on the training side or in the ability to integrate combined arms—that's artillery, engineers and air force all working together. It's just not there. Their logistical challenges are pretty significant.

What we as a force have learned and reinforced is just how powerful empowering a highly motivated force and giving them the authorities and the resources to act on the ground can be.

I am very proud of the training our forces have done since 2015 and of how they have been able to impart that leadership style at the lowest level. That training continues today with Operation Unifier.

With that I'll turn to Vice-Admiral Auchterlonie.

● (1140)

Vice-Admiral J.R. Auchterlonie (Commander of the Canadian Joint Operations Command, Department of National Defence): Thank you, Mr. Chair.

Thank you, Chief.

As the chief noted, we've been conducting Operation Unifier since 2015, training our Ukrainian armed forces partners along with our allies—U.S., U.K., Lithuania and other countries—to ensure that they had that capability and the training to maximize their capability in the field.

I really echo their comments. The Ukrainian armed forces have been exceptionally impressive, and they're determined in their will to fight for their country. That's been quite impressive.

You talked about lessons learned, which are quite key. Obviously we're learning from this conflict. We learned from the Ukrainians in 2015. With respect to the Donbass, we took a lot of the lessons from 2015 and modified our tactics and procedures within NATO and within Canada and our allies, and we're learning today against the Russian forces.

What I would caution is that we're learning; the Russians are learning and the Chinese learning. This is something for the committee. The fact is that we're not the only ones learning from this event.

What you have seen is that cohesion in the west has happened, and that has been phenomenal, and the cohesion in NATO has been great. I think our adversaries around the globe are seeing that, and they will react to it. So as it's going on, we're going to learn. We're a learning institution. The other organizations are also going to learn from this.

Mr. Alistair MacGregor: Thank you.

I want to get in another question for CSE. I have only a couple of minutes left.

You're aware, I think, of the government's legislation, Bill C-26, which is going to designate vital systems and vital service providers and which makes some pretty significant amendments to the Telecommunications Act. A lot of what you talked about regarding the disinformation campaigns we as a committee are very familiar with. It has informed a lot of the studying of ideologically motivated violent extremism.

Aside from what's included in Bill C-26, I'm interested in CSE's working relationship with social media companies. Can you provide an assessment of how that is and tell us what more policymakers and the legislative sphere need to pay attention to in order to maybe make your job a bit easier in that relationship?

Ms. Caroline Xavier: Thank you, Mr. Chair, for the question. I really do appreciate it.

We actually have a great cyber partnership program with industry, with academia and with the social media organizations. I'm actually going to hand this question over to the head of the cyber centre, because he works with them practically every day.

Mr. Sami Khoury (Head, Canadian Centre for Cyber Security, Communications Security Establishment): Thank you, Mr. Chair, for the question.

As the chief pointed out, we do have a very good working relationship with lots of tech companies out there, including social media companies. The nature of our relationship with those companies is to make sure that we understand how they mitigate cyber-threats and how we facilitate co-operation in the event that we need their help in tracking cyber acts or cyber-threats. That is the nature of our engagement with cyber-tech.

We've also put out some publications, especially this year, to help Canadians spot misinformation or at least be more aware of where to get their credible news and how to spot some kinds of misinformation or disinformation campaigns. That's the threat the cyber centre takes on misinformation/disinformation and engagement with tech companies.

The Chair: You have nine seconds. Thank you, Mr. MacGregor.

That wraps up round one and we will start round two. We won't be able to do a full round two. Each party will have time for only one question slot. We'll start with Mr. Lloyd for five minutes.

Mr. Dane Lloyd (Sturgeon River—Parkland, CPC): Thank you, Mr. Chair.

Thank you to all the witnesses for being here.

Sir, given what you've said about the recruitment and retention challenges in the Canadian Forces and how serious they are for our readiness, I'm wondering if you can tell us what the barriers or challenges are—are they philosophical, legislative or operational?—to including permanent residents in the Canadian Armed Forces.

Gen Wayne D. Eyre: Mr. Chair, it's an excellent question.

Right now there are no barriers for permanent residents. We are about to make that much more public to attract that segment of our society into our ranks.

Mr. Dane Lloyd: I was not aware of that. Thank you for saying that. I know, having talked to recruiters, that very often we have new Canadians or permanent residents who want to serve because they love our country. It's good that we're finding ways to include them in that.

Sir, one of the challenges we're seeing in Atlantic Canada, which we saw in Abbotsford last year, is that the Canadian Forces' ability to respond to disasters is limited, but they've taken an increasingly frontline role. I'm wondering if you can comment on your views about the benefits, perhaps, or the challenges of a civil protection force of civilians to be a force multiplier to support the military in these sorts of situations.

● (1145)

Gen Wayne D. Eyre: Mr. Chair, it's another issue that is near and dear to us as we take a look at our ability to respond.

Let me first say that our top priority is protecting Canadians here at home. When the call comes, we shelve everything else to make sure we have the capacity to respond at speed. That being said, with the increasing frequency and intensity of these natural disasters, we are being called upon more and more to respond not necessarily as a force of last resort, but in some cases as a force of first choice.

What is needed? It's additional capacity. It could be at the municipal or provincial level. That being said—and I've publicly stated this before—given the extent of the disasters we're facing, we still have to be that force of last resort. The Canadian Forces still has to be there as the ultimate insurance policy for this country if there is not sufficient capacity.

What we provide and what any other organization should provide is that formed, organized labour pool that has its own inherent sustainment so it can supply itself; it can move itself; it can provide its own command and control and it can look after itself. That's the real value of what we provide. Any similar organization, any supplementary organization, should provide the same kinds of attributes.

Mr. Dane Lloyd: This question relates to this study.

As we know, foreign state actors are trying to target our critical infrastructure. I'm wondering if you could speak to why that is, in your opinion. Is it just because of the intensity and the frequency of these disasters that the Canadian Forces are being called upon more regularly, or is it because we've seen a degradation in our other capabilities and that is leading to the Canadian Forces...? Are our non-military capabilities being degraded? Is that why the Canadian Forces are being called upon? Why is this happening?

Gen Wayne D. Eyre: Again, Mr. Chair, that's a great question.

One could argue about what other capabilities. Did they actually exist, or should they exist? The other piece you talk about is attacks on our critical infrastructure. As we take a look at deterrence, how do we deter those attacks? One of the concepts or one of the sub-elements of deterrence is deterrence by denial. What that means is that adversaries' attacks are not successful, so they won't try it in the first place. If we can identify those single points of failure, if we can prove to be resilient as a society, as a nation, to thwart the intent of those attacks, they may not happen in the first place.

Our adversaries are looking for soft targets. We've learned this on operations around the world. If we present a soft target, we invite ourselves for attack.

Mr. Dane Lloyd: Thank you.

In my last 30 seconds here, I'll just observe that I think General Omar Bradley said that amateurs study strategy and professionals study logistics. I think we're seeing that the Russian logistics are absolutely collapsing on the Ukrainian front. What can Canada do to ensure that our logistics are strong going forward?

Gen Wayne D. Eyre: Mr. Chair, it's another item of concern. One of the observations over the course of the pandemic was that our own internal supply chain and internal sustainment system needs work.

Currently, as one of our lines of effort, one of the initiatives we're working on is increasing our own ability to sustain ourselves and to ensure that our logistics are strong. It's a work in progress. It requires people. It requires technology. It requires equipment. Given the nature of our country and the geography of our country, where we are in the world, ensuring that we can project our capabilities to where they are needed internationally but also domestically requires a high degree of logistics, which we must continue to invest in.

The Chair: Thank you, Mr. Lloyd.

Mr. Noormohamed, you have five minutes, please.

Mr. Taleeb Noormohamed (Vancouver Granville, Lib.): Thank you, Mr. Chair.

I want to echo my colleagues' comments by thanking all of you for the work you do in keeping Canada safe. It's a complicated world, and we're grateful for all that you do.

General, you spoke in your opening comments about the importance of demonstrating strength. We know that we are never going to be the largest fighting force in the world. We're not going to spend the most money on the military. What do you think the strength that you talk about needs to look like?

● (1150)

Gen Wayne D. Eyre: Mr. Chair, I firmly believe that the competitive advantage we have as a country is in being in a group of like-minded friends, allies and partners—well, like-minded or like-minded enough—who share enough in common in terms of values so that they can stand together against aggression, against adventurism and against expansionist policies. Working together with those partners, allies and friends is incredibly important, as is doing our part to share in that collective strength and collective deterrence.

Mr. Taleeb Noormohamed: Thank you.

The second part of your closing struck me. You said that our way of life "needs to be defended". What does that defence look like, in your view?

Gen Wayne D. Eyre: Mr. Chair, in my view, that means engaging in the world responsibly, supporting our friends and allies when they need support, doing our part to support them, being ready to support them and being transparent about our intentions.

Let's face it, the rules-based international order that has been in place since the end of the Second World War has underpinned our national prosperity. It has underpinned our economic growth. I for one believe it's worth defending.

[*Translation*]

Mr. Taleeb Noormohamed: Ms. Xavier, you spoke at length about state-sponsored cyber-crime and the threat Russia poses to our way of living and the fabric of our Canadian society by spreading disinformation.

Based on your work and what you have seen, can you tell us what impact these threats are having on Canada?

Ms. Caroline Xavier: Thank you for the question.

I'd like to confirm that I understood your question correctly.

You're asking me to comment on what I've seen, based on my work.

Is that correct?

Mr. Taleeb Noormohamed: I'm talking about what you've seen in the course of your work.

I realize that there is classified information and you can't discuss that with us. Of the threats you can discuss, which ones have you seen and how have they impacted Canada?

Ms. Caroline Xavier: Thank you for the question.

What I can tell you is that the Communications Security Establishment Act authorizes us to shut things down using the tools available to us, to protect ourselves and to make sure that our systems can defend themselves against those threats.

As mentioned earlier, we work very closely with our international partners, especially those in the Five Eyes.

We make sure that we have the capacity to know what types of threats exist so that we can get the information to Canadians and businesses that need it. It's about protecting not just government systems, but critical systems that are essential to managing Canada.

[*English*]

Mr. Taleeb Noormohamed: The other thing you talked about, and it was almost like a passing comment, was that you had to resort to Twitter to explain something to Canadians.

How has CSE had to change the way you think about dealing with misinformation in your own operations and, in particular, how you talk to Canadians?

For a very long time nobody knew what CSE was, and everyone was quite happy about that. When I was a young public servant, somebody tried to recruit me to CSE, and I had no idea what it was. Now you've taken a more public posture. You've had to do that in the world in which we operate. How has it changed the way in which you do your business in terms of letting Canadians know about things they need to know about, and what has that meant for your organization?

Ms. Caroline Xavier: Thank you very much for the question. I really do appreciate that.

You're right that we have had to look at things differently. We've had to change the way in which we work. We're really proud of the fact that we've had to do this categorical shift on this aspect of having to use Twitter and declassify intelligence to be able to share it with Canadians but also with allies that are fighting...with partners that are in Ukraine. This is unprecedented.

These are not things we've had to do before, but we continue to explore ways and manners in which we can continue to ensure that Canadians are aware of the threats in whatever manner we can that doesn't impact our trade craft or impact the way in which we do our business.

This is the new world for us, and we're going to continue to explore how that can happen. One of the ways in which we've seen some good success in that space has been to declassify information and make sure that the real information is out there and to encourage me and others to amplify the correct information.

● (1155)

Mr. Taleeb Noormohamed: Thank you very much.

I'll share what time I have left.

The Chair: Thank you, Mr. Noormohamed.

[*Translation*]

Ms. Michaud, you have the floor for two and a half minutes.

Ms. Kristina Michaud: Thank you, Mr. Chair.

General Eyre, you said earlier that Canada might have something to fear and that, as a North American country especially, it could be a target.

Doesn't it have more to fear than other countries because of its vast northern border with Russia in the Arctic?

I imagine it does, but could you give us more details on how you are paying attention to the Arctic in your discussions with the United States, for example, and with NATO or NORAD?

In what ways are you paying close attention to what might happen in the Arctic?

Gen Wayne D. Eyre: Thank you for the question.

We must continue to focus on the Arctic to protect our sovereignty, not only today, tomorrow and in the coming weeks, but over the next decade.

The threats to our sovereignty are not very critical right now, but in the next decade they could get worse. So we must invest to protect our capabilities across all domains, whether on land, at sea, in the air, in space or in cyberspace.

With respect to our current operations, I will turn the floor over to the commander of the Canadian Joint Operations Command, Mr. Auchterlonie.

VAdm J.R. Auchterlonie: Thank you.

It's a huge challenge for the Canadian Armed Forces.

[*English*]

In the north there are a number of challenges we face. One of them would be training, as the chief has noted. There are infrastructure challenges in the north. There are capability challenges. The main awareness is a challenge because of the vastness of this.

In terms of specific training, we do conduct training annually in the region. We're seeing ever-increasing training across domains in the north involving the army, the navy and the air force and including our allies and partners around the globe. We conduct an annual series of exercises to make sure we're able to operate in the north, because it is a very hostile environment.

As I said, consolidating that infrastructure, that sustainment, that training and the exercising allows us to have those capabilities in the north to support Canadians.

[*Translation*]

Ms. Kristina Michaud: General Eyre, my next question is not about a threat to Canada specifically, but a threat that could disrupt the world order.

We were discussing China and Russia, but some states on the Security Council and in the United Nations General Assembly abstained from voting on a motion to condemn Russia's annexation of Ukrainian territory.

Do you fear that these states may join forces with countries like Russia and China to further disrupt the world order in the coming years?

Gen Wayne D. Eyre: Thank you for the question.

Yes, certain states, most of them authoritarian and friends or customers of superpowers like Russia and China, are taking the same position as them on the world.

Other countries do not wish to join the West or the authoritarian countries. They want to protect their strategic space and be able to make the decisions they deem necessary to protect their interests.

Ms. Kristina Michaud: Thank you.

● (1200)

The Chair: Thank you, Ms. Michaud.

[*English*]

We will go now to Mr. MacGregor for two and a half minutes.

Take us home.

Mr. Alistair MacGregor: Thank you, Mr. Chair.

I have just one question for CSE. We're talking about cybercrime. I want to focus specifically on the cybercrime that's originating from Russia.

We know that a lot of Canadian companies are very worried about attacks or threats coming their way going public. Such a thing can damage their reputation. It can cause a loss of investor confidence and can really harm their brand.

I know this is a real challenge for your organization, but with respect to the organizations or individuals who are launching these kinds of attacks, could you inform our committee what kind of a profile you're witnessing? Are these loosely affiliated criminal organizations in Russia? What kind of a relationship do they have with the Russian state? Are you witnessing some kind of a coordinated strategy?

I know a lot of that is probably fairly classified, but perhaps you could go into fairly broad terms for this committee.

Ms. Caroline Xavier: Thank you, Mr. Chair, for the question.

As was mentioned, we can't speak to the specifics, but what we can say is that when we become aware of what a cybercriminal's traits look like or what their profile is and that's something we are able to declassify, we definitely want to share that with industry.

That was witnessed in the bulletin we put out in January in particular. We went out and told private industry what Russia might be capable of in the critical infrastructure space just to provide a warning in general about what one should be concerned about, because we know they can operate in a sophisticated manner.

For industry, in relation to hostile states in general and not just Russia in particular, when we understand a profile, such as the one we've been watching for Russia, we give them the necessary advice so they can patch their systems to prevent them from being vulnerable and to really monitor them. That's the other piece that's really important—always keeping an eye on whether things are going as they are supposed to be going.

We offer information sessions, as well as bulletins with advice, on a regular basis. As soon as we are able to provide information that is transparent to the public, we do so.

That goes to the question asked previously about how we really work hard at trying to find ways in which we can declassify the information and make it more public so people are made aware of what the Russians are possibly capable of doing.

Unfortunately, that's about the extent of what I can say.

Mr. Alistair MacGregor: Sure.

I'll just end by again thanking each of you for appearing today. I appreciate it.

The Chair: Thank you, Mr. MacGregor.

That does in fact wrap up our questions.

On behalf of the committee, I would like to thank all our witnesses, the whole panel, for sharing their time with us today. I know you're very busy people, and we do appreciate it. You've been a help, so I thank you.

With that, we will suspend to go in camera. For the members online, you should have been sent a link for the in camera portion.

We will suspend for five minutes.

[*Proceedings continue in camera*]