HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

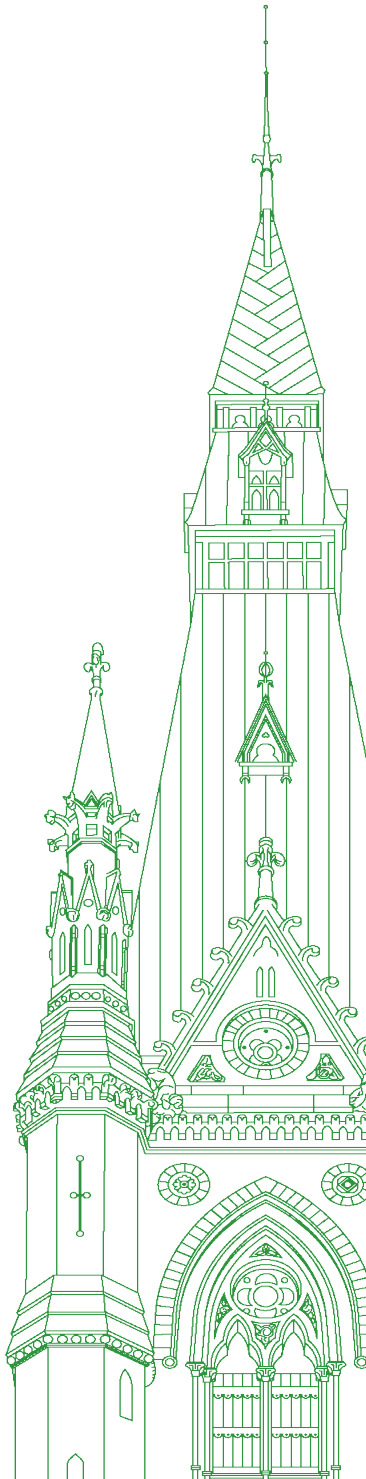
44th PARLIAMENT, 1st SESSION

Standing Committee on National Defence

EVIDENCE

NUMBER 050

Tuesday, February 14, 2023



Chair: The Honourable John McKay

Standing Committee on National Defence

Tuesday, February 14, 2023

● (1530)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): I call this meeting to order.

We have with us today one of our most frequent guests: Mr. Quinn. Welcome again.

We also have Admiral Carosielli with us. Welcome as well.

Both of you have opening five-minute statements.

Before I ask for the opening statements, I will say to colleagues that we are anticipating dealing on Friday with—for want of a better term—the balloon issue. We almost have confirmation from relevant authorities to appear on Friday morning. I say this in the context that today there may be an enthusiasm to ask questions about balloons, which I would encourage members to save until Friday.

We also almost have confirmation with respect to the minister appearing shortly thereafter.

With that, is it Admiral Carosielli or Mr. Quinn who will make the opening statement?

You have five minutes, Mr. Quinn.

Mr. Jonathan Quinn (Director General, Continental Defence Policy, Department of National Defence): Thank you very much, Mr. Chair. I'll have a few opening remarks and then turn the floor over to Admiral Carosielli for a few more.

Thank you very much, Mr. Chair, for the invitation to speak to you today as part of your study on cybersecurity and cyberwarfare.

My name is Jon Quinn. I'm the director general for continental defence policy at the Department of National Defence. My portfolio includes, among other things, cyber-policy.

Cyberspace has become an important domain in the context of increasing global strategic competition. It underpins the systems and infrastructure that not only DND/CAF but all Canadians rely on for their daily work, life and essential services.

Cyber-threats are pervasive, with both state and non-state threat actors increasing their investments in, and development of, their own cyber capabilities. Against this backdrop, our partners and allies are likewise advancing their military cyber capabilities through significant investments and partnerships between military and civilian agencies to ensure they are better postured to defend against threats and to advance their interests.

In tandem with the rise of cyber-threats, we must also consider the opportunities that cyber capabilities offer. They are a strategic tool that the Government of Canada can use to accomplish its foreign affairs, intelligence and defence objectives.

Cyberspace has become another domain of military and national security operations, characterized by constant low-level, below-threshold competition that draws in allies and adversaries alike. The conflict in Ukraine demonstrates that cyber capabilities play a critical role in modern-day warfare.

Canada's defence policy—"Strong, Secure, Engaged"—directs the CAF to assume a more assertive posture in the cyber domain to develop offensive cyber capabilities and employ them against potential adversaries in support of government-authorized military missions.

[*Translation*]

As we develop miliary cyber capabilities and conduct operations, Canada is also providing leadership on the global stage in advancing responsible state behaviour in cyberspace.

Last year, Canada published its statement on the applicability of international law in cyberspace, which articulates our position on this matter.

In addition, CAF cyber operations respect all applicable domestic laws and are subject to proven checks and balances that ensure full oversight and accountability.

[*English*]

DND/CAF is committed to seizing the opportunities of cyberspace in a responsible manner and will continue working toward advancing the ability of our military cyber-forces to conduct cyber-operations independently with allies and other government departments to make Canada safer from cyber-threats.

Thank you. I'll now turn the floor over to Rear Admiral Carosielli.

Rear-Admiral Lou Carosielli (Cyber Force Commander, Canadian Armed Forces, Department of National Defence): Thank you for the invitation, Mr. Chair.

I am Rear Admiral Lou Carosielli, the Canadian Armed Forces cyber force commander. It is a great honour to be here today and have the opportunity to brief you on the outstanding work that our military and civilians do in the defence of Canada in the cyber domain.

Cyberspace is critical when conducting modern military operations and is recognized by Canada and its allies as a domain of military operations, a true war-fighting domain, which I will get into later on.

As such, the CAF relies on the force multiplier effect of technology-enabled communications, intelligence and weapons systems, which must be adequately secured and defended from cyber-threats. The CAF defends its own networks and information systems against cyber-threat actors and supports partners and allies as capacity permits.

Our adversaries have demonstrated sophisticated cyber-espionage and cyber-offence capabilities for use in competition, crisis and conflict.

[*Translation*]

Indeed, potential adversaries are leveraging and developing cyber capabilities to attempt to exploit vulnerabilities in our command, control, communications, computers, intelligence, surveillance, and reconnaissance systems.

In addition to the threat posed by foreign powers, a variety of threat actors with different motivations, such as cybercriminals, hacktivists, terrorist groups, thrill seekers, and insider continue to use increasingly sophisticated means to disrupt our networks.

The CAF cyber forces contribute to international peace and security through cyber threat intelligence sharing with allies and partners and through the conduct of full spectrum cyber operations as authorized by the Government of Canada.

For example, in response to Russian aggression in early 2022, the CAF immediately stood up a cyber task force to help Ukraine bolster its cyber defence capabilities.

● (1535)

[*English*]

Canada provides Ukraine with cybersecurity expertise, cyber-threat intelligence, software tools and technical solutions that allow them to better defend their networks against malicious cyber-activity.

The threat is not limited to Ukraine alone, and therefore, in response to a request for support from Latvia, the Canadian Armed Forces have deployed a persistent cyber task force to Latvia to conduct joint threat hunt operations to assist them in better defending themselves from threats and to demonstrate Canada's commitment to its allies.

Lessons learned from the experience in Latvia in detecting adversarial activities are being applied to better secure our own Canadian national defence's networks and therefore represent a significant return on investment.

Mr. Quinn and I look forward to your questions, Mr. Chair.

The Chair: Thank you.

To start the six-minute round, we have Ms. Kramp-Neuman.

Mrs. Shelby Kramp-Neuman (Hastings—Lennox and Addington, CPC): Thank you.

Thank you for your presence and your contribution to today's committee meeting.

Allow me to indulge for just a moment and be the balloon in the room as it relates specifically to cyber. Were there any cyber officials within the CAF involved or consulted on any cyber risk related to the four objects NORAD shot down in the last two weeks?

RAdm Lou Carosielli: The cyber force is involved in all of these types of discussions with respect to the sharing of intelligence and cyber-related intelligence, so the cyber forces were involved in the conversations, but, as you were briefed yesterday, we are not the leads in these conversations.

Mrs. Shelby Kramp-Neuman: Changing gears, earlier you spoke of "Strong, Secure, Engaged", and within that it states that the regular force will grow by 3,500 up to 71,500 military personnel and that this growth will enable critical investments in important areas such as space and cyber. We understand that this has not happened, so has the recruitment and retention crisis delayed investments into the cyber force?

RAdm Lou Carosielli: As you know, the CAF reconstitution and recruitment is a priority for the Canadian Armed Forces, and we are endeavouring to improve our culture, grow the forces and represent the diversity of Canada and its population. We are making efforts to ensure that recruitment is expedited by ensuring that our systems are digitized, that they are streamlined and that we can process them proficiently.

With respect to cyber forces specifically, in 2017 the creation of cyber-operators was put in place. I am happy to be able to say that within the last three years, we are meeting all of our intake goals for cyber-operators. We have not had to provide any directed cyber-operator recruitment strategies because we have no issues getting the people in the doors. The Canadian Armed Forces are generating cyber-operators, and we provide that for general Canadian needs throughout the country.

Mrs. Shelby Kramp-Neuman: Thank you.

Given the unique nature of the role with the cyber force, has any consideration been given to exempting the cyber force from the universality of service—for example, the fitness?

RAdm Lou Carosielli: There have been discussions on universality of service for cyber-operators and other trades. As you may well be aware, universality of service is something that's very important to the Canadian Armed Forces as it ensures that our members are able to do operations, and cyber-operators do go on operations.

At this point, there hasn't been much talk about exemptions. We do have capabilities of cyber-operators to go become public servants and do cyber operations on the public service side to help the complete team of the Department of National Defence and the Canadian Armed Forces.

● (1540)

Mrs. Shelby Kramp-Neuman: Excellent. Thank you.

Going back to "Strong, Secure, Engaged", it suggests "that the Canadian Armed Forces must take its counter-space capabilities into account as it continues to develop the Canadian defence space program."

Does Canada possess the required technology and personnel to do this today?

RAdm Lou Carosielli: You're asking about counter-space capabilities, ma'am. That's not my portfolio, so I wouldn't be able to respond to that question.

Mrs. Shelby Kramp-Neuman: That's fair enough.

Beyond this, the report outlined the need for the retention of CAF from highly technical domains, such as cyberspace, including the addition of 120 new military intelligence positions and 180 new civilian intelligence positions.

Has this goal been effectively achieved? What are the numbers in this particular domain, if you're familiar with them?

RAdm Lou Carosielli: Your question is specifically with respect to intelligence positions. That is not something I am tracking, ma'am. That is something we can take on notice. We can get back to you in writing.

Mrs. Shelby Kramp-Neuman: That would be appreciated. Perfect. Thank you.

With regard to effectively implementing growth in cybersecurity, what numbers do you feel are effectively needed to assert ourselves in cybersecurity and ensure that we are competitors in this sphere?

RAdm Lou Carosielli: Thank you for the question.

The Canadian Armed Forces is investing imminently in the growth of the cybersecurity force, from both a technical and a personnel perspective.

As I indicated, over the last three years we have been meeting our recruitment intake goals. We will continue to monitor those and grow the capacity and capability as needed to support the Canadian Armed Forces' missions and operations.

Mrs. Shelby Kramp-Neuman: Are you recruiting more from reservists, from the private sector pool or from cyber expertise?

RAdm Lou Carosielli: The one thing about the cyber-operator trade within the Canadian Armed Forces is that we recruit right from the ground level. We have the ability to recruit people out of high school. We have the ability to recruit directly from industry or from other levels of academia, such as universities, etc.

We have all of those avenues available to us, and we grow from the ground up in those trades.

Mrs. Shelby Kramp-Neuman: Do you know how many reserve cyber-operators are currently employed?

RAdm Lou Carosielli: I don't have that number readily available to me, but that is a number we could take on notice and provide to you if needed.

Mrs. Shelby Kramp-Neuman: That would be helpful. Thank you.

In April 2021, the reserve report entitled "Evaluation of the Cyber Forces" said that one of the issues facing the cyber forces was the "lack of planned career progression".

Is this still an issue?

RAdm Lou Carosielli: That is a great question, and it's related to the conversation I've had with respect to recruitment and the creation of the cyber force operators.

With the creation of the cyber force operators, there is a career plan and a progression plan throughout, from entry all the way to retirement.

Mrs. Shelby Kramp-Neuman: Excellent. Thank you.

The Chair: Thank you, Ms. Kramp-Neuman.

Mr. Fisher, you have six minutes, please.

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

Thank you, Mr. Quinn, for being here.

Rear Admiral, thank you. I have to say that I'd like to have your business card, because to be able to say that you're the cyber force commander.... I imagine young children growing up now wanting to some day be the cyber force commander. I think that sounds like the future job description of Canadian children.

Last week a witness at this committee told us that the relationship between the CAF and the CSE is—I'm not quoting verbatim here—basically ad hoc. It's almost non-existent and informal. I was surprised.

Can you tell me if this assessment is accurate? If not, gentlemen, could you please expand on the ways that CSE and CAF operate together on cyber?

RAdm Lou Carosielli: That is a very important question, as the CSE and CAF relationship has been a long-standing relationship, and it is continuing through cyber. CSE and CAF work closely day in and day out.

As you would have heard last week from the CSE discussion, CSE personnel are embedded within the CAF teams and CAF personnel are embedded within the CSE teams. We share information. We share tools. We share intelligence between the two organizations and mutually support each other in operations for CSE, as well as in operations for the Canadian Armed Forces.

Mr. Darren Fisher: Is this a formalized relationship? If it isn't, do you have plans to further improve or formalize this relationship?

I saw Mr. Quinn wanted to start. I apologize if I cut you off there.

Mr. Jonathan Quinn: It's no problem.

I was simply going to add that Admiral Carosielli has outlined the really close operational ties and relationship between DND, CAF and CSE. I was going to add that the close relationship also extends to the policy sphere.

I work extraordinarily closely with my counterparts at CSE on policy questions, and we're fully joined. We collaborate very closely across the board with CSE.

● (1545)

Mr. Darren Fisher: How would this relationship compare with the one we have with our allies?

RAdm Lou Carosielli: Our relationship with our allies is as important as our relationship with CSE. We work very closely with the U.S. Of course, working with the U.S. is important for not only the defence but also the prosperity of North America.

We are very closely aligned with U.S. Cyber Command, so much so that I have a liaison officer embedded within U.S. Cyber Command, as well as numerous personnel who range all the way from cyber-operators to cyber operations planners. This is very important for us. It's an ability for us to have daily conversations. I participate in weekly discussions with U.S. Cyber Command, and that is absolutely critical for us.

We work with U.S. Cyber Command, and our allies within the Five Eyes and NATO, in order to ensure we meet the requirements of our allies and partners, as well as Canada's.

Mr. Darren Fisher: How does the CAF's cyber capability differ from CSE's?

RAdm Lou Carosielli: The CAF and CSE cyber capabilities differ for the principal reason that we do not want to duplicate or have redundant capabilities. CSE has more specialized technical expertise, while the Canadian Armed Forces are typically used for the last mile, in order to ensure that we have intelligence that supports both CSE and the CAF.

Mr. Darren Fisher: You mentioned that we're providing cybersecurity expertise to Ukraine. When and how do the CAF and CSE work together on operations, and under which circumstances would the CAF operate independently?

RAdm Lou Carosielli: The CAF and CSE operate together, depending on what support is required and under whose authorities certain operations are being done.

If a specific military operation is being done under CAF authorities and we need some support in the form of intelligence or tools, we can get that via section 20 of the CSE Act.

Similarly, if CSE is working on something and they need some of our subject matter expertise, there are ways for them to ask for our support. We can provide that and support them under CSE authorities in order to meet the requirements of Canada.

Mr. Darren Fisher: Thank you so much.

I'm going to switch, for a quick second, to cyber capabilities.

When we think about Russia, we certainly always put them in the top four. Perhaps they're even number one when it comes to cyber capabilities. We also thought the same about their military power, until we saw the unlawful war in Ukraine.

Is critical thinking making a comeback? Are their cyber capabilities less overwhelming than we thought? I know they practise hybrid warfare with a bit of disinformation, a bit of cyber capability, and then some traditional combat, as we're seeing in Ukraine.

RAdm Lou Carosielli: It is a very important question and it's very germane to what's going on in Russia and Ukraine.

Russia is still a very serious cyber-actor. As you indicated, the top four are Russia, China, Iran and North Korea.

With respect to your comments on cyberwarfare and more traditional conventional warfare, early in the fall we definitely saw a direct link between cyber events and kinetic activity. Just prior to any bombing of an area, we would see an increase in utilization of servers and IT systems that preceded a target being hit shortly thereafter.

There is a link between their cyber activity and their kinetic, conventional activity.

The Chair: Thank you, Mr. Fisher.

Before we go to Ms. Normandin, can you explain what you mean by “the last mile”?

RAdm Lou Carosielli: Absolutely, Mr. Chair.

We talk about “the last mile” in-country. CSE personnel do not typically go into war zones or conflict zones, so in Canadian missions the last mile is done by Canadian Armed Forces personnel.

The Chair: Thank you.

Madame Normandin, you have six minutes.

[*Translation*]

Ms. Christine Normandin (Saint-Jean, BQ): Thank you very much.

Thank you for being here, gentlemen.

Rear-Admiral Carosielli, I would like you to talk more about cyber operations. You mentioned the case of Ukraine, which was assisted by Canada as a result of attacks. I would like to hear more about how quickly you are able to get government approval to develop cyber projects.

Is there a problem with the time it takes to get the authorization, or is everything fine? Do you have any recommendations to make regarding authorizations?

● (1550)

RAdm Lou Carosielli: Thank you for your question.

Cyber operations by the Canadian Armed Forces may be conducted as long as they receive a mandate to do so during a mission. In such cases, authorizations are given by the Government of Canada or by Cabinet.

Operations are also done under a mandate given by the Communications Security Establishment, the CSE. I believe that, in that case, the approval is given by the Department of National Defence and the Department of Foreign Affairs.

Operations in the course of missions are approved through a very well-established process. As for those coming from the CSE, unfortunately I cannot tell you more.

Ms. Christine Normandin: I would like to know more about the supply of equipment that supports these missions. I am thinking about computer equipment, because you often have to be on the cutting edge of technology.

Does the equipment of the Canadian Armed Forces allow them to conduct successful operations?

Should they have access to more state-of-the-art equipment and should it be supplied to them quicker?

RAdm Lou Carosielli: Just as is the case for other government departments and for the industry, the Canadian Armed Forces and cyber forces have logistical support issues. They had that problem during the COVID-19 pandemic, for example.

With respect to procurement in Canada, this requires a full departmental effort. We work with Public Services and Procurement Canada and Innovation, Science and Economic Development Canada to make sure that our projects move forward efficiently and that we find innovative equipment.

We will certainly continue to reach out to industries so that they can maintain an open and competitive supply chain and be aware of what the future holds.

Ms. Christine Normandin: Thank you very much.

My next question may be more for you, Mr. Quinn, but please, both of you can answer, if you feel like it.

You mentioned international cyberspace policy. From what I understand, that involves accountability for governments to report malicious activity that is happening on their territory. I would like to know how easy it is to obtain this information from other countries, with a particular focus on the private sector.

Is the private sector an issue in other countries as well as here? Because they do not necessarily want to disclose information about attacks that we may have experienced, for example.

Mr. Jonathan Quinn: Thank you for your question.

[*English*]

Absolutely, attribution of cyber-attacks and malicious cyber-activity is a challenge. By their very nature, they tend to be intended to be covert action. Canada's position in the statement I alluded to on our interpretation of international law in the opening remarks is really just to be transparent and hold ourselves to account in Canada and to set a standard for our own behaviour in cyberspace and to lay out our interpretation of law.

There is an active effort when there is a malicious cyber-event in Canada to determine where it came from, but as you rightly mention, it is a challenging space. There's a process led by our colleagues at Global Affairs Canada to attribute publicly, when it's in our interest to do so, when those attacks occur and where they come from and to lay out some details, but it's only when there is really strong, defensible proof of the origin of that attack that a public attribution is made.

[*Translation*]

Ms. Christine Normandin: Thank you.

Are other countries in the world as transparent about the information they give out when they are under attack?

Mr. Jonathan Quinn: Thank you for your question.

[*English*]

I would say that among our allies and like-minded countries there's a concerted effort to be transparent.

Again, I'm slightly outside of my lane—it's a Global Affairs lead—but as I understand it, I think that publication of various states' interpretation of international law as it relates to cyberspace began as a G7 initiative, if I'm not mistaken. Certainly our like-minded allies are committed to it, and there are efforts to encourage other countries to take a similar approach, but as is the case in a lot of issues in this domain, it's a bit of a mixed bag in terms of different countries' adherence to and commitments to transparency in this domain.

● (1555)

The Chair: Thank you, Madame Normandin.

Mr. Bachrach, welcome to the committee.

Mr. Taylor Bachrach (Skeena—Bulkley Valley, NDP): Thank you, Mr. Chair.

Thank you to the committee members for allowing me to sit in on behalf of my colleague Ms. Mathyssen to talk about this very important and interesting matter.

I want to also thank Rear-Admiral Carosielli and Mr. Quinn for their testimony so far.

I want to pick up on a few of the lines of questioning we've heard already. Particularly with the events of the last week, I think there's a growing interest and concern on the part of Canadians when it comes to cybersecurity.

There's also some confusion as to where Canada's cybersecurity strategy is coming from. We have the cyber force that you command, Rear-Admiral. We have the Communications Security Establishment—the CSE—under National Defence. We have CSIS and Shared Services Canada. All of these different organizations work together when it comes to protecting our critical infrastructure from cyber-attacks and preventing vulnerabilities. Which department and decision-maker is at the top when it comes to establishing Canada's strategy on cybersecurity?

Mr. Jonathan Quinn: Mr. Chair, I'll start, and the admiral may have something to add.

It's a great question. It is a complicated space. There are lots of players across government in this area. In terms of the Canadian federal lead for cybersecurity—ensuring the security of government networks, providing assistance to holders of networks in critical infrastructure and that sort of thing— Public Safety has the overall lead.

The Canadian cybersecurity centre was specifically established. It's a CSE body, but it also works under policy set by Public Safety. It has an important role to play there in sharing best practices, providing assistance to Canadian companies, and identifying and mitigating threats.

The Canadian Armed Forces come in. Admiral Carosielli can speak a little bit more to this as well. Unlike other government departments, DND and CAF have the responsibility to defend and secure their own classified networks. That's a bit unique in the federal government.

As I mentioned in my opening remarks, in “Strong, Secure, Engaged”, the government announced its intention to allow the Canadian Armed Forces to conduct offensive cyber-operations as well, in pursuit of Canadian interests. As has been discussed previously, we do those in close partnership with our colleagues at the Communications Security Establishment.

Admiral, did you want to add anything to that?

RAdm Lou Carosielli: Thank you, Jon.

I do want to reiterate that absolutely the Canadian Armed Forces are responsible for defending the networks and IT systems for the Canadian Armed Forces and the Department of National Defence.

That said, we work very closely with our partners within CSE, RCMP, Global Affairs Canada, etc. We work to ensure that we share all of the information that we receive among the partners from intelligence, such as indications of compromises, etc., so that all of us have a good wealth of information and understand what's going on in the other networks. Of course, what's happening in one network could just be a precursor of what's to come on another one.

Mr. Taylor Bachrach: Thank you for that information. Obviously it's a complex answer, and who leads depends on which aspect of cybersecurity we're talking about.

When it comes to the offensive operations, these operations conducted in relation to other countries, who leads those cyber-operations when it comes to strategy?

Mr. Jonathan Quinn: I'll start and then hand it over to the admiral in case he'd like to add something.

The Canadian Armed Forces have the authority to conduct offensive cyber-operations in the context of approved military missions. In those, it's the Canadian Armed Forces leading and conducting offensive cyber-operations under their own authorities, often with assistance from colleagues at the Communications Security Establishment.

There are other offensive cyber-operations that are conducted under CSE authorities, under the CSE act. I think you had previous witnesses from CSE who would be much more qualified than I am to speak in detail about how those operations are conducted. Equally, as the admiral mentioned, when CSE is conducting offensive cyber-operations under the CSE act, they are able to reach over to the Canadian Armed Forces for assistance as required under section 20 of the act.

● (1600)

RAdm Lou Carosielli: I have nothing else to add to that, Jon.

The Chair: You have about one minute.

Mr. Taylor Bachrach: Thank you for that.

I wonder if you could speak a little bit more about the relationship between CAF and the CSE.

You spoke about the integration between your operations. I'm curious the relative size of those cyber-operations. Which of those teams is larger and how you would characterize the size ratio between those two operations?

RAdm Lou Carosielli: I won't be able to give you definitive numbers with respect to the sizes because I don't have the numbers for CSE. That's not within my area of responsibility.

With respect to the importance of the two teams working together, as I had previously indicated, the teams work together day in and day out, every single week. We have embedded personnel in each other's teams so that we understand each others' techniques, tactics and policies and can best support each other to meet our respective operational requirements.

At the various levels, we meet regularly. I meet with my CSE counterparts on a weekly basis in certain meetings and more globally on a monthly or quarterly basis. Those relationships are absolutely essential to ensuring that both organizations have the tools and the capabilities available to each other.

The Chair: Thank you, Mr. Bachrach.

Colleagues, since we only have one witness for the second half, I'm thinking that we should get in a full second round.

With that, Mrs. Gallant, you have five minutes.

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

Is it possible for surveillance balloons to jam or interfere with Canadian cyber-communications or infrastructure in ways not possible by other platforms?

The Chair: I'd encourage members to.... I had said we were going to be dealing with the balloons on Friday.

Mrs. Cheryl Gallant: This is cyber, Mr. Chair.

The Chair: I know.

I'm going to let the question stand, but I would encourage members to stay with the subject matter before us.

Mrs. Cheryl Gallant: Restart the clock.

RAdm Lou Carosielli: Unfortunately, I cannot answer that question, as I don't know what technology is on those high-altitude objects. I would not want to speculate on what the capabilities are or are not.

Mrs. Cheryl Gallant: Can cyber-communications from high altitudes be detected by radio telescopes?

RAdm Lou Carosielli: Radio telescopes are not within my area of expertise. I would not be able to answer that question.

Mrs. Cheryl Gallant: Okay.

You mentioned earlier that there's a buildup or increase in cyber-incidents before a kinetic attack.

In late January, we saw the FAA notification system go down. On the heels of that, we saw Canada's civil aviation NOTAM system go down. Then, within a matter of days, there was this airship going across our atmosphere.

Would that be considered something kinetic, after a lead-up through cyber-operations?

RAdm Lou Carosielli: I can't respond to that question, as I believe the two examples with respect to transport in the U.S. and in Canada were linked to software issues. They were not cyber-related, to the best of my recollection. It was several weeks ago. I have no understanding of the link between that and the high-altitude objects, as I've not read into that file.

● (1605)

Mrs. Cheryl Gallant: If our government can't get over its anathema toward nuclear-powered submarines, we'll have to rely on drones to provide subsurface awareness. Would underwater drones be vulnerable to cyber-attacks?

RAdm Lou Carosielli: The response to that is obviously quite complicated, as it depends on the technologies. I will indicate, as a naval officer and naval engineer, that underwater techniques are some of the most difficult to jam. They're also the most difficult to communicate with because of the medium.

I'll leave my answer at that because, again, it's not my area of expertise and it's not within my area of responsibility at this time.

Mrs. Cheryl Gallant: Okay.

This is for Mr. Quinn as well.

Do the Canadian Armed Forces have any infrastructure or equipment with components from a supply chain that China was involved in? That can be any kind of equipment, not just computer equipment.

Mr. Jonathan Quinn: I am not an expert on the components that go into the Canadian Armed Forces' capabilities. My suspicion is that there probably are some components of the Canadian Armed Forces' capabilities that have components that were manufactured in China, but I'm not an expert on that. I'm sorry.

Mrs. Cheryl Gallant: How does CAF harden its equipment to safeguard from intrusions via the Internet of things?

RAdm Lou Carosielli: As I previously indicated, the Canadian Armed Forces take responsibility for defending our networks and IT systems. We have various means and ways to protect our networks and the systems that are being used. We have levels at different granularity. We start off at perimeter defence, which is the external networks, and it goes all the way down to host space, which is, as an example, a laptop or a computer.

Of course, due to security classifications I cannot go into details in this room on how that's done, but it is something that we do on a daily basis to protect our networks.

Mrs. Cheryl Gallant: Nowadays, even a fridge in the staff room can have Wi-Fi on it. Is there anything done to make sure that the military software isn't connecting to the fridge?

RAdm Lou Carosielli: We definitely do security analyses of all of our systems. That's part of our security and accreditation process. Prior to any system going live, we ensure that we understand how they connect and who they connect to. As indicated, I will not be able to go into greater details on any specific systems, given the classification of this room.

Mrs. Cheryl Gallant: Italy's cybersecurity agency reported servers were compromised in Europe and North America on February 5 of this year. What can you tell the committee about the global ransomware attack that took place that week that affected Canadian servers?

RAdm Lou Carosielli: I don't have any information on the attack that you're referencing.

Mrs. Cheryl Gallant: Is there pressure—

The Chair: I'm sorry, Ms. Gallant; your five minutes are up.

With that, we'll go to Ms. Lambropoulos for five minutes.

Ms. Emmanuella Lambropoulos (Saint-Laurent, Lib.): Thanks, Mr. Chair, and thank you to our witnesses for being here to answer some of our questions today.

Earlier you answered a couple of my colleagues when they asked you about the work that we do with our partners in other countries and you spoke a bit about the relationship we have with the United States and how interconnected you are with them when it comes to all things cyber that affect our countries.

I'm wondering if you can speak to how the Canadian Armed Forces works with all Five Eyes partners. Specifically, how do we learn from the way they do things? Is there a difference? Are they better at certain things than we are, and how are we able to learn from them?

RAdm Lou Carosielli: Absolutely, I did talk about our American interactions earlier, but we do have coordination and discussions with all of our Five Eyes partners, and it's absolutely critical for us to do that. That's done at various levels.

We have several interactions as we go through different conferences together, etc. We also do have liaison officers with some of our other Five Eyes partners so that we can exchange information directly, but, most importantly, the best conversations are through the conduct of exercises. All Five Eyes participate in the exercises, and it gives us an opportunity to exchange best practices and build the relationships that we need so that when something goes wrong, we have points of contacts and easily share information together.

● (1610)

Ms. Emmanuella Lambropoulos: Thank you very much.

My next question is regarding a tweet that was put out by the commander of the Canadian Army last week. It reads, “Our key allies are digitally transforming — and rapidly. Without a similar effort on our part, our very relevance as a reliable ally will be compromised.”

First, what are your thoughts are on that tweet? Second, I'm wondering what specific actions National Defence is taking in order to ensure our continued relevance from a cybersecurity perspective.

RAdm Lou Carosielli: As Mr. Quinn indicated in his opening remarks, our allies are definitely investing in cybersecurity capabilities and improving their capabilities. So is Canada. We take that extremely seriously to be able to ensure that we provide the Government of Canada with the capabilities it requires to meet military missions, as well as missions that the CSE needs to conduct. We are doing that by ensuring that we have the right equipment and the right people. That was with the stand-up of the cyber-operators, and we are growing that trade.

As I indicated, we have met our recruitment numbers within the last three years, but we are on a steadily increasing path to be able to meet all of our capabilities.

Ms. Emmanuella Lambropoulos: Are there any specific actions other than recruitment and personnel that you can talk about here?

RAdm Lou Carosielli: No, not that I would be able to talk about in this room.

Ms. Emmanuella Lambropoulos: How much time do I have left?

The Chair: You have a little under two minutes.

Ms. Emmanuella Lambropoulos: You spoke a lot about the relationship that CAF has with CSE. There is a difference between what we heard last week from CSE and what you're telling us. Is there a reason for that? Would there be a reason for the difference in opinion? Are you both on the same page on that aspect? Can you speak a bit more on it?

RAdm Lou Carosielli: Having read the transcript from the meeting last week and knowing the conversations we've had today, I don't know what differences are being highlighted. If you would like to be specific, I may be able to answer, or you may have to cc that question.

Mr. Jonathan Quinn: Mr. Chair, if I could, I would share Admiral Carosielli's view. Our colleagues from CSE responded in very much the same way that we did. As I understand it, it was perhaps a witness from academia who shared a potentially contradicting view, which was that maybe there wasn't, from the public's view, as much close collaboration between DND, CAF, and CSE as in fact there is.

The Chair: Thank you.

[*Translation*]

Ms. Normandin, you have two and a half minutes.

Ms. Christine Normandin: Thank you very much.

One witness mentioned to us last week that perhaps there should be less focus on analyzing attacks that would, for example, have a large impact on critical infrastructure, because the likelihood of them occurring is low. According to this witness, we should instead focus more on smaller attacks that are likely to be in greater number and do just as much harm. SolarWinds comes to mind, for example.

I'd like you to talk about the training given to members of the military, and even civilians, to make sure that small attacks do not happen, that computer hygiene is good, in a way. Is training included in the basic military qualification? Are there follow-ups afterwards and ongoing training? I would like to hear you about that.

RAdm Lou Carosielli: Thank you for your question.

As I mentioned, the training of cyber operators in the Canadian Armed Forces is progressive. First they learn how to defend against small networks, small attacks. With experience and additional training, they are prepared, in terms of defence, for more sophisticated attacks.

Any information we receive on a network is passed on to all of our partners, including CSE and law enforcement, to make sure that information reaches everyone who needs to know, which means those who will be on our network over the next few days or weeks.

● (1615)

Ms. Christine Normandin: How can we make sure that Canadian Forces employees who are not cyber operators, who work in other areas do not become gateways to cyber attacks?

RAdm Lou Carosielli: Thank you. I had not understood that aspect of your question.

We provide general training to all members of the Canadian Armed Forces and to people in the public services. We just finished safety week. There are formal safety courses that they have to pass. There are also the usual messages sent out to counter phishing. We have to make sure that people know about the need to check where an email comes from before they open any attachments or click on any links.

[*English*]

The Chair: Thank you, Ms. Normandin.

Next we have Mr. Bachrach for two and a half minutes, please.

Mr. Taylor Bachrach: Thank you, Mr. Chair.

I would like to return to my previous line of questioning with regard to the relative size of the cyber force in the CSE's cyber team. Without referencing specific numbers of employees or that kind of thing, Admiral Carosielli, could you speak to the relative size? Which of these operations is larger, and by approximately how much? Does one have twice as many resources as the other?

Could you give the committee some sense of the relative scale of these two operations?

RAdm Lou Carosielli: I would not be able to give you the relative size. As I indicated, I don't know the size of the CSE team, as I'm relatively new. I've been in the chair since the summer, but it's not something that has come up in conversation. I would not be able to answer that question.

Mr. Taylor Bachrach: Okay. That's no problem.

Rear-Admiral, I'm curious. In your work with the cyber force, have you ever come into contact with any programs by DND or CAF or another federal department that involve the collection of data on Canadians?

RAdm Lou Carosielli: The Canadian Armed Forces cyber team works on Canadian missions, Canadian Armed Forces missions, so we would not be collecting any information on Canadians. As you would have heard in testimony from CSE, their mandate does not allow them to collect information on Canadians or personnel on Canadian soil as well.

Mr. Taylor Bachrach: Can I understand that to include publicly available information, such as metadata on social media? The modelling of Canadians' behaviour based on social media activity would not fall within the scope of the cyber force's operations.

RAdm Lou Carosielli: To the best of my understanding, it doesn't fall within the scope. I have not heard of that activity being conducted.

Mr. Taylor Bachrach: Okay.

Mr. Chair, I imagine I only have a few seconds left. I want to ask some questions about privately owned and controlled critical infrastructure.

Last summer, when we saw the Rogers outage, it became evident the federal government had very little role in protecting and recovering the Rogers network.

I'm wondering, Rear-Admiral, if you could touch on the differences between the capabilities of the cyber force and its reach into these privately controlled areas of critical infrastructure. Does the cyber force—?

The Chair: Mr. Bachrach rightly identified that he had very little time left, and he ran it out.

Mr. Taylor Bachrach: Well, it's a great intro to his next opportunity to answer.

The Chair: Yes, yes. That's a warm-up question.

Okay. Mr. Kelly, you have five minutes, please.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thanks.

On Friday, we had testimony from Alexander Rudolph, who said, "The CAF is in no way prepared to face cyberwarfare in the event of a conflict. I further question to what degree they are able to even co-operate and work interchangeably with allies, including the United States."

He went on to say, "At best, Canadian cyber-defence policy can be described as incomplete, ad hoc and inconsistent in strategy and definition...particularly [with] the United States."

That was some pretty strong stuff that we were told on Friday. Is he correct?

RAdm Lou Carosielli: As I indicated earlier, the Canadian Armed Forces are already providing support for Ukraine and Latvia. We are conducting operations with our American and Five Eyes partners as it is, and we continue to conduct exercises with them to improve our capabilities and align and exchange best practices with each other.

● (1620)

Mr. Pat Kelly: Okay.

You talked earlier about embedded personal. Is that just with the United States, or is that with NATO, our Five Eyes allies, Ukraine, Latvia or any other places?

RAdm Lou Carosielli: Yes, we do have embedded personnel with the Americans. We have embedded personnel with the United Kingdom. We have personnel as part of NATO, as you would know, on exchange. We have—

Mr. Pat Kelly: Thanks. That's good.

Mr. Rudolph mentioned that Russia, using wiper malware attacks against Ukraine, has used these attacks to destroy data irretrievably. Are Canada's defences and backup protocols and intentional built-in redundancies adequate to counter a similar attack on Canadian infrastructure?

RAdm Lou Carosielli: As I indicated, one of our primary raisons d'être as the Canadian Armed Forces cyber force is to defend our networks and IT systems. We have protocols to defend and ensure that we have access to our data.

Mr. Pat Kelly: If we were facing an all-out attack in the event of wide conflict involving, say, China over the Taiwan Strait or an expanded conflict with Russia, could Canada withstand these kinds of attacks?

RAdm Lou Carosielli: Canada, working with our allies, would deal with the cyber and conventional efforts put against it.

Mr. Pat Kelly: Is Canada's cybersecurity infrastructure currently ready to handle the F-35's capacity for intelligence and intelligence sharing with allied forces as we acquire these aircraft?

RAdm Lou Carosielli: The F-35 program is definitely one aspect that the cybersecurity force, as well as the CIO of Canada, is working on with the RCAF to ensure that they are capable of receiving the aircraft when they're delivered.

Mr. Pat Kelly: Will we be able to communicate and share intelligence with other allies?

RAdm Lou Carosielli: We currently share intelligence. Now that we have signed the contracts for the F-35, we will increase the number of discussions. The intent is there to ensure that the Royal Canadian Air Force is ready to fully utilize the aircraft when they are delivered.

Mr. Pat Kelly: In your opening remarks—perhaps it was Mr. Quinn—you talked about this area as a new domain of conflict. We've heard a lot about domain awareness and gaps in domain awareness. We've heard quite a bit about this in light of the airspace incursions that have occurred over the last two weeks. We heard a lot about underwater subsurface domain awareness, and the absence of it. What are the gaps that we have in cyber domain awareness? Are we certain of what our risks are? How can we have that level of certainty?

RAdm Lou Carosielli: Obviously, in this room, at this security classification, I would not be able to talk about the gaps and risks, as that is information that would be useful to adversaries.

Mr. Pat Kelly: Okay.

I have a different question to finish it off. Is Canada presently prepared to fend for itself in conflict, if a conflict were to arise or escalate within the cyberspace domain?

RAdm Lou Carosielli: As I have previously indicated, Canada already acts in the cyber domain space. We will continue to co-operate with our allies to defend Canada and our allies as required.

The Chair: Thank you, Mr. Kelly.

You have five minutes, Ms. O'Connell.

Ms. Jennifer O'Connell (Pickering—Uxbridge, Lib.): Thank you, Mr. Chair.

Thank you both for being here.

I have an area of questions that begin where you left off. We heard testimony earlier that made it sound like Canada wasn't prepared in the cyberspace, but in your opening remarks you spoke about how you're helping in Latvia and you're helping in Ukraine. Why would countries want cyber capabilities from countries if they weren't leaders in this space? Is this why Canada is called upon? Is it to help in these areas?

RAdm Lou Carosielli: Absolutely, Canada has definitely taken a very specific posture in supporting our allies, in that we ensure they maintain control of their networks. We provide them with the support that they need, either through engineering tools or throughout an intelligence perspective.

That said, we have capabilities that are improving consistently. There is still a lot that we need to be doing. We are working with our allies so that all of our capabilities are improved. We're ensuring that we're not duplicating each other's efforts.

● (1625)

Ms. Jennifer O'Connell: Following up on that, cyber and cyber-type attacks have been in the news a lot more recently. However, when I was in Estonia, we were talking—this was years and years ago, pre-COVID—about cyber and what happened in Estonia because of Russia. That was long before the invasion of Crimea. Globally, and being in this space, is it fair to say that Canada has been preparing and building its resources?

On the point you just made, Admiral, about the constant changing of the threat and being always ready, even being ready yesterday is going to look very different weeks from now, months from now or years from now. I look back at the Estonian case, when their entire digital infrastructure was successfully hacked by Russia. Was that a wake-up call in Canada back then? How are you continuing to prepare, based on what's happening in other countries and not just what's topical in the media at any given moment?

RAdm Lou Carosielli: I won't be able to talk about what was topical back then because I wasn't involved back then, but definitely since “Strong, Secure, Engaged”, cybersecurity is at the forefront for both the Canadian Armed Forces and the CSE. We have seen that with the CSE's standing up of the Canadian cybersecurity centre and its responsibilities for Canada in general.

The question is related to the threat to all of Canada, not just the Canadian Armed Forces, and that threat is taken seriously. As indicated, there are indications of ransomware or cyber attacks in the media quite regularly, and it is important for us to take those seriously and to prepare. The way the Canadian Armed Forces is doing that is by ensuring that its network defences are up and monitored on a daily basis. We also ensure that we exercise in some very complex scenarios so that we are not just preparing ourselves for yesterday's fight but can understand what's coming in the future. Ties to research and development are important there.

Ms. Jennifer O'Connell: Thank you.

In terms of questions about universality of service and the ability to recruit, the CSE has talked about.... I think it's a known fact that you're competing with, for example, Silicon Valley and things like that in this space. Does universality of service create an impediment for those who might be most trained in this space?

That also includes ensuring diversity in this space. Are you attracting women? Are you attracting people from different backgrounds? Are you attracting people with language skills that would be important, and not just Canada's official languages? Are you also ensuring that people in this space, in cyber, are actually wanting to be part of the CAF and cyber-defence?

RAdm Lou Carosielli: As I indicated earlier, the recruitment of personnel that represent the diversity in Canada is very important to us, not only from the diversity aspect but from an operational aspect, because having multiple languages helps us. As one who speaks three languages, I know it definitely is advantageous, and that is something that we do.

The universality of service is something that we don't control from a trade perspective; it's the Canadian Armed Forces. As I indicated, we are operational personnel, so we have to remain operational. We do have abilities for personnel to join the public service. However, most importantly, one of the biggest attractions of the Canadian Armed Forces and the CSE is the type of work that we can do. There are not many entities in the country or around the world that could do the work that we do and have the authorities that we have, so that is one of the biggest attractions. As someone previously said, when you can have “cyber force” in the title, our population is typically pretty intrigued with it.

The Chair: Thank you, Ms. O'Connell.

● (1630)

Ms. Jennifer O'Connell: Thank you.

The Chair: I think Mr. Fisher is going to be lining up for that business card pretty soon.

Voices: Oh, oh!

The Chair: Before I let you go, I want to ask you a question about the offensive operations.

The CSE has limitations on offensive operations with respect to Canadians, yet we are in a war situation, and it's reasonable to assume that there are people in this country who are supporting the other side, for want of a better term, and who may be of considerable interest to our security. I'm thinking particularly of people on the sanctions list, but others as well.

How does the policy of not conducting offensive operations against Canadians—which I assume can also mean residents—intersect with the security issues that we currently face when we're in a war?

Mr. Jonathan Quinn: Feel free, Admiral, to supplement.

I would say that's a great question. It's certainly a concern, but it's not a Canadian Armed Forces mandate. We have other agencies within the federal family that would play a lead role in, I think, what you're referring to there. CSIS, I think, would jump to mind as a more appropriate entity to tackle that side of the coin.

The Chair: The CSE is part of the Department of National Defence, and it is the one that has the limitation on the policy. I don't want to pursue the question too far, but I think it's in part what Mr. Fisher was getting at in his questioning about the limitations on conducting operations against Canadians.

In deference to my colleagues and my great esteem for you, Mr. Quinn, I won't push the question any further.

With that, colleagues, we're going to suspend.

On behalf of the members, I want to thank you for being here and particularly for your straightforwardness in responding the questions. Thank you again.

With that, we'll suspend.

● (1630)

_____(Pause)_____

● (1635)

The Chair: We're back, colleagues. I hope that was a more vigorous bang of the gavel.

An hon. member: Not really.

Voices: Oh, oh!

The Chair: No? I'm going to have to practise. I'll have to take lessons from Mr. Bezan.

Colleagues, before us again is Mr. Kolga, who is becoming a familiar witness at this committee.

I don't need to tell you about the drill, sir. You have five minutes for your opening statement.

Thank you.

Mr. Marcus Kolga (Senior Fellow, Macdonald-Laurier Institute, As an Individual): Thank you, Mr. Chairman and esteemed members of this committee.

I will focus my remarks today on primarily the information operations aspect of foreign cyberwarfare and the threat it poses to our information environment and our national security. I will talk about the direct impact Russian information warfare is having on our understanding of Putin's invasion of Ukraine and how the Russian government seeks to intimidate and silence Canadian critics of Russia's war.

Last week Alina Kabaeva, the head of a major Russian state media organization and Vladimir Putin's partner, characterized Russian government information operations as a weapon of war. She said that in terms of importance to Russia, information is in no way inferior to a Kalashnikov assault rifle.

Indeed, information warfare has become a primary tool in Russia's hybrid and cyber tool kit over the past decade, and it has directly targeted Canada. Russian disinformation operations targeted Canadians during the pandemic and last year's Ottawa trucker protests. Russian information operations have also targeted Canadian Forces stationed in Latvia. The Russian GRU's Ghostwriter campaign published false stories that claimed Canadian soldiers were spreading COVID in Latvia during the pandemic. Today, the Kremlin's anti-Ukrainian narratives aim to erode public support for Ukraine and to intimidate and dehumanize Canadians of Ukrainian heritage, including those elected to government.

The broad goal of Russian information warfare is to undermine public trust in our democracies and the cohesion of our societies. They do this by weaponizing issues and narratives that have the greatest potential to polarize us. They inject and amplify narratives that exploit both Conservative and Liberal biases and any issues that have the potential to drive wedges between Canadians.

Since Russia's initial invasion of Ukraine in 2014, we have witnessed Russian information operations target both Conservative and Liberal leaders. Prime ministers Harper and Trudeau both, with their governments, have been falsely accused of supporting Ukrainian neo-Nazism by Russian state media and its constellation of proxy platforms for their support of Ukraine's sovereignty and their criticism of the Putin regime.

During the course of Russia's latest invasion of Ukraine, the Kremlin has significantly intensified information operations designed to erode Canadian public support for Ukraine. Among the most successful is the Kremlin's ever-present fearmongering about military escalation, including the possibility of nuclear war. It prevented us from arming Ukraine after Russia invaded Crimea in 2014. It prevented us from first sending shoulder-fired anti-tank missiles, then artillery and then tanks to Ukraine. Today it prevents us from sending fighter jets to Ukraine.

One year ago we were told that Vladimir Putin's three-day special operation was intended to demilitarize and denazify Ukraine's government. This same narrative about Ukrainian support for Nazis is today being aggressively deployed to dehumanize, devalue and discriminate against Canadians of Ukrainian heritage. Such narratives are leading to an alarming rise in threats and violence toward Canadians of Ukrainian heritage and other central and eastern European communities.

Direct intimidation of these communities and critics of the Putin regime is equally concerning. A recent article published by a Russian independent media outlet, Meduza, reports that the Russian embassy in Canada is actively monitoring the social media activities of Russian diaspora members and critics of the Putin regime in Canada. One Russian Canadian was sent a message by the Russian embassy in Ottawa warning him, “We know you, we're watching you, we know what you do.” Last year the Estonian honorary consul in Toronto received a letter threatening to spread anthrax if Estonians continued to support Ukraine. There have been reports of attempted phishing attacks in various diaspora communities as well.

Canadian parliamentarians also face a daily barrage of emails and trolls on social media that seek to influence their decision-making. I've been told by some members that their support for Ukraine is frequently attacked by anonymous social media accounts. Such political intimidation and manipulation, artificial or not, may result in suppression of political and military support for Ukraine.

● (1640)

While I've focused on current Russian threats, Chinese government information operations also represent a significant and persistent threat to our national security and defence.

I'll leave it there for now, and I very much look forward to your questions.

The Chair: Thank you, Mr. Kolga.

Mr. Kelly, you have six minutes.

Mr. Pat Kelly: Thank you for that statement.

When you were here at the committee about a year ago, you talked about how Putin is exploiting democratic nations and trying to drive wedges within western alliances like NATO. Obviously much has changed over this past year. Do you want to update your thoughts on the situation as it relates to our cybersecurity study?

Mr. Marcus Kolga: I think that we knew and that we could have anticipated one year ago that Russia would be intensifying their information operations in the context of the war in Ukraine. We also anticipated that they would try to erode Canadian public support for Ukraine. Those operations have only intensified during the past 12 months.

As someone who observes these operations and these narratives and who monitors and analyzes them on a day-to-day basis, I'm deeply concerned that domestic elements in Canada on the far left and on the far right are both adopting some of these narratives and are using them to create a wedge between us. This is, in effect, legitimizing some of these Russian tactical narratives. It's something I think we should be deeply concerned about in the context of national security.

Mr. Pat Kelly: You've commented that the Canadian Armed Forces have been the target of disinformation campaigns. Can you describe what they look like?

Mr. Marcus Kolga: Absolutely. These campaigns against the Canadian Armed Forces have been ongoing since around 2015, when Prime Minister Harper ordered our forces to Ukraine and to Latvia as part of Operation Unifier and Operation Reassurance. With the operations in Latvia specifically—and this was around 2017 or 2018—they injected narratives into the Russian state-controlled media that were operating in Latvia. There were stories that suggested that our then defence minister, Harjit Sajjan, because of his appearance, was leading a Muslim army to conquer Latvia.

There was another story that featured an image of convicted serial killer Russell Williams in uniform and also in women's lingerie, suggesting that Canada was sending this individual to lead troops to, quote, “homosexualize” Latvia.

Those are two narratives that are quite well known that tried to target Russian-speaking Latvians in order to turn them against our forces. Also, I mentioned—

● (1645)

Mr. Pat Kelly: These were campaigns that were more designed against the civilian population where our forces were deployed as opposed to targeting our forces.

Mr. Marcus Kolga: I'm not so sure. I mean, they were specifically targeting Latvians and Russian speakers in Latvia, but by targeting them, they were also targeting our forces. They were trying to manipulate the opinion of those local Latvians to turn them against our forces.

Mr. Pat Kelly: I've got it. That's just unbelievable stuff, really.

You've talked about the consular offices in the embassy and the diplomatic mission here and the way they intimidate Canadians and the Ukrainian and Russian diasporas in Canada.

In terms of responding to cyber-attacks, including those that may be initiated from Canada through their missions here up to the present, are we still behind our allies in using Magnitsky sanctions, naming names and going after individuals who undermine our security and safety here in Canada?

Mr. Marcus Kolga: Thank you for that question. It's a great question.

I think we could be using our sanctions regime to greater effect to target Russian propagandists, the ones who are promoting these sorts of narratives that target Ukraine and that target Canadian interests as well. We should be ensuring that those sanctions are enforced and that Canadians, either wittingly or unwittingly, are not contributing to the platforms that are used by Russian state media to target us with this disinformation.

I've recently seen a few Canadians appear on RT. This is Russia's state media channel, which has been banned from our public airwaves for almost a year already and placed on our sanctions list. Canadians should not be appearing on that platform, and they should not be supporting Russian weaponized narratives through that platform.

I think we need to be making sure that our sanctions, when it comes to these Russian propaganda platforms, are enforced so that Canadians don't fall prey to them and do not somehow benefit from appearing on them and that the Russians aren't able to use Canadians to weaponize and legitimize their narratives.

The Chair: You have about 15 seconds.

Mr. Pat Kelly: Should Russia be permitted to have any consular representation in Canada or should all their personnel be sent packing?

Mr. Marcus Kolga: Should—

Mr. Pat Kelly: You can give a yes or no with the time you have.

The Chair: I find it interesting that when members are told they have 10 seconds left, they ask a question anyway and see if they can squeeze it out.

If you can squeeze that out in 10 seconds, we'll go with it.

Mr. Marcus Kolga: I question why Russia needs to have nearly 80 diplomats or perhaps more in Canada. That makes no sense to me. What are they doing here?

The Chair: Okay. With that, we're going to go to Mr. May.

Go ahead for six minutes, sir.

Mr. Bryan May (Cambridge, Lib.): Thank you, Mr. Chair.

First of all, thank you for being here with us again to help us with this study.

I know we've just started, but we're increasingly hearing about the risk to critical infrastructure and particularly about how these sectors could be a target of state-sponsored cyber-attacks as a means for adversaries to attack Canada or any of our allies without the use of conventional military means.

In your opinion, what sectors do you see as being under the greatest threat?

● (1650)

Mr. Marcus Kolga: The ones that are under the greatest threat from Russian cyber-operations are obviously those areas of critical infrastructure.

We've seen over the past few months—at least a year—how our health sector has fallen prey to ransomware. A lot of the same organizations that engage in criminal activity such as ransomware are in Russia. If they're allowed to operate in Russia, they do so with the blessing of the Kremlin. I think there is clearly a threat to health and other critical infrastructure from Russian operators and that they've demonstrated very clearly that they will not hesitate to attack critical infrastructure. They've shown us that in Ukraine. There's no reason they would not do that in Canada or among our allied nations.

I suspect that right now their focus is primarily on Ukraine, but once that focus ebbs, I think the threat to Canada will increase as well.

Mr. Bryan May: Is Canada adequately protected, and what should be done to improve protection of those critical infrastructure pieces?

Mr. Marcus Kolga: I can't specifically answer that. I'm more of an expert on disinformation. My understanding is that CSE is taking a closer look, but I can't specifically answer that question.

Mr. Bryan May: Do you have any recommendations on improvements to existing policies or new policies that should be developed in that area?

Mr. Marcus Kolga: I think that education is probably among the best things. Over the past several years, we've seen that it's really basic cyber-hygiene issues that have opened up some of these major institutions to the theat of cyber-attack. It's just about educating and making sure that those individuals who are operating in those organizations—and, I would say, within the government as well—have strong cyber-hygiene skills, including using strong passwords and such. I think that's where we need to start in order to protect the critical infrastructure and other organizations in Canada.

Mr. Bryan May: Should reporting an attack be mandatory?

Mr. Marcus Kolga: That's a very good question. I would say yes, those attacks should be reported. I don't think we should be sweeping them under the rug. That way we'll have a better understanding of where the threat is.

Mr. Bryan May: How can the federal government better collaborate with the provincial and territorial governments to better defend those critical infrastructure pieces?

Mr. Marcus Kolga: Again, I can't answer specifically to the relationship the federal government has right now with the provinces or territories with regard to cybersecurity.

Mr. Bryan May: Am I good for time, sir?

The Chair: You have two minutes left.

Mr. Bryan May: You've spoken a lot about Russia specifically. Are there other actors we should be keenly aware of at this point?

Mr. Marcus Kolga: Absolutely. Russia has been doing this for a very long time, but China is becoming increasingly sophisticated. As far as threats go, I think we need to be keeping a very close eye on what China is doing. They also have, again, these developing capabilities, and I'm certain that Canada will become, and already is, a target of Chinese cyber-activity.

Mr. Bryan May: How are China's efforts different from Russia's?

Mr. Marcus Kolga: Again, I'm not a cyber expert. I can't specifically answer that question. I can't tell you what the differences are between China and Russian threat actors.

Mr. Bryan May: Maybe I can ask this in a different way.

You talked about the misinformation and certain events that have happened in Canada over the last number of years. You talked about education. How do we, on the federal side, push that education piece out without it looking political? The idea that it's coming from one party or another could have that connotation.

Mr. Marcus Kolga: You're absolutely right. Any effort to address foreign disinformation specifically needs to be non-partisan. I've long advocated for a whole-of-society approach and an approach especially within the context of Canada's Parliament and the possible formation of an all-party committee that looks at that disinformation.

● (1655)

Mr. Bryan May: Is any country doing a good job in this area?

Mr. Marcus Kolga: There are lots of countries that are doing a great job in this area. These are frontline countries—Estonia, Latvia, Lithuania. Taiwan is doing an exceptional job in combatting Chinese disinformation. Finland and Sweden as well have adopted early childhood education programs into their curriculum to make sure that all future generations of Swedes and Finns have the cognitive resources necessary to critically assess the information they're consuming.

The Chair: Thank you, Mr. May.

[*Translation*]

Welcome to the committee, Mr. Perron.

You have the floor for six minutes.

Mr. Yves Perron (Berthier—Maskinongé, BQ): Thank you, Mr. Chair, for having me on the committee.

Mr. Kolga, thank you for being with us today.

In your last answer, you mentioned that you already knew about Canada being the target of Chinese cyber attacks.

Can you elaborate on that?

[*English*]

Mr. Marcus Kolga: In terms of the information realm, we know that China has targeted Canada with various different nefarious activities to try to undermine our democracy during the past three elections.

During the last election, my organization, DisinfoWatch, detected Chinese state actors trying to inject narratives through state media into our information space. We also saw various different domestic Chinese language platforms repeating some of those narratives that targeted one specific political party here in Canada.

In terms of foreign disinformation, China has very much targeted Canada over the past two to three years at least.

[*Translation*]

Mr. Yves Perron: Thank you very much.

There are even rumours of funding for some candidates. I do not suppose you have any data on that.

[*English*]

Mr. Marcus Kolga: No, unfortunately I don't have data on which candidates received funding and which received support from the Chinese government.

[*Translation*]

Mr. Yves Perron: Let us go back to Canada's preparedness to defend itself from future cyber attacks.

How would you characterize Canada's ability to defend itself in a hybrid war, that is, a war where an attack could be partly kinetic, but also include a large cyber attack? Is Canada equipped to deal with that? Is it sufficiently developed independently of its allies?

For example, Canada could lose sporadically the defence capability of the United States. Would Canada be helpless in that case?

I know this is a big question.

[*English*]

Mr. Marcus Kolga: When we're talking about hybrid warfare, cyber and the information realm, Canada might have some challenges in defending itself.

From my understanding, there were capabilities that were being developed by the CAF to defend against psychological warfare and information operations. That effort was terminated in 2020, from my understanding, due to some media reports that suggested that the Canadian Armed Forces were preparing to use psychological warfare and information operations against Canadians. I'm not sure there was much evidence to support that.

Since then, it doesn't appear that the Canadian Armed Forces have continued or started developing those efforts to defend our forces against the sorts of information operations I mentioned earlier, including the Russian one, the GRU Ghostwriter campaign that targeted our forces in Latvia by suggesting that they were spreading COVID in that country. From my understanding, the Canadian Armed Forces do not have the capabilities to defend against those sorts of information attacks right now.

[*Translation*]

Mr. Yves Perron: The question was asked earlier, however, do you have a specific recommendation on this aspect?

What steps should be taken?

I know that in 2020, a doubt was raised and these operations stopped. However, there is a balance to be struck between the privacy of citizens and national protection. It is not easy.

● (1700)

[*English*]

Mr. Marcus Kolga: Again, that's a very good question.

Having read some of the information about those capabilities when they were being developed, I know the Canadian Armed Forces take information and psychological warfare very seriously. As I mentioned earlier, Vladimir Putin's partner, Alina Kabaeva, has mentioned that information is like a Kalashnikov. I think that our armed forces understand that as well.

There was never any suggestion that information operations would be used against Canadian citizens. They were only going to be used where there were active operations. The fact that our armed forces don't have that capability right now is concerning for someone like me who does monitor and analyze foreign information operations.

[*Translation*]

Mr. Yves Perron: Thank you very much.

What do you know about quantum computing, which is reportedly developing quite significantly and could revolutionize hacking capabilities from the outside?

Do you consider us to be lax in this regard?

Is there anything going on in Canada? Are we preparing for these potential attacks?

[*English*]

Mr. Marcus Kolga: I find that any future technologies are a deep concern, especially when it comes to the information realm. AI is developing very quickly. The speed with which our foreign adversaries can put out information and disinformation is going to be quite alarming. I'm not sure we're prepared to address that growing threat.

The other threat that is growing and will become problematic in the coming years is the creation of deepfakes. These are fake videos, fake images and fake audios that are increasingly created by AI. It will take an image of President Biden, for example, and make it seem as though he is saying something that he's not actually saying. The technology used to create these videos is becoming terrifyingly accurate.

Again, I'm not sure we're prepared to deal with the emergence of these deepfakes.

[*Translation*]

The Chair: Thank you, Mr. Perron.

[*English*]

Next we have Mr. Bachrach for six minutes.

Mr. Taylor Bachrach: Thank you, Mr. Chair, and thank you, Mr. Kolga, for your testimony so far.

You've written about the impact of disinformation on several different events, including the pandemic, the convoy and the war in Ukraine. I'm curious about all of those, perhaps starting with the pandemic.

Could you speak a bit as to whether, in your view, these attempts at disinformation by foreign actors had an impact specifically on the political discourse around the pandemic? Did you see that those efforts had some effect in the way that the political discourse in Canada evolved over the course of the last three years?

Mr. Marcus Kolga: Thank you for that question—

The Chair: I'm sorry. Hang on for a second.

It's a good question and it's an interesting question, but we're a straying a bit from the study. I'm going to allow it, but could you somehow or other tie it back into our security situation here?

Mr. Marcus Kolga: Thank you, Mr. Chair.

Foreign information operations—cyber-operations—in that context were absolutely targeting Canada during the pandemic. We had anticipated this already in 2020, when the pandemic was just starting. Our allies in the EU at the eastern StratCom also anticipated that foreign actors, including Russia, would use disinformation and online platforms, etc., to intensify the effects of the pandemic.

In the summer of 2020, we saw platforms such as RT and other Russian state media platforms legitimizing anti-vaccination movements and anti-lockdown movements in Germany. We further saw them giving a platform to and amplifying similar movements in North America, including right here in Canada. One extremely aggressive anti-lockdown organization that had an account on Twitter had spent the year or two before the Russian invasion of Ukraine tweeting anti-vaccination and anti-lockdown narratives. On February 24, those narratives switched to anti-Ukranian narratives. In fact, they were advancing and amplifying narratives that were promoted by the Russian embassy right here in Canada, and they continued to do so several hundred times between February and March.

We saw a fairly clear and distinct correlation between the two. We definitely saw Russian state actors amplifying those narratives during COVID.

● (1705)

Mr. Taylor Bachrach: Thank you, Mr. Kolga.

With reference to the chair's previous comments, I'm curious to know if you feel that disinformation is a form of cybersecurity threat. Perhaps you could comment on whether the cybersecurity establishment in Canada recognizes it as such.

Mr. Marcus Kolga: Well, absolutely. I mean, disinformation is often a form of digital communication. It's used by our adversaries, as I mentioned earlier, to destabilize our democracy, to turn each of us one against another. They do this using various different platforms of social media.

I mentioned as well that email is used to do that, and then, of course, in the cyber realm, we see doxing and phishing attempts to try to lure individuals to provide data and such and we see individuals opening up their computers to cyber-attacks or cyber-hackers to steal data and such. We saw that happen in 2016, of course, when Russian hackers went into the Democratic Party servers, stole information and exposed it. There is a definite blurred line between cyber-activity and disinformation. I think they very much belong in the same realm.

Mr. Taylor Bachrach: Thank you for that.

Continuing along that same line, you've mentioned disinformation attempts related to the pandemic, related to the convoy and related to the war in Ukraine. You also mentioned that Canadian parliamentarians have been the target of some of this disinformation.

In your view, have Canadian parliamentarians been shown to be vulnerable to these disinformation attacks? Could you provide some examples of how that might be the case?

Mr. Marcus Kolga: There have been clear instances in which provincial parliamentarians in Ontario fell victim to foreign information operations during the pandemic. There was an Ontario MPP who supported anti-vaccination and anti-lockdown views, which is perfectly normal in Canada, but the Russian government, the Russian state media, recognized this and asked him onto RT. He went onto RT, which helped to provide a global platform for his views. After he gave an interview on RT, he tweeted out to all of his followers that they should not be following mainstream media but should follow RT because Russian state media were the only trustworthy ones out there—

The Chair: We're going to have to—

Mr. Marcus Kolga: —so yes, there are definitely parliamentarians who've been—

The Chair: We'll have to leave the answer there.

Again, colleagues, we're in the same situation we are every time: We have 20 minutes left and 25 minutes' worth of questions. I'll take a minute off everybody's time, and then we'll start with Ms. Kramp-Neuman.

Mrs. Shelby Kramp-Neuman: Thank you.

Mr. Kolga, thank you for your interesting and thought-provoking testimony so far.

I'd like to complement what my colleague was suggesting earlier in the conversation you had with regard to our forces being targeted regularly. How can we better train CAF personnel to ensure that they are equipped to handle the challenges of cognitive warfare and cybersecurity?

● (1710)

Mr. Marcus Kolga: Thank you. That's a very good question.

I don't think it's just our forces. I think there needs to be broader awareness in general for all Canadians so that they can recognize information operations and defend themselves against them. In the context of our forces, again, I think we need to develop that capability to directly address those sorts of narratives that I mentioned earlier and challenge them and push back on them.

When it comes to a conflict situation, as we've seen in Ukraine, Russia doesn't hesitate. Cognitive warfare is an extremely important tool in their tool kit, and we need to make sure that we have the capabilities to address those threats and to go on the offensive against our adversaries when they engage in that sort of warfare.

Mrs. Shelby Kramp-Neuman: Thank you.

In your comments on February 16, 2022, almost a year ago, you indicated that cyber will be the primary battlefield of the 21st century and that Canada is in need of resources and knowledge to confront those challenges. I think you had a crystal ball.

A year later, has Canada taken this advice and prepared itself to deal with these threats?

Mr. Marcus Kolga: I think that Canada had, and all of our allies had, a huge wake-up call on February 24 of last year. I think that most of us, including Canada, rapidly developed our capabilities to try to address this threat. I think now, finally, our government and certainly our forces and those of our allies are taking the Russian threat seriously.

Are we prepared? Are we better prepared now? I would say that we are. Are we completely prepared? Probably not.

Mrs. Shelby Kramp-Neuman: Agreed. The state of urgency has definitely been noted, but it's time to continue on the path that we're on.

Furthermore, you've written several times on the significance of the energy industry infrastructure for the war in Russia. You indicated that Canada has fallen victim to Putin's energy blackmail and deception.

How could cyber-attacks in the energy industry play a role in succeeding or failing in this war with Russia? As it stands, how vulnerable is Canada's energy industry to an attack?

Mr. Marcus Kolga: I don't have an assessment of how well defended our energy industry is. I think that each company probably has its own protocols.

I think we would be wise as a nation to try to create some sort of standards for cybersecurity for various different industries and such so that there would be guidelines for those companies, whether it's the oil patch or pipeline companies, so that they have an understanding of the minimums that they need to meet in order to secure themselves. I don't think we're there yet, but it's a policy that we should be looking at.

Mrs. Shelby Kramp-Neuman: As my last question with the time I'm provided, do you think that enough has been done to protect civilian infrastructure from potential outages?

Mr. Marcus Kolga: We can always do more. The threat is always evolving, and we need to make sure that we're keeping up with it. My understanding is that the capabilities of CSE are growing, but we need to make sure that in those specific organizations that control the various different parts of the infrastructure, the people there are well trained and have an understanding of how to defend against these cyber-attacks. I'm not sure that we're there yet.

The Chair: Thank you, Ms. Kramp-Neuman.

Ms. O'Connell, you have four minutes.

Ms. Jennifer O'Connell: Thank you, Mr. Chair.

Thank you, Mr. Kolga, for being here. I have a few questions.

In terms of plans and capabilities for CAF to defend against disinformation targeting our troops, you said that they don't have them. Is that really a fair assessment, though? Why would we post online, for example, or why would CAF share what our plans are for future attacks and things like that for our adversaries to know?

Mr. Marcus Kolga: Thank you for the question.

I think CAF intelligence command is doing a great job of posting and debunking various different Russian disinformation narratives right now. In terms of public affairs, that capability certainly is there. However, when it comes to our forces tactically, if they were engaged in a conflict, the capability that was being developed up until 2020 is no longer there.

In the CAF right now, I don't know if there is discussion about reconstituting or developing that capability. When our forces are in a conflict right now, when it comes to psychological warfare and information operations, they don't have the capability to defend themselves or go on the offensive against an adversary.

● (1715)

Ms. Jennifer O'Connell: Is that clarification specifically about when they're in conflict?

Mr. Marcus Kolga: Yes.

Ms. Jennifer O'Connell: Okay.

In terms of disinformation or misinformation, you talked about examples related to COVID-19 and the anti-vaccine movements. I think it was in response to a question about parliamentarians being vulnerable, and you gave a good example of someone actually promoting Russian TV. Future information would then be sent to a new group of individuals who probably never would have stumbled upon RT.

I've noticed this too in the U.S. Lots of American comedians are showcasing, in a way that's meant to be satirical, some of these beliefs in fake interviews and by asking questions. I've seen ones in which people think President Trump is still the president, or there are two militaries—one that the president controls and one that he doesn't. It's sad to watch, actually, because these people really believe these things.

Knowing how that disinformation starts and then takes on a life of its own, is this not the point of foreign adversaries? It's not really about vaccines or COVID-19 conspiracies or lockdowns; it's really about building mistrust in government. When I use that comedic example, it's really about saying we no longer trust our leaders. We don't even believe the outcome of elections. It's really about breaking down democratic institutions.

Mr. Marcus Kolga: Thank you again for, I think, that question.

The problem comes in when our foreign adversaries take those issues that are polarizing us and weaponize them against us. As Canadians, we have the right to freedom of expression, so if we don't like our government, we're absolutely free to say that we don't like it. If we don't like the vaccine policy and if we don't want to be vaccinated, we're free to make that choice as well.

When a foreign adversary, Russian state media, tells us that the vaccine is going to kill us, they're not free to do that. That costs us money and that could cost us lives, and that's where we need to stand up and push back.

The Chair: Thank you, Ms. O'Connell. I'm sorry.

[*Translation*]

Mr. Perron, you have one minute.

Mr. Yves Perron: Thank you, Mr. Chair.

Mr. Kolga, when my previous time ended, we were talking about quantum computing and you were telling me that we were not prepared. You also talked about deepfakes, and you said that, again, we were not prepared.

I would like to talk to you about the left-of-launch actions. I do not know if you are aware of this rumour. It seems that there would be capabilities to hack the launch of missiles. This has reportedly already been tested.

What should we do to prepare for these threats?

You have an opportunity to make a recommendation to the government so that we are better prepared.

[*English*]

Mr. Marcus Kolga: In order to be better prepared, we need to make sure that we have the resources available to train experts in this field—to make sure that programmers are able to identify where these threats are and recognize them when they do target our military systems and our critical infrastructure. That's the only way to defend ourselves against it.

[*Translation*]

Mr. Yves Perron: Would it be appropriate to create an all-party committee on misinformation in Canada?

● (1720)

[*English*]

Mr. Marcus Kolga: Absolutely. I think a committee for cyberthreats and, I would argue, one for disinformation as well should be created. An all-party committee much like the national security and intelligence committee could be created, one that is non-partisan and that can meet on a regular basis with regard to disinformation. Disinformation narratives could be brought to light there and discussed. All parties can either agree or disagree that these are foreign disinformation narratives and let members of their caucus know about them.

The Chair: Thank you.

You have one minute, Mr. Bachrach.

Mr. Taylor Bachrach: Thank you, Mr. Chair.

Mr. Kolga, you've made the case that the national cybersecurity establishment should have a strategy for combatting disinformation by foreign actors. Should our security agencies also be equally concerned about dangerous disinformation coming from domestic sources?

Mr. Marcus Kolga: Absolutely, and I believe that our intelligence agencies do keep an eye out. Specifically, CSIS does monitor domestic extremism and such, as does the RCMP. That definitely is happening, but I don't think we're doing a very good job or an effective job of monitoring how foreign actors amplify and further intensify the radicalization within some of these organizations, because this is happening. These sorts of narratives are emerging from state platforms and also the constellation of proxies. Russian proxies at least are helping to pour fuel onto this radicalization and extremism that's happening right now.

The Chair: Thank you, Mr. Bachrach. I apologize; my colleagues have been criticizing me for mispronouncing your name for the last two hours.

Voices: Oh, oh!

Mr. Taylor Bachrach: That's no problem, Mr. Chair. I answer to just about anything.

The Chair: Well, I'm not inviting you to supper, so there you are.

Voices: Oh, oh!

The Chair: These bad jokes get embarrassing, don't they?

Go ahead, Ms. Gallant.

Mrs. Cheryl Gallant: Thank you.

How does China capitalize off Russian propaganda disinformation for its own purposes?

Mr. Marcus Kolga: That's an excellent question.

What we're seeing is a close alignment right now of Chinese disinformation and Russian disinformation. They support each other. The Chinese information ecosystem, so to speak—the media ecosystem—is absolutely parroting Russian disinformation when it comes to Ukraine and other subjects right now. Russian state media does the same with China. They're in lockstep right now and supporting each other.

Mrs. Cheryl Gallant: We have some superior cyberwarriors, but they don't want to deploy to a theatre of war. How necessary is it that our cyberwarriors be deployable?

Mr. Marcus Kolga: Well, in terms of cyberwarriors, I would also say that in the realm of disinformation, it's really important that we have offensive capabilities and that we push back. I think we've spent the past several years trying to figure out what this threat looks like and how to defend ourselves. If we're constantly on the defence, we're not going to stop Russia or China.

Ukraine has demonstrated as well that the only way to stop Putin's aggression is by stopping him. That means going on the offensive and pushing back, as Ukraine is doing right now with Russia's forces. We need to do the same in the cyber realm with disinformation. Pushing back and going on the offensive will stop Vladimir Putin and other authoritarians like him.

Mrs. Cheryl Gallant: Can we do that, though, without enlisting into the military the people who are very good at doing exactly what you just described?

Mr. Marcus Kolga: Well, I think some of these people get good at what they're doing by not necessarily always.... It's a good question. I would say that at least in the information realm, I think we can train the right people. We don't have to go and find these actors who are operating with others, whether it's criminal organizations or foreign adversaries. We can train them right here at home.

Mrs. Cheryl Gallant: Okay.

One of the narratives being propagated is that high-ranking Ukrainian officials are using the international contributions toward the war for their own purposes. How does one expose that disinformation so that they're not countering the efforts of Canadian parliamentarians who are trying to do the right thing to protect democracy all over the world?

● (1725)

Mr. Marcus Kolga: Thank you for that question.

This is one of the top narratives that Russia is trying to promote in the west to try to erode our support for Ukraine. Facts and the truth are what will debunk that narrative. The fact that Ukraine is fighting corruption in Ukraine....

All of the military support we're sending them is being closely tracked and monitored. These narratives that suggest some of this equipment is being sold on the black market are completely false, and there is proof of that. The problem is that Russian state media will ignore the facts. They don't report the truth, and they will continue to report lies like that. All we can do is make sure that our media do have the facts; that our elected officials, when they speak about supporting Ukraine, have the facts; and that those facts are promoted properly in this country and Canadians are aware of them.

The Chair: Thank you, Ms. Gallant.

Mr. Fisher, you have the final four minutes.

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

Thank you, Mr. Kolga.

Some of the topics are starting to blur a little bit, and some of the same questions are being asked by the same people.

I think you were here during the first hour in the back of the room. Were you?

Mr. Marcus Kolga: Yes, I was.

Mr. Darren Fisher: I asked this question at a previous meeting as well. Today's response from the rear admiral was considerably different from the response I got last week. I want to ask you for your perspective.

The world generally believed that Russia was a cyber-power, and arguably they are. We think of them as being the best at misinformation, disinformation and cyberwarfare. I think we also felt as a world generally that they were a military superpower as well. Over the last year, I think some of that stuff has been debunked.

I'm curious about your thoughts on their philosophy of hybrid warfare, which is a little bit of cyber and then throw in a bomb. I know this was touched on a little bit with some of the other members, but I'm interested in your thoughts on whether they are underwhelming in the cyber world and the military world, or whether you think that's just the wrong perspective. I'm interested in your thoughts on that.

Mr. Marcus Kolga: I think Russia has failed in many ways over the past 12 months.

Certainly, militarily, as you mentioned, they are clearly not the force we feared they would be. With regard to disinformation, they have certainly been losing the fight against President Zelenskyy and his government, who have done an incredible job of countering many of those Russian narratives. Russian information operations and cyber-operations as well were targeting the cohesion of our allies and our alliances. The fact that we are more aligned than ever before on Ukraine, the fact that we continue to support Ukraine.... We are sending them tanks. We will, hopefully, start sending them F-18s in the future. I think all of this demonstrates that in those two realms, Russia is not the adversary we feared it was.

With regard to cyber, I think we've seen a lull in activity. Russia has really focused its efforts on Ukraine specifically. I'm deeply concerned that once this war ends—and it will end—and when Russia is able to regroup in the cyber realm and in the information realm, but primarily in the cyber realm, and is able to focus on our European allies and on us, we may yet be unprepared. I don't think we can really assess Russia's cyber capabilities right now, because they've changed and their focus has shifted, so I think it remains to be seen.

As I said, when this war ends, I think we're going to see Putin unleash those cyberwarriors against us. Hopefully, we will be prepared.

● (1730)

Mr. Darren Fisher: You gave a couple of examples that were probably meant to be a little bit silly. You talked about sending people in dresses to—I don't know what you were talking about—Estonia and Latvia. Can you give us some examples?

I can remember that one time when I was flipping through Facebook, I saw that somebody on my Facebook page had shared this incredible fake newscast that the Americans had just attacked the Russians. It looked so real.

I wonder if you could give us a couple of examples of some of the things they've done that might have been worthy of the fear that we might have allowed them—

The Chair: Answer very briefly, please.

Mr. Marcus Kolga: Those two examples that I gave you did have a significant impact on Russian speakers in Latvia. That is of serious concern. In 2020, the GRU Ghostwriter campaign that suggested that Canadian troops had caught COVID when they were at home and were spreading it to Latvians made national headlines in Latvia. It was a complete fabrication, but it was picked up.

Stories like this may sound small and insignificant and they may sound silly, but they do have an impact.

The Chair: That will conclude our session today.

On behalf of the committee, I want to thank Mr. Kolga for his always lucid testimony. We appreciate your attendance here.

With that, we are adjourned.