HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

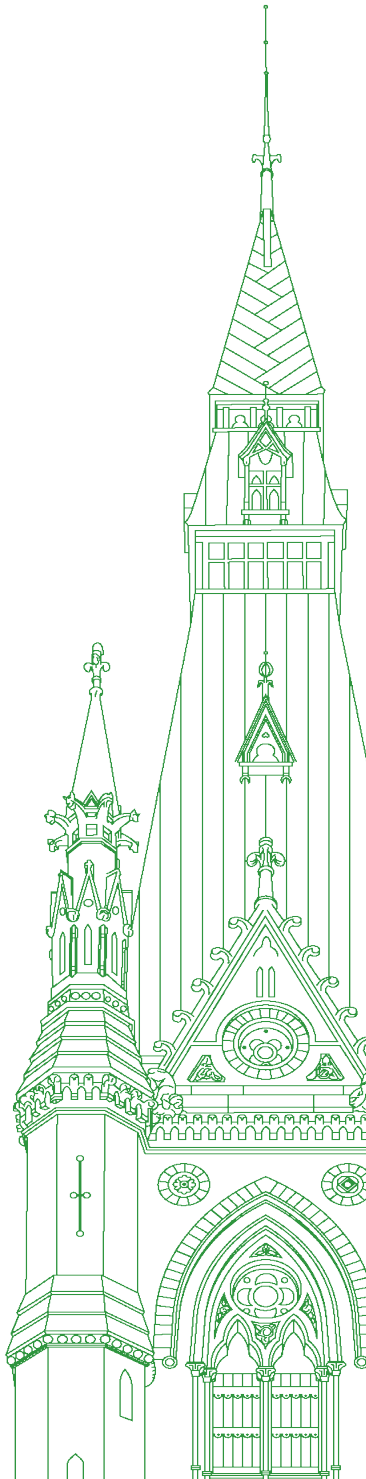
44th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 017

Tuesday, April 5, 2022



Chair: The Honourable Jim Carr

Standing Committee on Public Safety and National Security

Tuesday, April 5, 2022

● (1105)

[*English*]

The Chair (Hon. Jim Carr (Winnipeg South Centre, Lib.)): Good morning, everybody.

I call this meeting to order. Welcome to meeting number 17 of the House of Commons Standing Committee on Public Safety and National Security.

I will start by acknowledging that I am meeting here on Treaty 1 territory in the home of the Métis nation.

Today's meeting is taking place in a hybrid format pursuant to the House order of November 25, 2021. Members are attending in person in the room and remotely using the Zoom application. Per the directive of the Board of Internal Economy on March 10, 2022, all those attending the meeting in person must wear a mask except for members who are at their place during the proceedings.

Members and witnesses participating virtually may speak in the official language of their choice. You have the choice at the bottom of your screen of either the floor, English or French.

The committee clerk will advise the chair on whose hands are up to the best of his ability, and we will do the best we can to maintain a consolidated order of speaking for all members whether they are participating virtually or in person.

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

With us today by video conference as individuals are Dr. James Fergusson, deputy director, centre for defence and security studies at the University of Manitoba; Dr. Robert Huebert, associate professor, department of political science, University of Calgary; and Dr. Veronica Kitchen, associate professor, department of political science, University of Waterloo.

Up to five minutes will be given for opening remarks, after which we will proceed with rounds of questions.

Welcome to all of you.

I now invite Dr. Fergusson to make an opening statement of up to five minutes.

Sir, the floor is yours.

Dr. James Fergusson (Deputy Director, Centre for Defence and Security Studies, University of Manitoba, As an Individual): Thank you, and thank you for the invitation.

I want to begin my brief comments with a concern I have. I think it's very important that the committee and the government do not overreact, if not go into panic, with regard to existing vulnerabilities both in the cyberworld and defence world of Canada from Russian capabilities.

Certainly the war has heightened the attention, but as I would argue to you, these vulnerabilities have been here for a long time now. We need to recognize, given the adversarial relationship that exists between Russia and Canada, Russia and the west, that this is not a new Cold War. There are other issues and other threats out there which have to be taken into account in trying to respond to the Russian side of this equation.

In terms of the cyberworld, what I would point out in my central concerns is primarily the question of whether the government and particularly our relationship with the United States as a function of economic integration and the integration of critical infrastructure is structured properly to deal with the vulnerabilities that exist. There is no central agency as in the defence world, in this case NORAD, to coordinate responses to potential Russian cyber-attacks, whether they are for espionage reasons or attempts to undermine or sabotage critical infrastructure. I think this is an important issue. NORAD for some time has sought to be, or believed that it could be, responsible for the cybersecurity world, cyber-defence in North America. I still argue that this is very problematic.

Some restructuring is necessary, I believe, particularly in the relationship with the United States, but the cyberworld is a unique world from the defence world, not least of all because the critical infrastructure is by and large in the hands of the private sector. Private sector issues, of course corporate issues, with regard to threats have different dynamics and different concerns on the corporate side relative to government. This is not just the federal government, but also includes the provincial government.

In terms of disinformation, I'm not one who believes that Russian disinformation, Chinese disinformation or anyone's disinformation campaigns really have much of an effect at all. I think that's highly overblown and exaggerated. Espionage has been around and that is a concern, but that's a concern to ensure that government and military cyber-networks are closed and secure.

Canada has no capacity except to deny access as best it can across the spectrum. We have no ability to retaliate in terms of a cyber retaliation, so I think we need to think about those things in particular.

In the physical world, the defence world, I would point out to the committee that for a long time, Russian strategic doctrine has been one of first use of nuclear weapons. The Russians have developed a new set of capabilities beyond their ballistic missile capacities. These are in the world of longer and longer range cruise missiles and the future nuclear-powered cruise missiles and hypersonic vehicles, all of which are nuclear and conventional capable. It's hard for defence, of course, to know what is coming, if it's coming. We have significant gaps and vulnerabilities which have existed for over a decade in terms of the ability of NORAD, and as a result Canada, to be able to detect these threats, to track them, to discriminate, and then to be able to cue interception capabilities.

Interceptors are another issue. The F-35 is a step forward, but there's a broad need to rethink the way Canada in conjunction with the United States via NORAD undertakes and modernizes North American defence to reduce our vulnerability and to be able to deter potential Russian threats. This will affect the way Canada and the United States—North America—respond to threats that originate overseas as we see today in Ukraine.

I shall leave it there. I look forward to your questions.

● (1110)

The Chair: Thank you very much.

I would now like to ask Dr. Huebert to make an opening comment of up to five minutes.

Sir, the floor is yours.

Dr. Robert Huebert (Associate Professor, Department of Political Science, University of Calgary, As an Individual): Thank you very much. I'm very honoured to be asked here to contribute to this very important topic.

In the five minutes, I have five points.

The first point is that Russia is an existential threat to Canada and it is growing.

The second point is that we have either ignored or appeased Russia since the signs of the type threat that we are dealing with, which has been developing since 2008. We are not talking about a threat that developed in February 2022. We're not talking about one that developed in March 2014. It is one that clearly has been indicating to us what it means to Canada and what it ultimately means to Canadian security.

This threat comes from Putin and the administration of Putin seeing an existential threat to his regime by the activities and the existence of NATO. NATO, of course, is the alliance in which Canada is a participant, along with NORAD, which means that any conflict that involves NATO will involve Canada.

Now, where does this threat come from? There are two major elements that drive the Russian threat to Canada. The first one is that we have seen Putin, even on his first days as acting president in 1999, move to reconsolidate the Russian empire. What do I mean by this? One of the very first steps he took as acting president was to intensify the war in Chechnya, which the Russians had come close to losing in 1994. They were subsequently successful in being able to put down the moves for secession. We see a series of military moves to expand Russian control starting with Chechnya and Georgia, and then when the Ukrainian war actually starts, which was 2014. We see that there is this effort.

The second part is the protection of the regime. Once again, we have tended to ignore the threat, but we see the manner in which the Russian regime has moved against any opposition within and even those opposition that are physically outside of Russia.

Perhaps the most important element of this threat that Canada has in fact been ignoring is the Russian way of war and its willingness to use that way of war to achieve its policy objectives, which places it on a direct collision course with NATO.

When we talk about Russia, there are at least three levels to their multi-domain processes of warfare.

The first one, which Dr. Fergusson also touched on, is the existence of the Russian commitment to use tactical nuclear war. We have tended to pretend, after the initiations under the Gorbachev regime of significant arms control movements, that this was a thing of the past. The reality is that in Russian doctrine, Russian force projection and Russian force delivery, we see that they are modernizing their tactical capability. We see the threat that Putin gives today to utilize nuclear weapons. This illustrates and is further amplified by the Russian commitment to also learn how to blind NATO countries.

We have seen the demonstration effect when the Russians demonstrated how they can shoot down one of their own satellites with their missile capability. In February of this year, they also demonstrated how they can cut cables and, hence, communications. All of this points to a very concrete tactic, so that if they indeed feel it necessary to use nuclear weapons, we would be involved.

They have also demonstrated a very strong willingness to engage in conventional war with means that I'm afraid we do not have a full appreciation of. Some of the evaluations coming out at this phase of the Ukrainian crisis illustrates that we did not pay attention to the Georgian war, the Chechnyan war and the Syrian war.

Dr. Fergusson has already touched upon cyberwarfare. I am more concerned about the weaponization of social media. I do think that the Russians are problematic, in light of some of the evidence that our American and British allies have shown.

Ultimately, we are facing a threat from Russia. It is growing and it is reaching the level of an existential crisis.

Thank you very much.

● (1115)

The Chair: Thank you very much.

I would now invite Dr. Kitchen to take the floor and give up to five minutes of an opening statement.

The floor is yours, Dr. Kitchen.

Dr. Veronica Kitchen (Associate Professor, Department of Political Science, University of Waterloo, As an Individual): Mr. Chair and members of the committee, thank you for the kind invitation to speak to you today on the topic of Canada's emergency preparedness for threats posed by Russia.

My remarks today draw on a career studying Canadian security in a global context, and specifically on the work I've done with the Canadian Network for Research on Terrorism, Security and Society and as co-director for North American security at the Defence and Security Foresight Group.

The threat to Canada is exacerbated by Russia's clear desperation. Missiles over the Canadian Arctic or the use of weapons of mass destruction look more likely than they did a few months ago, even accounting for the fact that Russia is clearly preoccupied by its invasion of Ukraine not going as it expected. This may mean that the prospects for widening its targets to include Canada or NATO allies may be smaller in the short term, but possibly only the very short term.

What are the most immediate threats? My colleagues have already discussed some of the military threats. I want to focus on some of the immediate but more indirect threats to Canadian public safety.

Russia's disinformation campaign has been hindered by sanctions that have removed Russian media from our airwaves, but they are still prevalent on social media and in forums frequented by adherents of other kinds of populist conspiracy. The weapon of disinformation is not going away. One of the lessons of sanctions research is that sanctions become less effective over time, so we should expect this to be an ongoing threat from Russia. Canada is a target as a member of NATO, but also as a long-standing supporter of Ukraine as personified in the Deputy Prime Minister, Chrystia Freeland.

Russian disinformation campaigns connect the invasion of Ukraine to QAnon and other deep state conspiracy theories that feed hate crimes and distrust of the Canadian government. A concrete example is the recent QAnon claim that President Putin endorsed the sovereign authority of Romana Didulo, the self-styled “queen of Canada” and QAnon adherent. The attractiveness of conspiracy theories has been increased by the COVID-19 pandemic, and will be increased even more by Russian misinformation, whether targeted directly at Canada or not.

Certainly there's a risk that adherents of these conspiracy theories will commit violent acts, but the political action of supporters of populist extremism can also have harmful effects that don't escalate to the level of security threat or crime. We saw examples of this in the recent trucker convoy in Ottawa, where traffic prevented ambulances from leaving downtown and convoy supporters flooded the 911 system with calls. I want to be very clear that I'm not suggesting that the trucker convoy was a product of Russian misinformation, because I don't think we know that, but these are examples of the kinds of effects that are threats to human security, exacerbated by Russian disinformation, that we're not used to dealing with in the context of security and law.

The good news is that only a narrow swath of Canadians will be attracted to these ideas and influenced by Russian misinformation. The bad news is that their effects are easily amplified by bots, and the solutions may be long term. Media literacy can help in some instances, but in many cases the disinformation will be too sophisticated to educate ourselves out of. Working with private companies, as has already been mentioned, and our allies to improve our technological responses to disinformation is essential. The recent creation of the advisory group on online hate is a step in the right direction, as is the security and intelligence threats to elections task force, which some have suggested should have a role [*Technical difficulty—Editor*] in now.

We also need to find ways to turn down the temperature on social polarization caused in part by human insecurity and exacerbated by the necessity for global action against Russia. Examples include increasing fuel and food prices, but reinforcing trust in institutions through transparency, reform and cultural change also has a role.

We should not underestimate the ways in which Russia's actions have affected Canada's security by destabilizing the world. Russia has undermined the United Nations, committed war crimes, generated massive flows of refugees and threatened our borders and our allies. Canada is less secure in a world where international law is not respected.

It is easy to be overwhelmed by the scale of the threat when we're talking about everything from a potential nuclear attack to hate crimes. Foreign policy and domestic security are linked. Working to protect Canada from the most direct threats, from missiles to misinformation, and contributing to end the war are obviously imperative. Welcoming refugees and ensuring that the social services that help them are adequately resourced is important, but so too is ensuring that there's a perception that refugees from other conflicts are treated equitably, because not doing so contributes to mistrust in government.

● (1120)

The Chair: You have 10 seconds, please.

Dr. Veronica Kitchen: The need to provide military aid or come to the defence of our NATO allies in Europe stretches our military and forces choices about how to use it.

The biggest—

The Chair: Thank you very much. My apologies again; it's our world.

Thanks to the witnesses for those opening remarks.

We'll now move into the first round of questions from members of the committee. I'll start with Ms. Dancho.

You have six minutes. The floor is yours, Ms. Dancho.

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

I'd like to thank our expert witnesses for sharing your very critical and important testimony today.

My first question will be to Professor Fergusson, a fellow Manitoban.

Thank you again, Professor, for being here.

I would like your thoughts. We've been talking a lot in the last few months about modernizing NORAD and the north early warning system. Can you explain why it's important that we modernize those systems and how we go about doing so?

Dr. James Fergusson: The first answer is that we're vulnerable. The north warning system is out of date and, in fact, it's too limited to deal with the 360-degree threat environment that North America faces.

Government tends to talk about NORAD modernization as equivalent to modernization of the north warning system. It's much bigger than that. It's about North American defence modernization and developing a group of new sets of sensors, both land, sea, air and space-based, and developing the computer capabilities, the processing of analytical capabilities to be able to integrate an all-domain defence requirement. The F-35 is an important step forward, but it's only one step of thinking about the need for a much more complicated, complex, layered defence capability, one that has to move farther north.

All of these are major issues when we talk about dealing with the vulnerabilities that Canada faces in conjunction with our close ally, the United States, in trying to ensure that our deterrent, the Western deterrent, the U.S.-led deterrent, the global deterrent, is not undermined because of vulnerability at home.

Potential adversaries like Russia can hold Canadian populations as hostage, which would then reduce the willingness of governments in Canada and elsewhere to respond to deter these threats overseas.

Those are the two key elements in my mind.

● (1125)

Ms. Raquel Dancho: You mentioned that a U.S.-led deterrent should not be undermined by any vulnerabilities in Canada.

My understanding is that right now, with the advanced weapons technology and hypersonic missiles of Russia, we wouldn't even be able to detect any incoming missile threat, given our outdated system. Is that accurate? Is that the type of undermining and vulnerability we have in Canada?

Dr. James Fergusson: Certainly. The north warning system has no capacity to be able to detect a hypersonic missile flying over the Arctic region heading towards targets in the south. The American ballistic missile early warning system is optimized to deal with long-range ballistic missiles, not hypersonics, so you have a major gap there.

Moreover, the north warning system has a difficult time. It can potentially briefly detect cruise missiles in flight, but because of the long range, they'll be launched well over the Arctic Ocean, and that is another important detection gap we have. If we can't detect, we can't deter and we can't defend.

Ms. Raquel Dancho: Do we have adequate information sharing among Transport, the Canadian Armed Forces and any northern agencies? Do we have adequate Arctic coordination among departments currently, and do you see that as an issue?

Dr. James Fergusson: I think that's an important issue. Right now it's more or less ad hoc, depending on the specific issues that emerge, particularly in the Arctic.

If you ask who is responsible at the bureaucratic level for the Arctic, the answer is everyone. If everyone is responsible, no one is responsible. Government needs to rethink how it's going to organize to ensure that the various agencies—and this ranges from the Defence department to Transport Canada, the Coast Guard, Health, Industry, Foreign Affairs, etc.—all have a piece of the pie, and that needs to be looked at seriously.

I understand that government never likes to do this big reorganization, but we have to remember that we are structured for a world that no longer exists, with the Arctic as a function of climate change. This coordination and co-operation needs to be developed quickly.

Ms. Raquel Dancho: In essence, you would recommend that there should be a central agency responsible for Arctic defence, and there is currently not one of those.

Dr. James Fergusson: Exactly. I would call it a centre for Arctic security, with defence as a component.

Ms. Raquel Dancho: Okay. Thank you very much.

I have about a minute and a half left.

Professor Huebert, if you would like to just top up anything that Professor Ferguson has said, you're welcome to conclude my minute and a half.

Dr. Robert Huebert: The one area that Dr. Fergusson didn't have time to talk about is the maritime dimension of the approaches. He's talked very correctly about the hypersonics, but we know that Russian submarine activity has been increasing. We know that their deep diving capabilities are increasing. We've seen how they can do the cable, and NORAD has the mandate to deal with the underseas threat, but that is one area where we are really weak.

The Russians have even developed underwater autonomous vehicles that can go, allegedly, 10,000 miles and carry a nuclear warhead. Once again, these are all elements of the overall domain type of warfare that Russia now brings to the table that we ultimately and completely need to be able to detect and, as Dr. Fergusson said, respond to.

Ms. Raquel Dancho: In my remaining 25 seconds, do you have anything else to add about the critical importance of building our defences and where we should be focusing our efforts, for example, in the upcoming budget?

Dr. Robert Huebert: First of all, we have to make sure that we are getting that domain awareness. It's a 360-degree threat that is happening now. That means the entire entity of Canada is under threat of these new weapon systems.

If the Russians believe that they have an advantage that we can't detect or we can't respond to, we've seen the lengths to which they go in the engagement of the achievement of their objectives. That makes us very vulnerable.

The Chair: Thank you very much.

I would now like to invite Mr. Chiang to begin a six-minute block.

Mr. Chiang, the floor is yours, sir. Take it away.

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

I'd like to thank all the witnesses today for participating in this important study that we're doing.

My question is for Dr. Fergusson.

What are some strategic geographical advantages that Canada enjoys related to national security? How can we use these advantages to our benefit?

● (1130)

Dr. James Fergusson: The answer is twofold. We enjoy the strategic advantage of geography, which constrains the military and defence threats to North America to the aerospace realm. It can be maritime, as a function on maritime launch capabilities, but basically we can focus our attention on that.

The second big strategic advantage we have as a function of geography is that we sit beside the United States. It is a global superpower with the capabilities across the board to lead the global deterrent against not just Russia, but any other threats of importance to Canada that emerge. We benefit, of course, in our relationship with the United States from American support, the provision of American capabilities and American funding support for modernization on a 60% basis for infrastructure in Canada.

All of those work in our favour while at the same time providing us with access to American information and American planning, to ensure that Canadian interests are taken into account in the construct of NORAD as a binational command.

Mr. Paul Chiang: Based on your comments, is there something we could improve in our partnerships with the Americans? Can the Americans improve the NORAD system, or is that a joint venture?

Dr. James Fergusson: It's a joint venture and, importantly, NORAD is the driver behind the issue surrounding NORAD modernization, which is North American defence modernization. It is the planning centre right now, which will start to move requirements forward, hopefully, over the near term.

In terms of processing information, because that is centralized at NORAD headquarters in Colorado Springs, that's by and large American. That, I would note, is what's known as their pathfinder initiative, which is going to try to deal with the use of artificial intelligence for the massive amounts of data that are going to pour in from the sensor system.

That's part of it, but the key thing to me is that because of the nature of the changing threat environment—the origins and the platforms relative to the missiles—it's time Canada and the United States sat down and started to seriously think about a functional, integrated North American defence command. We have close bilateral defence co-operation with the United States in the maritime and the land sectors, but because of the nature of the all-domain environment, we need to take the step that we took in 1957-58 for the air world. We now need to move it into a true, integrated North American defence command.

Mr. Paul Chiang: Thank you so much, Dr. Fergusson.

Dr. Huebert, could you expand on some of the cybersecurity threats that Russia poses to Canada, and some of the measures that are needed to address these threats?

Dr. Robert Huebert: Absolutely. What we're seeing, and what we can see from some of the open reports, is that the Americans, of course, had to deal with the interference in their 2016 election. A British House of Commons committee examined what happened with Russian interference in Brexit, and there have been studies on Russian interference in the Castilian independence movement in Spain.

What we are seeing, or at least what seems to be appearing—and this is something of course that is Dr. Kitchen's expertise—is a focus on areas where society can be divided. This is what everybody refers to when they talk about the weaponization of social media. What the Russians have discovered...And we can't leave the Chinese out, because the Chinese are also heavily involved, or at least that is what comes out of the open literature. They try to divide societies by focusing on the various feeds that exist. This is then followed by a hope that somebody within that society will pick up that cause and become the leader.

It's sort of the issue that Lenin referred to back in the early days of Communism. “Useful idiots” basically tried to divide society. The effort today is actually to have a way of separating and neutralizing any support for the type of collective actions we need.

With regard to other cyber threats, we also know the Russians have shown an increasing capability of being able to interfere in various electronic systems and cyber systems of other states. We've seen this with their ability to influence the Ukrainian electrical system prior to the onset of the war in 2014. We're seeing this in other locations

Once again, it's hard to know exactly how well-defended we've become in being able to harden that part of cyberwarfare. There's no question, whatsoever, that the attention the Russians and the Chinese are giving this is increasing, if the reports from the Americans and British are indications of this capability.

● (1135)

Mr. Paul Chiang: Thank you so much.

The Chair: I would now like to invite Madame Michaud to begin her six-minute block of questioning.

[*Translation*]

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

First, I thank the witnesses for being here. Their expertise is more than welcome, given what is happening in Ukraine. We have good reason to be concerned.

Ms. Kitchen, I'm going to start with you.

You mentioned direct threats, but also indirect threats, including disinformation, the use of social media, phishing campaigns and the use of ransomware.

Aluminerie Alouette in Sept-Îles, one of the largest aluminum smelters in America, fell victim to a Russian ransomware attack in late February. The Russian group claimed responsibility for the attack, saying it had harvested up to 20% of the smelter's data. It said it was directly related to the west's economic sanctions against Russia. We are not immune to these kinds of attacks, which put our businesses, our citizens, our critical infrastructure and our democratic institutions at risk.

How do we protect ourselves from this? Do you think Canada is prepared to deal with these kinds of threats?

[*English*]

Dr. Veronica Kitchen: I think there are many levels to this. There is a level at which individuals need to take personal responsibility, making sure they're using things like two-factor authentication to protect their own systems, and obviously, that also applies at the level of organizations.

From a governmental perspective, it is really, as has already been discussed, a question of co-operating, both between the private sector and public authorities. This also includes across borders, recognizing that these kinds of threats are not easily contained within domestic borders, because of the transnational nature of companies and groups.

As Dr. Huebert mentioned, there is this effort with disinformation to inspire others to take action, rather than taking action directly, so that's one of the ways you can see this crossover from the cyberworld into the physical world.

Certainly, it is very important to ensure that the types of software that run big systems like refineries are up to date and protected from the Internet.

[*Translation*]

Ms. Kristina Michaud: One company actually offered free credit monitoring protection to employees who had been affected. My impression is that this is a service that the company offered on its own, in good faith, to its employees. That said, it is an afterthought, not prevention.

I would like to come back to what the government can do to protect businesses. What can it do upstream? What can it do afterwards?

Ransoms are certainly being demanded; most of the time these groups want money. In fact, there was a CBC/Radio-Canada article that explained how this kind of group could demand a second ransom.

How can the government intervene? To your knowledge, is this kind of surveillance protection service currently available to Quebec and Canadian businesses?

[*English*]

Dr. Veronica Kitchen: I'm certainly not an expert on ransomware attacks and on cyber-attacks of that nature. Unfortunately, I'm not aware of any specific services that might be offered, but again certainly trying to stop vulnerabilities before they happen...and I think the government can have a role in providing information on the kinds of threats that might be faced and, on the side of disinformation, providing accurate information to help combat the tendency to be taken in by things like phishing scams and ransomware attacks could be helpful.

● (1140)

[*Translation*]

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

Mr. Fergusson, do you have anything to add to this? I know you specialize in defence. Is it possible, to your knowledge, for the government to provide this kind of service? Does it need to modernize the services it offers to protect institutions and businesses from this kind of attack?

[*English*]

Dr. James Fergusson: I can't respond specifically. I'm like Professor Kitchen in my ability to answer these details. The key agency to provide information and notification is probably the Communications Security Establishment, CSE, but I don't know in detail how much they have moved in this area, because their work has always been dealing with the electronic world.

One of the dangers here—and I agree with Professor Kitchen that this is information—is stepping over the line with the government trying to regulate and to force on private companies certain procedures or certain systems. You could imagine a central system. That's going to be problematic because of the private sector issues involved, so care needs to be taken there.

[*Translation*]

Ms. Kristina Michaud: So it's not necessarily about interfering or imposing this service, it's about offering it and relying on the good faith of companies to put services in place to protect themselves.

Is that what you are saying, Mr. Fergusson?

[*English*]

The Chair: You get the last word on this, Ms. Michaud.

[*Translation*]

Ms. Kristina Michaud: Thank you.

[*English*]

The Chair: Now I will move to Mr. MacGregor.

Sir, you have a six-minute slot. The floor is yours whenever you want to grab it.

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

I will echo my colleagues in thanking the witnesses for helping inform our committee study into this very important and very interesting subject.

Dr. Fergusson, I'd like to start with you. Our committee's mandate is specifically to review legislation, policies and programs for government departments that are responsible for public safety and national security. I want to keep it focused on our internal security and efforts.

During your opening statement, I was taking notes and you made mention of the fact that there is no central agency to respond to cyber-attacks and that some restructuring may be necessary. In the United States there is an alphabet soup of different security and intelligence agencies that, to various extents, have capabilities to investigate cyber-attacks. Here in Canada the RCMP, CSIS and CSE also have their capabilities.

I'd like to invite you to expand on those remarks. Are you talking about more American-Canadian co-operation into an agency to take care of North American cybersecurity?

Dr. James Fergusson: I wouldn't necessary say that we need an agency, but we certainly need a structure with the United States. Remember, the United States is structured differently. All those agencies you're talking about all live in one house, the Department of Homeland Security. They are a bit of a step ahead of us, whereas, if you look at us, the RCMP are dealing with criminal activities, as a lot of ransomware is about crime, as hackers are out to make money. Then we have CSE on the intelligence side, as is CSIS, both coordinated under Public Safety.

Does Public Safety have the authority, and what are its links to Homeland Security in the United States? Are there regular meetings? Is there a bilateral committee? You can think about a variety of forms, for example, in the maritime warning world, where there are these developments, not just with the United States but also with the Five Eyes community.

I think it's important to look at those things in detail, such as whether we are structured right, particularly because the Internet cyberworld knows no borders. Information coming into Canada comes into the United States. It flows in patterns I don't know about or understand, really. Critical infrastructure is integrated with that in the United States, so we have a common interest as a function of our close relation of integration with the United States.

● (1145)

Mr. Alistair MacGregor: Thank you very much for that.

Dr. Kitchen, I'd like to move to you.

Thank you for your remarks informing our committee about the disinformation campaigns. Some of the narratives concerning Russian aggression that are coming out of some of the elements of the United States Republican Party and even some news organizations like Fox News have certainly raised some eyebrows. We do have the American mid-terms coming up. There could be a shift in how the United States Congress is governed following those mid-terms.

Considering how successful some of the disinformation campaigns have been in the United States, do we as a country need to closely examine what the potential pitfalls are from that disinformation campaign in the United States?

Dr. Veronica Kitchen: Certainly. There are a few different ways to think about this. One is in terms of the effect it might have on swaying an American election, both in the sense of whether there might be Russian interference and also broadly in terms of the direction in which the American people will decide to vote. Certainly some administrations and some policy positions will be easier for Canada to deal with than others will.

The other thing to be concerned about is the fact that individuals inspired by these kinds of narratives to take political action, whether it rises to the level of criminal activity or security activity, could be on either side of the border. The media landscapes in Canada and the United States are very closely integrated. This is not to say that there aren't separate causes in both countries, but we do see groups being inspired by each other across the border, and also groups that simply exist transnationally that might take action.

Canada's maintaining and diversifying our relations with the United States can help to make sure that our interests continue to be heard, even if we have a change in government.

Mr. Alistair MacGregor: Thank you.

I have a final question for Dr. Huebert. Is there anything that we as a committee should be examining or making recommendations to the Canadian government on with respect to Russian involvement in financial crimes in Canada, money laundering, etc.? Is there anything you might be able to inform the committee about on that particular subject?

Dr. Robert Huebert: It goes beyond Russian involvement. It goes into international crime, and we suspect also that there is Chinese involvement. It is, of course, the issue of transparency. One of the difficulties we've always had, in terms of being able to determine just exactly what the involvement of others is in the financial system, is that it's very hard to trace, in terms of both any regulatory regime and any government action.

If I have any overall statement on that, it is that it has to have some greater visibility in terms of what the transactions are, and there has to be a move away from the privacy that often protects these types of actions.

The Chair: Thank you very much.

Colleagues, that completes the first round of questioning. A quick look at the clock tells me that if I cut everybody's time in half in the second round, we'll finish more or less on time.

To begin, I would ask Mr. Lloyd to give us two and a half minutes.

The floor is yours, sir.

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

My first question is to Dr. Fergusson.

Considering the misinformation campaign, some people have been calling for censorship. Do you think that would backfire, if the government were to engage in censorship?

Dr. James Fergusson: Definitely it's going to backfire. As I said, I don't agree that disinformation campaigns—and they're not all coming from Russia; there are issues about our information campaigns as well—have that much of a significant impact in terms of exploiting social differences. But if you—

Mr. Dane Lloyd: Thank you.

I've always felt that the best way to fight misinformation is to fight it with true information, and so I'll ask the same question of Dr. Kitchen.

Do you think it would be more effective to fight misinformation with a vigorous campaign of putting forward true information? Do you think censorship would be effective or would it backfire?

Dr. Veronica Kitchen: Certainly providing true information I think is always a good strategy, but for true information to be effective, it has to come from institutions that people trust. Maintaining that trust in institutions through transparency, as Dr. Huebert mentioned, is vitally important.

Mr. Dane Lloyd: Do you think that censorship would undermine trust in those institutions?

Dr. Veronica Kitchen: Quite possibly.

Mr. Dane Lloyd: Thank you. I have a remaining one minute or so.

I'm just amazed that North America has such superiority in information technology, and obviously we have to work on improving that. Militarily, with our allies—and this is for Dr. Fergusson—we also have tremendous superiority. I'm amazed to see the footage out of Ukraine, with Russia's superior technology being shot down by relatively cheap technology like MANPADS and Javelins.

What I'm wondering, though, is on the missing piece, economic security. It seems that we have a gaping hole when Europe is completely dependent upon oil and gas from Russia, and copper and palladium.

What do you think the government could have been doing better for the last 20 years in this country—multiple governments—to address that economic insecurity?

● (1150)

Dr. James Fergusson: I don't know if there's much the government could have done. Remember, we're living in a world of globalization. This is the downside of globalization. It's not just about Russian resources being provided to the Europeans, but how that international marketplace is structured and works out.

Certainly, we could have been more aware of this potential; I don't think a great deal of attention has been paid.... We tend to see globalization as good, in economic terms, but we didn't pay attention to security.

The Chair: Thank you very much.

I would now like to invite Mr. McKinnon to take the floor for two and a half minutes.

Go ahead, Mr. McKinnon.

Mr. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.): Thank you, Chair.

My question will be for Dr. Fergusson.

In our world, of course, we're becoming evermore interconnected electronically. That includes domestic and international communications. To get from A to B, our messages end up getting routed all over the place and in-between.

The core functionality that makes us secure is encryption. One of the key aspects of encryption are that at some point there will be asymmetric encryption involved there. We know that asymmetric encryption has a public part of it and a secret part of it, and we know the secret part can be brute force, if the adversary has enough time and willingness to do so.

State actors such as Russia, China and so forth have possession of massive computing facilities, with massive parallel processing. I'm wondering what we can do to change our communications infrastructure to protect our communications security and our encryption.

That's a big question, and you have a minute and a half.

Dr. James Fergusson: I can only comment in terms of the defence side, and keeping closed, highly encrypted and the most advanced encrypted systems in the intelligence and the defence world.

Again, it's not necessarily the case that government or Defence are going to let anyone know when they get hacked and these systems are actually penetrated. However, this is an interactive process—not so much for Canada, but certainly for our allies besides the United States, so there's always the capability that we retaliate. This is nothing new. This is what we used to call “electronic and counter-electronic warfare”. This is something that's gone on. It's become more sophisticated and it's become quicker because of the nature of the technological piece and the changes that have occurred.

There's no 100% guarantee, but certainly ensuring that you know when you get hacked is the most important thing. The biggest danger is not the hacking, but the implanting of viruses, such as the one planted in the Iranian nuclear system years ago, and—

The Chair: Thank you.

I would now like to invite Ms. Michaud to take a minute and 15 seconds.

[*Translation*]

Ms. Kristina Michaud: That is generous of you, Mr. Chair. Thank you very much.

[*English*]

The Chair: Make the best of it.

[*Translation*]

Ms. Kristina Michaud: I will now turn to Mr. Huebert.

As you were saying, cybercrime is such a fast-moving world. Given that, and given that you know Canada's preparedness, do you think we are in a position to deal with the worst-case scenario, whether the threat comes from Russia or another country?

In terms of public safety and national defence, do you believe we are prepared?

If not, what should the government's priority be?

[*English*]

Dr. Robert Huebert: We never know if we're ready.

At the University of Calgary we were hacked with ransomware even though we have computer science and individuals that do.... We weren't prepared for that. In fact, our entire computer system was shut down.

Part of the problem is that until we know the level of what's coming in...what that requires is a very well-funded counter-cyberwarfare capability.

Be it the CSE or whomever you're giving that to, it's that grungy day-to-day.... Make sure that you have the best computer analysts that are able to look at it and constantly be re-evaluating. It's dull. It can't be shared, so people like me, Dr. Kitchen and Dr. Fergusson won't know how good or weak it is, but it's something that the government needs to be totally on top of.

● (1155)

The Chair: Thank you very much.

Mr. MacGregor, you have 75 precious seconds. Go for it.

Mr. Alistair MacGregor: Thank you.

Very quickly, this is for Dr. Kitchen, on the disinformation subject.

There have been a lot of parallels between this study and our study into ideologically motivated violent extremism and the way major companies, social media companies and companies like Amazon, can be exploited using their algorithms. Even in some cases like Amazon, their platforms are used to sell hateful propaganda. The potential exists for a determined state actor to take advantage of that.

If not through censorship—I think there's an argument to be made to remove untrue information—in what ways can the Canadian government effectively make sure that social media companies are not going to be vulnerable to these types of attacks?

Dr. Veronica Kitchen: This is where possibly regulation does become helpful to make sure that we're getting rid of bots, to make sure that we're getting rid of things that act automatically. Working together with those companies who are open to the idea of trying to control extremism—many of them—on their platforms is important. It's also important to recognize that there are a whole series of secondary platforms where this kind of misinformation spreads that are a little more underground and less willing to work with governments.

The Chair: Thank you very much.

Mr. Shipley, I'll now turn to you for two and a half minutes of questioning, sir, whenever you're ready.

Mr. Doug Shipley (Barrie—Springwater—Oro-Medonte, CPC): Thank you, Chair.

Thank you to the witnesses for being here today.

I'd like to direct my first question to Mr. Fergusson and Mr. Huebert.

I was trying to frantically take notes as both of you were talking. I was finding it very interesting and informative. We don't have time to have an open-floor debate here for a long time. I'd like to have answers on both of these from both of you, please.

Mr. Fergusson, you stated that disinformation is overblown, exaggerated and doesn't pose a real threat. That's as close to a quote as I could scribble at the time.

Mr. Huebert, I took from some of your quotes that you are very concerned about Russia's social media and the weaponization of social media.

I'm sensing a bit of a difference there. Perhaps I could get some clarification, first from Mr. Fergusson, on the threat seen by that and then Mr. Huebert after him, please.

Thank you, Mr. Chair.

Dr. James Fergusson: My answer to that is simply the lack of confidence and trust in the public. You're certainly going to have small proportions, as Professor Kitchen pointed out, of extremists who can be manipulated, but there's already fertile ground to be manipulated.

If you look at the overarching component of the public, who are more involved in this than I am, I think we can trust them. I think they understand when they are being taken down the garden path. Issues of the small minority becoming radicalized and violent probably existed prior to any misinformation or disinformation, whatever you define that to be. One person's disinformation is another person's truth. It's complicated.

I think we put too much of a scare sense, a panic, if you will, around this without stepping back and saying.... I'll put this bluntly: Trump won the 2016 election and it was not because of the Russians. That's an excuse that's then dragged out to explain this anomaly which the elites couldn't understand.

Mr. Doug Shipley: Thank you, Mr. Huebert.

Where I disagree and where I think we're being complacent is when we look at the type of advice we are now seeing in society. In other words, there is no question that this has been attempted before. We know that from the Cold War period, but now because of algorithms and the efficiencies of these new systems, I think the divides within Canadian society on the COVID issue alone illustrate that it's not simply a sort of silent majority in the middle that is always going to get it. We see the divides between families and friends, and it's directly a part of the problem.

The Chair: Thank you very much.

You have two and a half minutes to pose the last question, Mr. Noormohamed. Take it away.

● (1200)

Mr. Taleeb Noormohamed (Vancouver Granville, Lib.): Thanks very much.

Given the brevity of time and recognizing the limitation of the scope of this committee, I have a question for Dr. Kitchen.

Can you spend a little bit of time talking about the specific concerns related to disinformation and the way it is starting to have an impact on Canada, and in particular how you are seeing it impact action in Canada? Are there specific ties to international actors, particularly Russia?

I would love to hear your thoughts on that.

Dr. Veronica Kitchen: Dr. Huebert already gave some of the international examples. We also know that SITE identified international attempts to influence the 2019 election. We've seen individuals who have been inspired by Russian propaganda. For instance, there was a threat to the Prime Minister. I'm blanking on the date; it was earlier in the year.

Where this is important is the way it interacts with tendencies that already exist in Canadian society, such as on the appeal of COVID misinformation. Where we will see Russia and other international actors acting is in trying to exacerbate those existing social polarizations.

This is a Canadian problem that is exacerbated by foreign interference.

Mr. Taleeb Noormohamed: Thank you, Mr. Chair.

I may be out of time.

The Chair: You actually have about 45 seconds.

Mr. Taleeb Noormohamed: Dr. Kitchen, could you just follow up? You talked about COVID as one of the pockets of misinformation.

Where are some of these other pockets where you see this really starting to foment? What trends are you seeing that concern you?

Dr. Veronica Kitchen: Certainly there is the violence we have seen in the COVID context against Asian Canadians and other minority Canadians. We could see that replicated, possibly against Russians or against Ukrainians in Canada.

We could also see various other instances where racialized individuals are being targeted because of the appeal of white supremacy that is in part promoted by Putin's world view, which is certainly that Russia is the correct leader of western civilization. That helps to fuel those right-wing extremists as well.

The Chair: Thank you very much.

On behalf of members of the committee, and indeed on behalf of all parliamentarians, I would like to thank the witnesses. Collectively, you have literally decades of experience and a very deep understanding of the complexities of these issues. We're very grateful that you have shared your expertise and your insights with us this morning.

Colleagues, we'll now take a short, five-minute break to change panels, then we will resume the meeting.

For those who leave now, thank you so much for being a part of this.

Colleagues, we'll see you in about five minutes.

● (1200)

_____(Pause)_____

● (1205)

The Chair: Colleagues, I now call the meeting back to order. If you could take your seats, I will assume everybody is where they are supposed to be.

With us this hour by video conference is Dr. Ahmed Al-Rawi, assistant professor, Simon Fraser University. I would also like to welcome Dr. Alexander Cooley, Claire Tow professor of political science, Bernard College, and academy adjunct faculty at Chatham House; and Dr. David Perry, president, Canadian Global Affairs Institute.

There will be up to five minutes for opening remarks from our guests, after which we will have two rounds of questions. I'll begin by inviting Dr. Al-Rawi to make an opening statement of up to five minutes.

Sir, the floor is yours.

● (1210)

Dr. Ahmed Al-Rawi (Assistant Professor, Simon Fraser University, As an Individual): Thank you, Mr. Chair.

Russian disinformation in Canada has been an ongoing issue. The Russian government has an ongoing interest in interfering in Canadian politics using a variety of information operations, propaganda and disinformation.

Using publicly available datasets released a few years ago by Facebook and Twitter, I found that Russian trolls were the most invested in targeting Canada, far more than Iranian and other state-run trolls from China and Saudi Arabia were. These information operations were conducted with the use of carefully concealed social media users with the assistance of fake websites as well as news channels like RT, Russia Today and Sputnik.

For example, the Internet research agency, IRA, created fake Facebook pages and purchased ads often targeting Canadians in 2016 and even earlier. Fake websites like peacedata.net that seemed legitimate were also used like to spread favourable messages towards Russia. I also found in 2017 that Russian trolls even promoted a rally in Ottawa against the Liberal government.

In my research, the content analysis of social media messages clearly showed that the ideological position of the Russian government aligned well with far-right groups and individuals in Canada.

In my view, the main reason behind this information operation strategy is to sow division, create tension and confuse people about what is real or fake. For example, the main targets of Russian trolls were Liberals, especially due to their immigration policies, with a focus on attacking Justin Trudeau and Chrystia Freeland. The second target is related to Canadian Muslims, with emphasis on visible minority MPs followed by other targets on issues like refugees, diversity and multiculturalism.

Today and due to the increasing pressure on traditional social media companies, the public activities of Russian trolls have been relatively curtailed, as there is some scrutiny and general awareness. The same applies to the way Russian state news outlets like RT have been flagged as promoters of disinformation and sometimes banned from operating. However, I personally think that the decision of the CRTC, Canadian Radio-television and Telecommunications Commission, to ban RT remains only symbolic and ineffective, because RT can be viewed in multiple other ways in Canada and elsewhere.

We can see today a different information strategy that uses Russian government diplomatic missions as its main means to spread propaganda. For example, the Russian embassy in Ottawa runs its own Twitter account as well as recent Telegram and VK public channels. The embassy has been active in spreading disinformation and promoting the Russian perspective on the events taking place in Ukraine. Instead of heavily relying on RT or Sputnik, the embassy mostly retweets messages from the Russian foreign affairs ministry and other Russian diplomatic accounts and missions from around the world as well as Russia's foreign allies like China.

Also, the embassy frequently posts statements attacking Canadian officials as well as national news media for what it views as biased attitudes towards the war in Ukraine. Any factual reporting on the war is considered fake news, and the term itself is weaponized by the Russian foreign affairs ministry to serve the interest of Putin's regime.

One of the most troubling features of this disinformation campaign by the Russian government is related to the weaponization of fact-checking practices. In a recent tweet, the embassy in Ottawa announced the launch of a new website called WarOnFakes.com, which attempts to give credibility to official Russian propaganda. The website allegedly provides fact-checking services with regard to the war in Ukraine and is offered in five languages: English, French, Spanish, Arabic and Chinese, denoting that the main targeted groups are non-Russian speaking audiences.

Finally, the embassy is trying to create a direct link with the Canadian public that cannot be blocked by the CRTC. For example, the embassy often sends direct messages to Canadians via its Telegram channel and Twitter account. In fact, more than 3,000 Twitter users who retweeted recent messages from the embassy are found to be Canadian users who were further spreading these messages.

Though the official and public focus has been on banning RT and Sputnik news channels, the reality is that Russian embassies are creating their own information ecosystem with the help of fake fact-checking websites like WarOnFakes.

● (1215)

The official Russian disinformation has evolved today to heavily rely on multiple sources, including the social media outlets of these diplomatic missions—

The Chair: Thank you very much.

I would now like to invite Dr. Cooley to make an opening statement for up five minutes.

Sir, whenever you're ready.

Dr. Alexander Cooley (Claire Tow Professor of Political Science, Barnard College, and Academy Adjunct Faculty, Chatham House, As an Individual): Thank you very much, Mr. Chair. It's an honour to be able to address the committee.

I would like to focus my remarks on two distinct groups of global and transnational networks that the war has spotlighted and that I believe reverberate back into western societies, Canada included. They also pose some significant policy challenges.

The first you will have certainly heard of and deliberated about, and that is the group of oligarchs. We have seen Russian oligarchs targeted with sanctions by the U.K., Canada, the EU and the U.S. Here, we have acknowledged in some ways that a bet that we made a long time ago has failed, and that is the idea that if oligarchs had access to western stock markets and boardrooms and philanthropic types of circles, then their behaviour would be moderated and somehow they could influence the Kremlin itself into moderation.

We face two challenges with the oligarchs going forward. One is going after their assets and freezing them, and the other one is their reputations. In both of these areas, we also have to contend with service professionals who work here in the west, in the U.K., in the U.S. and in Canada, who enable both of these processes. They take their money, put them into luxury real estate, purchase shell companies and hide them in complex networks of bank accounts, as well as the PR agencies and the reputation management firms and lobbyists who try to recast them, not as politically exposed persons with links to the Kremlin but rather as global philanthropists. This is a challenge across all western societies.

The second group perhaps is less on your radar, so I will focus a little more time on them. That is this emerging community of new Russian exiles that we see the war has created. Certainly, we have seen a steady stream of opposition and journalists go out of Russia during Vladimir Putin's increasingly authoritarian reign, but the dislocations of the last month are truly striking. I would focus on three distinct groups here.

First, hundreds of journalists are fleeing Russia. They are setting up their own networks and channels. We already have a number of distinct Russian independent media outlets that operate from abroad, from the Baltic states or via Telegram channels. I believe they should be supported and openly encouraged because they're the only source of Russian-language independent media out there.

Second, tens of thousands of IT workers, with 50 to 70 this month, possibly up to another 70 next month, have fled the country. They are in places like Georgia, Armenia or Uzbekistan. As the Russian government has sanctioned big tech and declared Facebook undesirable, you have seen a flight of qualified IT workers outside of the country too.

The third group would be hundreds of academics and think tank analysts who have also left the country, who do not want to face the consequences of 15 years in prison for calling out this war. They're also exiled in places like eastern Europe and Istanbul, and they are also looking for new types of affiliations and academic homes.

My suggestion to the committee here is to think about strategies to enhance and strengthen these new networks of exiles as they try to promote independent thought and affect, as much as they can from outside, the disinformation propaganda within the country, and to think about what kinds of policies can be adopted to sort of make us a force multiplier as the Kremlin tries to decouple from the west, to ensure that these independent and critical voices can be encouraged from outside of the country.

● (1220)

The Chair: Thank you very much.

I would now like to turn to Dr. Perry.

Sir, you have five minutes to make an opening statement. Whenever you're ready, the floor is yours.

Dr. David Perry (President, Canadian Global Affairs Institute, As an Individual): Thank you, Mr. Chair and members of the committee, for the invitation to speak today.

The horrific events we're watching unfold in Ukraine are demonstrating that Russia is prepared to employ its modernized military without provocation in ways that are fundamentally anathema to Canadian interests and values, and that we in Canada find difficult to comprehend.

In response, we have moved with urgency and ingenuity to help Ukraine defend itself and deter further Russian aggression in Europe by strengthening eastern Europe's defences. We should act with similar urgency and ingenuity to ensure that Canada and North America are better defended against potential Russian aggression closer to home. Russia is challenging Canadian and western interests in multiple places around the world and with many different means, including cyber and disinformation activities.

In my comments today, I will focus on the impact of Russia's military modernization over the last two decades, and the increased threat it poses to Canada, the United States and North America. Russian aircraft, ships and submarines can now carry advanced cruise missiles that could accurately hit targets in North America at long ranges, as can other long-range Russian missiles, including hypersonic glide vehicles.

We cannot at present detect and track these threats well enough, nor can we prevent them from damaging targets here in Canada. We need to quickly improve our ability to do both. As a result of the Canada First defence strategy in 2008, and “Strong, Secure, Engaged” in 2017, Canada has been progressively improving our ability to defend Canada over time, including through the purchase of a fleet of modern fighter aircraft, aerial refuelling tankers, surveillance platforms and a modern naval fleet.

I was happy to hear in the last several weeks that the government is moving to further address the defence of the continent through the modernization of NORAD and continental defence. This will presumably involve a new policy framework and a combination of new equipment, the people to operate it, new or enhanced infrastructure training and the other support required to turn that equipment and those people into a useful military capability.

Let me offer some suggestions now for how we can turn this long-evolving commitment to act with our American allies to strengthen the defence of the continent into concrete action, by focusing on the equipment procurement needed to make that happen. However, some of these elements, I think, are applicable to the other activities we might want to consider.

First, defending Canada must be a priority of government. Successive governments have been improving our ability to defend Canada over the last decades and we have been discussing the modernization of continental defence for years, but those efforts have not moved ahead with the urgency required.

As a result, the pace of implementation has fallen short of expectations. Money has gone unspent year after year, and needed equipment projects have been delayed. The war in Ukraine is demonstrating the importance of having a capable modern military at the moment, when Russia or any other military power precipitates an international crisis, not when we in Canada can get around to doing it.

We need to continue implementing “Strong, Secure, Engaged” and move forward on the modernization of continental defence with urgency we have not seen recently. Doing so will require that this be made a top priority of the government, set by the Prime Minister and cabinet and clearly communicated throughout the Government of Canada and all of its department and agencies.

Second, a bigger defence budget is needed now. Canada's current defence spending plans are insufficient to deal with the threats posed by Russia and other powers like China. Our military, like everyone else's, is facing historically high inflation pressures that are exacerbated by procurement delays. We also have lingering maintenance and infrastructure deficits, as well as personnel shortfalls.

Looking forward, continental defence is an unfunded liability that the 2022 budget must address. Beyond our immediate spending requirements, how much we spend on defence sends a signal to both allies and adversaries of our commitment to our own defence, as well as to international peace and security more broadly. NATO's 2% of GDP spending target is an imperfect measures of allies' contributions to collective defence, but it is one that all allies, including Canada, agreed to meet. If we remain unprepared to reach our alliance spending targets, we should be prepared for our allies and adversaries to question our commitment to defence and international peace and security.

Third, and finally, more money is required, but more capacity is needed to actually use it. Canada is in the middle of the largest defence recapitalization effort since the Korean War. This is in large part because we're making up for lost time during the decade and a half following the end of the Cold War, when we invested insufficiently in our forces.

Many of the key combat fleets we operate today, including fighters and frigates, were purchased in the 1980s—which is the last time period when we spent at a 2% of GDP level—and those assets should have been replaced years ago. Today, we're trying to make up for lost time, using a procurement workforce that was cut in half in the 1990s and never fully rebuilt.

Moving our military modernization forward faster will require an increase in the procurement system's capacity, because we have too few people with the right skills at present to manage the projects that are already funded, never mind what may come this Thursday with the additional budget dollars.

Thank you, Mr. Chair.

● (1225)

The Chair: Thank you very much.

Colleagues, we'll now move to the first round of questions. This is a six-minute block and we'll start with Mr. Van Popta.

Sir, the floor is yours.

Mr. Tako Van Popta (Langley—Aldergrove, CPC): Thank you, Mr. Chair, and thank you to the witnesses for being with us here today and sharing your knowledge for the benefit of this committee and Canadians.

Dr. Perry, I'll start with you. In 2018, you told the foreign affairs committee at a hearing that “Canada's official position is that the Canadian Arctic is a zone for peace and co-operation.” You added that to increase our chances of realizing that desirable outcome, we would have to bolster our defences to better deter Russia.

That was three or four years ago. What would you say today about Canada's defence capability in the face of Russia's naval and air presence in the north?

Dr. David Perry: I'd say that in the intervening time, we haven't done enough to actually close the gap that I was talking about back then. We have programs under way. You mentioned a couple of them. We just saw, a week ago, an announcement about acquiring future fighter aircraft. Those also remain works in progress, and not enough tangible action has been taken to close that gap, so most of that gap or delta with what we can do and what we should be able to do, unfortunately, remains in place today.

Mr. Tako Van Popta: I was looking at the mandate letter for the Minister of Defence,Minister Anand, and it says, among many other things, that we will maintain a strong contribution to NATO and work with the U.S. to modernize NORAD.

Would you characterize our contribution to NATO as strong?

Dr. David Perry: Our operational contribution to NATO is strong. Our commitment of providing good personnel to what the alliance does has been strong, but we have fallen well short of our alliance commitments toward burden sharing, expressed as a share of our economy that we're devoting to military spending.

For years, we have been well short of the target of 2% of GDP overall going to the military [*Technical difficulty—Editor*] Now, more than ever, our allies, as well as adversaries, are taking note of those shortfalls.

Mr. Tako Van Popta: If we were to increase our military spending to 2%, as we have agreed to with our NATO allies, what would that look like for upgrading the north warning system? I understand it's still 1980s technology.

Dr. David Perry: If we were to move to that threshold of spending, it would allow us to move forward meaningfully with continental defence modernization, which has a number of Arctic elements as part of it. It would allow us to bolster the use and utility of the infrastructure that we have up there, the types of assets that we can deploy into our own Arctic, and provide us with a quite significant increase in our ability to defend Canada as part of North America.

Mr. Tako Van Popta: What specifically should we be looking for in that vein in the upcoming federal budget when it comes to military spending?

Dr. David Perry: I'd be looking for details on how the government plans to translate the high-level statement of intent, signed in a letter last August with the United States Secretary of Defense, into specific lines of action to move forward on continental defence, along with a funding plan to make that happen.

Mr. Tako Van Popta: You also stated there was money that had been allocated, but not spent. With the recent announcement of Canada purchasing F-35 fighter jets, is that a step in the right direction? Perhaps you could comment on that.

Dr. David Perry: I think it's absolutely a step in the right direction. Over successive years, we've had money set aside to buy new fighter aircraft, but because of delays in that project, that money continued to go unneeded in the immediate term because we hadn't got to the point where we could sign a contract. The announcement last week of a new fighter fleet is long overdue, and a more necessary commitment to improve the defence of the country.

Mr. Tako Van Popta: I've heard it said in conversations, and I've read it as well, that there are people in our policy-making community who say that in order for the United States to defend itself, it must also defend Canada.

Is that true, in the sense that there are those conversations going on, and is it true in the sense that the U.S. must defend itself?

● (1230)

Dr. David Perry: I think that's true, and it's a risk. It's one that is actually a risk to Canada. If the United States felt that it was in that particular position, it's as much of a benefit to us—not just for our own security, but our position with our closest ally on the continent we share—to be viewed as a partner in national defence, and not as a liability.

Mr. Tako Van Popta: How would you characterize our level of partnership with the United States when it comes to NORAD?

Are we okay?

Dr. David Perry: I apologize. I've lost the audio feed.

Mr. Tako Van Popta: Okay, I'll just repeat the question.

The Chair: Mr. Perry, can you hear us?

Mr. Tako Van Popta: Could I ask another question of another witness? Do I still have some time left, Mr. Chair?

The Chair: You just have a few seconds, sir, yes.

Mr. Tako Van Popta: Okay, I'll give it back to the chair.

The Chair: Mr. Noormohamed, you're now up.

You have a six minute block. Whenever you're ready, take the floor.

Mr. Taleeb Noormohamed: Thank you, Mr. Chair. Again, I'd like to echo my colleagues in thanking all of you for being here with us today.

Dr. Al-Rawi, since our world here at SECU does not necessarily allow us to think about defence spending or defence procurement, I'd like to focus on some of the areas where we do have some responsibility.

I'd like to talk a little bit about some of what you said with respect to the Russian trolls. You talked about their areas of interest right now being around the war.

Can you talk about some of the other areas of interest that they are particularly leaning into or curious about?

Dr. Ahmed Al-Rawi: Historically, the Russian trolls have been very much invested in supporting the far right in different countries. It's not only in Canada, but also in the U.S. and in many places in Europe. The reason is definitely to create tension.

There is a term called “agitainment”, which means making people really agitated, but at the same time entertained. That is done using, for example, funny memes and funny messages, but they are very much militant, aggressive and often racist.

You can see a pattern. This pattern shows that the Russian trolls usually align themselves with extremes and sometimes even with the far left.

That's the strategy in general. Often the targets will be the minority groups, especially refugees and immigrants in different countries. The focus sometimes will be on the Netherlands or in the U.S.A., but that will be the main issue.

I hope I answered your question. Did you want me to focus on today?

Mr. Taleeb Noormohamed: You did. Maybe we can dig a little bit into that.

You've talked about them being anti-Muslim, anti-immigrant and anti-refugee. You mentioned anti-liberal in the last election.

Are they just anti or are they actually doing things to promote other causes? Are they pro certain things that we should be concerned about here in Canada?

Dr. Ahmed Al-Rawi: Usually they promote far right groups. Sometimes they don't show a lot of animosity towards Conservative figures and politicians, but that kind of animosity is usually shown against Liberals and NDP figures. That's their strategy. Again, it's about what aligns with their own world view and with what they want to achieve.

It actually echos Putin's policies inside and outside Russia. It makes a lot of sense. For instance, when they talk about the White Helmets in Syria, they consider it a terrorist group because the White Helmets are actually trying to undermine the Russian efforts in Syria by documenting human rights violations and so on. They do this with the help of allies, as well as friends from the region and elsewhere.

Mr. Taleeb Noormohamed: Thank you, Dr. Al-Rawi.

My next question really is for you, but I would also like Dr. Cooley to weigh in once you're done,.

We had seen a lot of the impact of Russian misinformation in the lead-up to January 6. On January 6 in the United States, there were clear links and support for what was happening with the QAnon movement. There was a very successful attempt by Russian bots to try to tie what happened on January 6 to antifa. Evidence in the January 6 reports shows that there was a pro-Trump effort on the part of Russian bots. Harvard Law School Professor Yochai Benkler said that the primary goal of Russian propaganda is to “create a world where nothing is true and everything is possible”.

I'd love to hear your thoughts on the impact on Canada and whether or not Canada needs to worry about those trends we saw in the January 6 uprising in the U.S.

I'd like Dr. Cooley to weigh in on that one once you're done, sir.

● (1235)

Dr. Ahmed Al-Rawi: I think we definitely need to be concerned because the goal is to confuse people and make their vision of reality blurred in a way that they will not understand what is right and what is wrong or what is real and what is fake. This is very concerning. This is definitely related to what is going on in Ukraine and also in terms of COVID-19 and so on.

I can talk a lot, but I think maybe Dr. Cooley wants to also add here.

Dr. Alexander Cooley: I would agree with that. I think from the Russian world view, there's sort of an outside world, which is this drive towards multipolarity and not having the liberal west dominate the international system and having spheres of influence. There's also a domestic internal component with that: breaking down consensus for this kind of movement to collective liberalism, whether it's NATO, support for transnational co-operative solutions or respect for human rights and liberal values. Any time they can poke holes in that, either by exacerbating partisanship or political polarization or by targeting vulnerable communities, they will do it.

I want to emphasize this. The goal is not to make Russia look better. It really is to try to show what they think are contradictions and weak points in our own messaging and our own societal debates, and take that from being a strength to somehow being a weakness of our own domestic institutions.

Mr. Taleeb Noormohamed: Dr. Cooley, if I could, I'll ask you to follow up. Can you talk a bit about—

The Chair: You have 10 seconds.

Mr. Taleeb Noormohamed: In that case I'm going to give my time back.

Thank you so much to all of you for your time.

The Chair: Thank you.

Now I would like to ask Ms. Michaud to take her six-minute block, please.

Go ahead, whenever you're ready, Ms. Michaud.

[*Translation*]

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

I thank the witnesses for being here.

Mr. Al-Rawi, I'm going to take advantage of your expertise in social media, communication and disinformation to ask you a few questions. I would like to know what influence you think Russian disinformation has on the population of Canada.

We know that several means are used, for example misleading claims, manipulated photos and conspiracy theories. We know that this is used a lot in social media and that this may have been exacerbated not only by the COVID-19 crisis and the rise of the anti-vaccine or anti-system movements, but also by what is happening in Ukraine.

What is the influence of this phenomenon and what could the consequences be?

[*English*]

Dr. Ahmed Al-Rawi: In terms of the actual impact of disinformation on the population, it's a really difficult question to answer because I don't think anyone has quantified that or fully understood this kind of influence. However, there are indications of the impact of disinformation on Canadians. For example, we saw some kind of violence against the Ukrainian diaspora community in Canada, and this is a clear indication or evidence of the influence of Russian disinformation—or if you want to call it propaganda—on certain communities.

If you look outside Canada, I'm seeing very worrying signs about the outreach of Russian disinformation. For example, when I looked at Arabic language disinformation spread by the Russian government on social media, I was really [*Technical difficulty—Editor*] so widespread and so overreaching in so many places in the Middle East.

Our problem here is that we're mostly focused on English and French in Canada. We forget that we have millions of people who do not only speak these languages; they speak other languages. I think this is a major gap in our understanding of the real influence of Russian disinformation on our diaspora communities. There is a very direct connection, but we miss a lot. These are all gaps in our understanding, unfortunately, but there are clear indications that a lot of people were influenced.

We also have some people who are replicating this kind of disinformation. One example is Global Research, which is a so-called news organization based in Montreal that is only echoing Putin's propaganda on its website.

● (1240)

[*Translation*]

Ms. Kristina Michaud: Thank you.

I am trying to understand how the government can intervene to protect the public from this disinformation. Perhaps banning Russian state media broadcasts like RT or Sputnik would be a good way to protect the population who would tend to associate themselves with this kind of movement of very anti-system “Putin” rhetoric. I know that Canada is doing it in the case of RT, but I don't know if it is doing it in the case of Sputnik. The European Union, on the other hand, has gone that far.

Do you think this can have a positive effect for the people of Canada?

[*English*]

Dr. Ahmed Al-Rawi: Thank you, Mr. Chair.

I need to explain why banning RT, as I mentioned in my speech, might not be fully effective. The reason is that RT could be viewed in different ways—through TV apps, the Internet and so on. I think if anyone wants to view RT, it's there, and I don't think it's the only source.

As I said in my speech, the Russian government is now using its own diplomatic missions to spread disinformation using these fake websites and so on. They are trying to create another information source because the focus has been on banning RT, and now they are looking at producing more disinformation from other places.

I think the best way to protect Canadians from this kind of disinformation is by debunking, by fact-checking, anything that is related to Canada or Canadians in relation to the war on Ukraine.

We cannot catch up with what the Russian government and its allies are doing. It's really hard to do so unless, of course, there is some kind of collaboration between Canada and other countries, but what we can do is debunk what is related to us so that we can better protect Canadians, especially if something is related to what happens inside Canada or within the diaspora community living in Canada.

[*Translation*]

Ms. Kristina Michaud: Thank you.

In fact, in this sea of information, it's very difficult for citizens to sort out the real from the fake. How do we analyze all this? I know that Canada is doing some prevention. For example, the Communications Security Establishment runs campaigns on Twitter, advising people to check the source of the information they consult.

But beyond that, what role can the government play in prevention and in helping citizens sort out the real from the fake?

[*English*]

Dr. Ahmed Al-Rawi: Thank you, Mr. Chair.

It will sound self-serving, but I think academics need more funding to run maybe research projects, fact-checking in an ongoing way, these incentives—

The Chair: Thank you.

I now would like to turn to Mr. MacGregor.

Sir, you have a six-minute block of questions, whenever you're ready to go.

Mr. Alistair MacGregor: Thank you very much, Mr. Chair. I'll start with Dr. Al-Rawi.

In your opening statement when you were talking about the role that Russian diplomatic posts in Canada have in spreading disinformation, it's always very tricky when dealing with diplomatic outposts because, of course, we have to be concerned about reciprocal actions against our own diplomatic missions, particularly in Russia.

Do you feel that we are effectively countering the Russian embassy's role in spreading disinformation currently? Is there a heightened awareness of what they're doing, or do you feel that our committee could make recommendations for further countermeasures by the Canadian government?

Dr. Ahmed Al-Rawi: Sorry, Mr. Chair, with regard to the Russian mission?

Mr. Alistair MacGregor: The Russian missions and diplomatic posts in Canada and their role in spreading disinformation.

Dr. Ahmed Al-Rawi: Because of freedom of expression and freedom of speech, I think it's important to at least flag these efforts and to talk about what the Russian embassy is doing in the public domain. I've already written a piece that I hope will be published soon on The Conversation website.

We cannot ban what is going on but at least flag what is happening and debunk, fact-check these claims and at least warn Canadians not to be enticed or drawn to this type of propaganda. It's the only thing we can do, I believe.

● (1245)

Mr. Alistair MacGregor: Thank you very much.

Dr. Cooley, I'd like to turn to you. In your opening remarks you were talking about the new Russian exiles, journalists, IT workers, academics, and you were asking an open question of how we can enhance and strengthen these networks. The expression that came to mind as you were speaking was that “the best defence is a good offence” and I wonder if we are strengthening these groups to learn more about how Russian society functions, the different power structures that sustain Putin, and possibly launching counteroffensives.

I would just like to invite you to maybe further expand on that subject because I know five minutes is not a lot of time in your opening remarks.

Dr. Alexander Cooley: Thanks so much.

The presence of exiled Russian media is not new; it's just being magnified now because of this sort of conflict. We've had very effective Russian investigative reporters doing work on Putin's corruption, holding investigations of Yevgeny Prigozhin and what he's been doing in Africa. Dossier and Proekt, these organizations that are based overseas expose some of the most devastating inner secrets. In fact, a New York Times reporter, when he reported on Prigozhin, had much of the same information that these Russian exile reporters reported months before.

First of all, we can support them financially. Groups like Meduza, like Nexta—let's not leave Belarus out of here—have been so key in mobilizing against Lukashenko. Certainly, TV Rain, which is now shut down in Russia and is operating from outside, is one.

We have to anticipate what's going to be, at some point, the Russian reaction to this, which is to engage in more transnational repression. I will say that transnational repression is the kind of systematic targeting of political opponents, journalism, civil society, business community, of co-nationals overseas. Actually, this use of disinformation against diaspora communities is one aspect of this. It could also be actual attempts at assassination, rendition, coercion, or intimidation of family members.

The Russians are going to have a real problem because they're going to see all of these communities increasingly engaged to break down this disinformation wall and they are likely to target them. We need to be aware of how we can protect them, not only by supporting them, but also by realizing the status that these exiles and diasporas have as communities of interest of the crimes.

Mr. Alistair MacGregor: Thank you, Dr. Cooley.

You're always welcome to send the committee a submission if you want to go into further detail on some of the specifics. I would invite you to do that.

I have a final question for Mr. David Perry.

Our committee's mandate is very much on national security and public safety within the borders of Canada. I don't want to get caught up in the military side of things, but when you look at our cybersecurity and the role that CSE plays under National Defence, but also CSIS and the RCMP under Public Safety Canada, do you have recommendations as to whether Canada needs a way to reorganize how those agencies functions?

Is there anything pertinent that this committee can make as a recommendation to the Government of Canada?

Dr. David Perry: Thank you.

I think there's a lot of room to expand our collaboration between the government and the private sector. We should have an ability to leverage what is our real national strength in our cybersecurity and high-tech sector to find a better synergy between.... There's too much of a silo approach that we have right now. More collaboration would be helpful.

Mr. Alistair MacGregor: Thank you.

The Chair: You have 10 seconds left.

Mr. Alistair MacGregor: I'll send the 10 seconds back to you, Mr. Chair.

The Chair: Thank you.

I'll move right into the second round of questioning and invite Ms. Dancho to begin a five-minute round.

The floor is yours.

Ms. Raquel Dancho: Thank you, Mr. Chair.

Thank you to the witnesses for being here.

My questions are for Mr. Perry concerning procurement.

We hear a lot about difficulties of getting money out the door in DND. There have been a lot of promises made to buy frigates, planes and various defensive capabilities for Canada in order to defend itself against any sort of threat posed by Russia or other state actors.

How critical is it that we fix procurement and how would you recommend we go about doing so?

● (1250)

Dr. David Perry: I think it's fundamental because that's the way that we basically develop our ability to respond, whether or not that's for defence specifically or many of the other aspects of national security. You certainly need good human capital, but, fundamentally, those people need tools, and the procurement system is the way that we give them the tools to do their jobs, whether these are airplanes, ships or computer systems.

There's a whole range of issues with our procurement system, but I think, fundamentally, to the point of my opening remarks, we need to decide how important this is to us. Is procuring this type of equipment and gaining this kind of capability—again, whether it's for defence or other agencies in the national security community—something that matters to us? If so, how much relative to all of the many other priorities of government? That's part one.

Part two is that we need to calibrate better what we're doing with the workforce and the amount of work required to do it against the human capital available to us. You need resources, both financial and human, to get all of this done, and I don't think that match has been calibrated appropriately for about a decade and a half now. Until we fix that, we can't really expect to see much of a different result.

To be fair, successive governments have increased how much we are spending on this kind of procurement, and that's gone up progressively over the last 15 years. We're now spending more money on this than we have at any point, by my math, since basically the Korean War, if you adjust for inflation. The problem, though, is that we took a decade and a half off doing any of this, so the requirements to catch back up to a status quo level are far in excess of what they would have been if we had stuck to a regular spending pattern over time.

Beyond that, there's a whole number of other issues with the procurement system, from conflicting government priorities and some of the institutional structure, but I'll stop there.

Ms. Raquel Dancho: Can you elaborate a little bit on making the commitment to improve procurement? We're hearing a lot about this, and I'm just trying to understand for Canadians what exactly that means. Is it a signal that government needs to be send within cabinet or to the public? How would the Prime Minister communicate such procurement and that improving it is a priority?

Dr. David Perry: I think there are two broad ways. There are written, formal statements or speeches, but also commitments of time. I think you can point to examples. The indigenous file has been one where the current Prime Minister has indicated that the file matters very much to his government. I don't think it's any accident that we've seen spending on that particular file over the last several years effectively double, which is a remarkable increase in a short amount of time. Talking about the huge increase in the financial commitment to that particular file, that was clearly communicated to all ministers in the 2015 mandate letters and remains in the current version of those mandate letters today.

If we want to see an equivalent type of change in output or outcomes on the procurement file or on defence/national security writ large, you need to see that type of a commitment of government to identify that as a key set of activities and priorities that they're looking to see progress on. Absent that, procurement officials, other officials and other department agencies will take their cue that other things simply matter more and focus there first.

Ms. Raquel Dancho: In the upcoming budget, what are you looking to see on the procurement side? From what you're sharing, it sounds like we need not only investment in the tools to defend Canadian territory and the Canadian people but also human resources in the procurement area. Are you looking in the upcoming budget for a direct indication that this government is investing more in procurement for human resources?

Dr. David Perry: Whatever new financial level we potentially move to in terms of defence spending— with presumably a big component of that being oriented around procurement, given some of the needs that have been articulated for continental defence and the modernization of NORAD—if we want to see that money move out the door in, say, a short number of years rather than multiple decades, you need to make a commitment to increase and provide the capacity to ensure that those funds get spent by the end of each fiscal year. Otherwise, they won't.

Ms. Raquel Dancho: A good indicator to do that would be—it sounds like from what you're saying—a very strong indicator from the Prime Minister, whether in mandate letters to all of cabinet or in their general communications, that procurement must be a top priority. Is that correct?

Dr. David Perry: Yes, I think it's critical to identify that as a key priority of the government going forward.

● (1255)

Ms. Raquel Dancho: Thank you very much.

The Chair: Ms. Damoff, we'll go over to you for a five-minute line of questioning. The floor is yours.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you so much, Chair.

Thank you to all three of our witnesses.

My first question is for Dr. Al-Rawi. We've talked about disinformation on social media, but we haven't really touched on platforms that aren't quite as common as Facebook, YouTube and Twitter. I'm thinking of platforms like Telegram and Gab, where their position is to appeal to extremist or fringe discussions.

Could talk about the impact of that in terms of Russian interference? Also, are there any recommendations you could make to the government on these less well-known platforms?

Dr. Ahmed Al-Rawi: Thank you, Mr. Chair.

A few years ago, a few [*Technical difficulty—Editor*] in United States and elsewhere were de-platformed from mainstream social media, like Facebook and Twitter, including former President Trump and many conspiracy theorists like Alex Jones and so on. This actually led to what they call a “migration” to new, alternative outlets, including the ones you mentioned, Telegram, Discord, and a few other ones. Some of them unfortunately are even based in Canada. What we have today is platforms that are dominated by conspiracy theories and disinformation.

In our study about the convoy protest, we found that Twitter contained very few conspiracies in relation to the protest and that the dominant discourses or conspiracies were actually elsewhere, specifically on Telegram.

The major problem I am seeing is that the big search engines like Google have indexed Telegram. When I search for a message posted by Alex Jones on Telegram, I can't actually find it. I think that's the major problem. I do not think we can moderate these small platforms because it's like playing whack-a-mole—if you try to silence one of them, four others will emerge, because this is a thriving business for them. They are actually profiting by probably billions of dollars, not millions.

I don't think there is a way to completely stop these smaller social media platforms. What we can do is pressure the big search engines to index these sites less so that searching for a specific comment will be hard.

Ms. Pam Damoff: That would have to do with the algorithms they use as well.

Thank you. I'm sorry to cut you off. Time is limited at the committee.

Professor Cooley, I have a question for you. You were recently quoted in a Hill Times article talking about how we need to move beyond sanctioning financial facilitators of Russia and target western proxies of Russian funding.

I'm wondering if you can talk about how these Russian proxies and management firms that provide their services to Russian elites are influencing cybersecurity and what recommendations you would make to the government in terms of dealing with that influence.

Dr. Alexander Cooley: You're talking about how they're influencing cybersecurity?

Ms. Pam Damoff: You wanted them sanctioned. I guess it would actually be in terms of national security.

Is there—

Dr. Alexander Cooley: It would be national security, yes. Thank you for that.

What we had prior to the war was the compartmentalization of issues into two streams. One was that we used to think about national security issues in terms of classic objectives and foreign policy. The other one was sort of the realm of domestic politics. Or when we talked about kleptocracy or counter-kleptocracy, that was very much viewed as sort of a niche governance issue. Now we've seen how the two relate to each other.

The question isn't just about the specific oligarchs to go after, who have ties to the Kremlin, like Abramovich or Usmanov or Sechin or Deripaska; it's rather about looking at our own professional industries. How is it that we have industries like real estate brokers, lawyers, shell company providers and reputation management firms that perfectly legally can offer these services, which all amount to the same thing—anonymizing the source of this wealth in a manner that is legal and turning it into property or social capital that enhances the status and standing of these oligarchs?

That's not just a Russian oligarch—

● (1300)

The Chair: Thank you very much.

I would now like to invite Ms. Michaud for a two-and-a-half-minute block.

The floor is yours when you want to take it.

[*Translation*]

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

Mr. Cooley, based on your knowledge of Russia, do you believe that Canada is prepared to deal with some strategies of intimidation or interference from that country? According to the Canadian Centre for Cyber Security's "National Cyber Threat Assessment 2020", it is very likely that state-sponsored cyber threat actors will secretly pre-position themselves in Canadian critical infrastructure for attack or intimidation.

Given the current situation in Ukraine, how likely is it that Russia will intentionally or unintentionally cause damage to our critical infrastructure?

[*English*]

Dr. Alexander Cooley: I would say that the probability is high. The more groups of exiles or diasporas that exist in a particular country or community that are viewed as oppositional to the sending authoritarian country, the greater the likelihood of digital surveillance, digital intimidation and then actual physical intimidation. This isn't just a Russian issue. You also have experience of this, for example, with Chinese agents operating within Canadian territory. This is a broader phenomenon of the extraterritorial reach of authoritarians and how information technology enables that.

I do think that making sure that these particular diasporas, these particular vulnerable groups, understand their own role here and the sort of digital citizenship involved...but I think for sure you can expect that the transnational dimension here will become another battlefield for Russia. It has been for the last 10 years.

[*Translation*]

Ms. Kristina Michaud: Still, this is particularly disturbing. Is Canada prepared to deal with this and protect infrastructure, institutions, businesses and citizens? This is all changing extremely quickly. Is our protection system up to date?

[*English*]

Dr. Alexander Cooley: I think that's something that you probably are in a better position to answer than I am regarding Canada. I do think that getting all different kinds of agencies on the same page to realize that it's a national security issue should be the priority here. That includes—

The Chair: Thank you very much.

Dr. Alexander Cooley: —asylum hearings.

The Chair: Thank you.

I'd like to move to Mr. MacGregor.

Sir, you have two and a half minutes. The floor is yours.

Mr. Alistair MacGregor: Thank you, Chair.

Dr. Cooley, I'd like to continue on the subject of the western agencies and individuals who have provided perfectly legal aid to Russian oligarchs so that they can manage their assets here in a perfectly legal way. They've used Canadian law to set up shell companies. They've invested significantly in real estate. I know that the U.K. probably has a much deeper problem with that than we do, but Canada is not immune to that.

There was a pledge in the last election to set up a federal financial crimes agency. The Minister of Public Safety's mandate letter instructs him to speed up work to establish a dedicated unit to investigate this. Do you want to take a minute and a half to expand on the financial aspect of this issue that we're looking at? Does it in any way link to Canada's national security? Is this something that our committee should be focusing on when we make recommendations to the government?

Dr. Alexander Cooley: Yes, I do believe it does influence national security, especially because we've seen the outsized influence that so-called oligarchs or politically important persons with this extreme wealth have. They can influence certain political party positions. They can influence certain national campaigns. Through media contacts they can set certain agendas. Of course, they can intimidate reporters to prevent them from looking into their own origins of wealth.

I actually think that the move to a federal beneficial ownership registry is an absolute national security requirement. Whether this is 2025 or 2023, it should happen as soon as possible. I think every country needs to know what the anonymous shell companies are and who's behind them that are buying luxury real estate but also other assets. I think any time you put the norm of privacy, and my client's privacy, against transparency—

● (1305)

The Chair: Thank you.

Dr. Alexander Cooley: —I think you're on the losing side.

The Chair: Thank you very much.

I'm going to cut the last two speakers to two minutes each, which will take us inside the extra time that the clerk has been able to negotiate for us.

Mr. Lloyd, take two minutes, please.

Mr. Dane Lloyd: Thank you, Mr. Chair, for this unexpected time.

Professor Cooley, we're talking a lot about misinformation. I'm wondering if you're aware of and can comment on the well-documented misinformation campaign in the 2021 federal election.

Dr. Alexander Cooley: I'm sorry. Which election did you say?

Mr. Dane Lloyd: The last federal election, the 2021 federal election.

Dr. Alexander Cooley: No. That's not my area of expertise.

Mr. Dane Lloyd: Mr. Al-Rawi, there was a social media.... I forget. I believe it was WeChat. Is this another tool that's being used that is of concern for misinformation?

Dr. Ahmed Al-Rawi: I would start with Dr. Cooley about the attempts of foreign states to influence immigrant or diasporic groups in Canada. This has been an ongoing issue, so the WeChat thing is there. Definitely, there is clear evidence and an indication that the Chinese government has been and is still trying to influence the Chinese community living in Vancouver and elsewhere.

The same applies to other states. For example, the Iranian government is very active in doing the same thing regarding the Iranian communities living here in Canada. This is an ongoing issue. They usually target or make use of specific tools, let's say—

Mr. Dane Lloyd: Thank you.

Can you give us some examples, from your experience, of how that worked out in the 2021 federal election?

Dr. Ahmed Al-Rawi: In the 2021 election, WeChat was a clear sign of this kind of interference. There are so many other gaps that we do not fully understand.

One thing that I really like to highlight is the importance of studying ethnic Canadian media. For example—

The Chair: Thank you very much. I'm sorry that we don't have more time.

Mr. Zuberi, you have two minutes to take us to the end of this panel.

Mr. Sameer Zuberi (Pierrefonds—Dollard, Lib.): Thank you, Mr. Chair.

Thank you to all the witnesses.

I'd like to start with Dr. Al-Rawi. You spoke about Russian bots and misinformation. Can you let us know if the bots were trying to advantage any individuals or advantage any issues, or disadvantage any issues, aside from what you've already discussed and shared with us?

Dr. Ahmed Al-Rawi: Thank you, Mr. Chair. I assume the question is about today, and the misinformation that happened today.

Mr. Sameer Zuberi: Yes.

Dr. Ahmed Al-Rawi: Thank you very much.

Scientifically, I cannot prove these are bots, because bots are automated accounts. What I have seen is some kind of organic users, which means real users spreading propaganda. Most of the propaganda I have seen so far about the war on Ukraine is related to supporting the position of the Russian government and sending a lot of what we call confusing messages, again, to blur our idea of what is happening and to confuse people.

I think they are really on top of the game, because they are very fast in making this kind of disinformation and spreading it. Unfortunately, we are late.

Mr. Sameer Zuberi: Can I ask you if the disinformation is in both English and French? Is it in any other languages aside from those two?

Dr. Ahmed Al-Rawi: With regard to the Russian diplomatic mission, it's mostly in English, but there is evidence that it's in French.

I've never looked at the Telegram channel WarOnFakes.com. They have a huge Telegram channel, which is now one of the most popular in Russia. Now the targets will also be—

● (1310)

Mr. Sameer Zuberi: In the 45 seconds that are left, what are the impacts of disinformation? You mentioned diversity, inclusion, refugees, Muslims and others.

What are the real impacts on these communities for the disinformation campaigns you mentioned?

The Chair: You actually have 10 seconds.

Dr. Ahmed Al-Rawi: It's trying to make people mistrust what is legitimate. That includes multiculturalism.

The Chair: Thank you very much.

That completes the time that's available and then a bit more.

On the committee's behalf, I would like to thank the witnesses for a fascinating hour and change. There was a very complex and important set of questions and subjects.

With that, I would seek permission of the committee to adjourn the meeting.

Some hon. members: Agreed.

The Chair: I think I have it.

Witnesses, thank you so much for your time and your insights.

We'll see everybody on Thursday morning.

This meeting is now adjourned.