HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

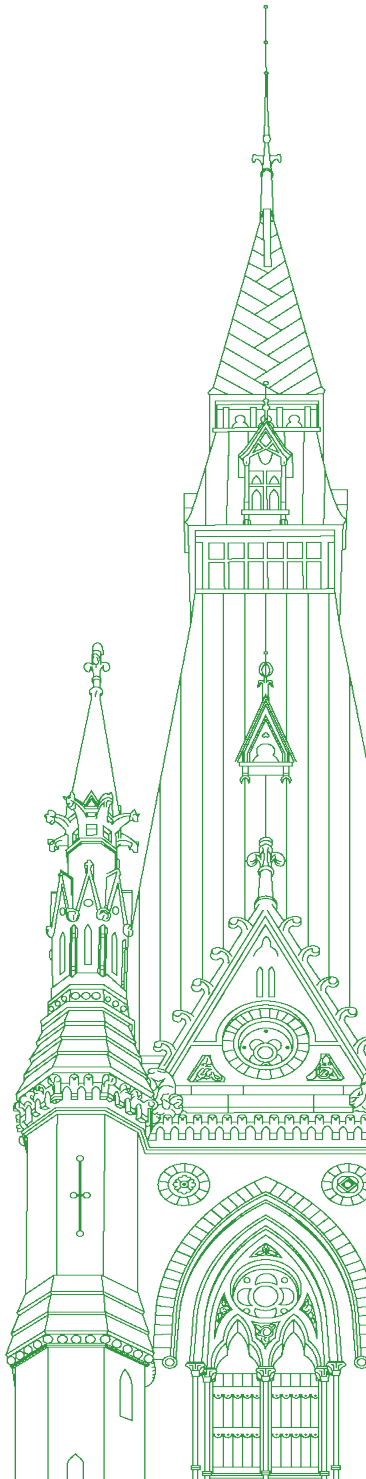
44th PARLIAMENT, 1st SESSION

Standing Committee on National Defence

EVIDENCE

NUMBER 048

Tuesday, February 7, 2023



Chair: The Honourable John McKay

Standing Committee on National Defence

Tuesday, February 7, 2023

● (1540)

[*English*]

The Vice-Chair (Mr. James Bezan (Selkirk—Interlake—Eastman, CPC)): I call this meeting to order.

We're here at meeting 48. We welcome here today the Communications Security Establishment, CSE, for the first part of our study on cybersecurity and cyberwarfare, pursuant to Standing Order 108(2).

I'm not going to be able to give us the full hour because we're starting 10 minutes late, so we're going to do 55 minutes in this round and 55 minutes in the next round with our next set of witnesses.

Joining us for the first hour, we have Sami Khoury, who is the head of Canadian centre for cybersecurity; and Alia Tayyeb, who is the deputy chief of signals intelligence at CSE.

I will open up the floor. You have seven minutes between the two of you to bring forward your opening remarks.

Mr. Sami Khoury (Head, Canadian Centre for Cyber Security, Communications Security Establishment): Thank you, Mr. Chair and members of the committee, for the invitation to appear today.

My name is Sami Khoury. My pronouns are he and him. I am the head of the Communications Security Establishment's Canadian centre for cybersecurity, known as the cyber centre.

I am joined today by my colleague, Alia Tayyeb. She is the deputy chief of CSE's signals intelligence branch.

[*Translation*]

I'm glad to appear before the committee to discuss cybersecurity and cyber operations.

[*English*]

As this is the first meeting of your study, I'd like to begin by providing an update on the current cyber-threat landscape and what CSE is doing to protect Canada and Canadians. I will largely focus on the cybersecurity aspect of our mandate, whereas my colleague, Ms. Tayyeb, will focus on the foreign intelligence piece of CSE's mandate, our support to partners, and our active and defensive cyber-operation capabilities.

Now, more than ever, we understand that cybersecurity is the foundation of Canada's future: for our digital economy, our personal safety and privacy, and our national prosperity and competitiveness. In October, the cyber centre released its third national cyber-threat assessment. This report outlines the current cyber-threat environment.

[*Translation*]

One of the key points in the report is that cybercrime remains the largest cyber-threat to Canadians and that critical infrastructure is the main target of cybercriminals and state-sponsored threat actors.

[*English*]

Ransomware, specifically, was prominent in the past two years, and it remains a persistent threat to Canadian organizations. The state-sponsored cyber-programs of China, Russia, Iran and North Korea continue to pose the greatest strategic cyber-threat to Canada. In the face of these threats, and as Canada's technical and operational authority on cybersecurity, CSE defends Government of Canada networks and the cyber centre leads the government's response to cyber-incidents. However, cybersecurity is not solely a federal government responsibility or concern, as cyber-threats continue to target and impact Canadian individuals and organizations.

[*Translation*]

CSE works with partners in the industry, including those outside government, sharing information about threats and best practices in cybersecurity. The Canadian Centre for Cyber Security regularly publishes guidance and expert advice for Canadians.

[*English*]

Moving forward, to continue to adapt to the evolving threat environment, bolster defences and help better protect Canada and Canadians, we hope to see the continued progress of Bill C-26, an act respecting cybersecurity, in Parliament. This legislation would establish a regulatory framework to strengthen cybersecurity for services and systems that are vital to national security and public safety and give the government a new tool to respond to emerging cyber-threats.

We also look forward to continued work to support public safety in the renewal of Canada's national cybersecurity strategy. The renewed NCSS will articulate Canada's long-term strategy to protect our national security and economy, deter cyber-threat actors and promote norms-based behaviour in cyberspace.

[*Translation*]

For CSE, the renewal of the strategy provides an opportunity to review the situation and build on what the Canadian Centre for Cyber Security has achieved over the past five years. The creation of the centre was actually one of the main initiatives set out in the National Cyber Security Strategy, developed in 2018.

[*English*]

Finally, as we work to build relationships with Canadian industry and other levels of government, we are also focused on collaboration with our international partners, in the Five Eyes and beyond.

I will now hand it over to my colleague, Ms. Tayyeb, to speak to her area of responsibility.

Ms. Alia Tayyeb (Deputy Chief of Signals Intelligence (SIGINT), Communications Security Establishment): Thank you, Sami.

As my colleague noted, I am the deputy chief of CSE, signals intelligence branch, and I'm also responsible for the foreign cyber-operations aspect of the CSE mandate. My pronouns are she and her.

As mentioned, the severity of cybercrime and cyber-incidents targeting Canadians and Canadian critical infrastructure, both public and private, is growing exponentially. Beyond cybercriminals, however, state and state-sponsored cyber-actors also pose a continuing threat to Canada. Through CSE's foreign intelligence mandate, we continue to provide intelligence on foreign cyber-threats, including the activities and intentions of state and non-state actors, which is used by government clients, including the cyber centre, to defend Canada.

Recognizing the evolving threat landscape, the CSE Act came into force in August 2019, which allowed CSE to expand its tool suite to conduct active and defensive cyber-operations, together referred to as foreign cyber-operations.

● (1545)

[*Translation*]

Since being granted these new powers, CSE has leveraged its cyber operations capability to hinder the efforts of foreign-based extremists seeking to recruit Canadians, to carry out online campaigns and to disseminate violent extremist content.

[*English*]

We have also used these authorities to disrupt the activities of cybercriminals planning ransomware attacks.

Recognizing the importance of investing in cyber-resilience and bolstering Canada's capability, budget 2022 provided Canada's first stand-alone investment in its cyber-operations capability, earmarking $273.7 million over five years and $96.5 million ongoing annually for CSE to build its foreign cyber-operations capabilities and conduct a specific range of cyber-operations focused on countering cybercriminals and protecting Canadian critical infrastructure from cyber-attacks.

[*Translation*]

Further to CSE's role of providing assistance, CSE has also used its capabilities to support the Canadian Armed Forces in carrying out its mandate.

Our allies, international partners and adversaries all invest heavily in their capabilities, working to build broad-based cyber operations capacity. It goes without saying that CSE monitors cyberspace closely to ensure a responsive approach in protecting Canada and defending its interests.

[*English*]

As the cyber-threat landscape in Canada continues to evolve, CSE is dedicated to advancing cybersecurity and increasing the confidence of Canadians in the systems they rely on daily.

With that, I thank you for the opportunity to appear before you today, and I look forward to answering any questions you may have.

The Vice-Chair (Mr. James Bezan): Thank you for your opening remarks.

We'll kick off the first round of six-minute questions.

Ms. Gallant.

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

I'd like, first of all, to put a motion on notice. I believe the motion will be distributed. It is:

> That the Standing Committee on National Defence invite the Minister of National Defence, the Hon. Anita Anand and the Deputy Commander of NORAD, Lt. General Alain Pelletier, to provide a briefing of no fewer than two hours concerning the foreign airship from the People's Republic of China that recently violated Canadian airspace, and that the briefing be held in public within the next four days.

The Vice-Chair (Mr. James Bezan): Okay, that is on notice.

You have the floor. You have five and a half minutes left.

Mrs. Cheryl Gallant: Mr. Chair, through you to CSE, how and when was CSE made aware of the Chinese balloon in our airspace?

Ms. Alia Tayyeb: As the minister said over the weekend, she indicated that we've been working very closely with our U.S. allies on this matter, particularly through NORAD, which had been tracking this high-altitude balloon and monitoring its activities since last weekend, I believe.

However, I think it would be better placed for the CAF to answer more specifics on that question.

Mrs. Cheryl Gallant: Has the CSE been made aware of similar instances or incursions in the last 10 years?

Ms. Alia Tayyeb: From the balloons...?

Mrs. Cheryl Gallant: That's correct.

Ms. Alia Tayyeb: I'm unsure about how to answer that question at this time without getting into what could be intelligence or operational details, so I would have to defer to my Canadian Armed Forces colleagues on this question.

Thank you.

Mrs. Cheryl Gallant: Did the CSE play a role in electronic warfare or blocking or jamming the devices attached to the spy balloon?

Ms. Alia Tayyeb: Again, I apologize that I am not able to answer your question. I hope you can understand that, in matters of intelligence and operations, I wouldn't be able to provide any further details on this question.

Thank you.

Mrs. Cheryl Gallant: Okay, let's get back to the first question that was answered. When exactly did the CSE learn of the Chinese balloon in Canadian airspace?

Ms. Alia Tayyeb: I wouldn't want to provide you with an incorrect answer, so if you'll permit me, I could verify that information exactly and return to the committee.

Mrs. Cheryl Gallant: I'm not interested in when the armed forces.... I'm interested in when CSE first learned of its existence.

Ms. Alia Tayyeb: My understanding is that it was sometime over the last...two weekends ago. I'd have to get the exact date for you, but I'd rather be precise and return to you with a more detailed answer.

● (1550)

The Vice-Chair (Mr. James Bezan): If you could return in writing with that answer, we'd appreciate it.

Thank you.

Ms. Alia Tayyeb: Absolutely.

Mrs. Cheryl Gallant: How did the CSE learn of it? Was it with its own equipment, or was it notified by another part of the government, National Defence or NORAD?

Ms. Alia Tayyeb: Again, just to be absolutely precise and not to mislead anyone at the committee, if I could return to you in writing on that question, it would be very much appreciated.

Mrs. Cheryl Gallant: Okay.

Given the unknown nature of the payload of the Chinese balloon, whatever it was carrying, was there an additional risk to cybersecurity or of cyberwarfare that was or was not addressed by the CSE?

Ms. Alia Tayyeb: What I can say is that we do work very closely with our U.S. allies in addition to the Canadian Armed Forces and all other Canadian agencies who would have been monitoring this event. We would be monitoring for any risk to Canadian information, Canadian assets or Canadian infrastructure in partnership with those agencies.

Mrs. Cheryl Gallant: You haven't clarified how you found out, but if CSE learned of the balloon in the same way most Canadians did—through the news—how would you advise changing any of the protocols related to incursions into Canadian airspace?

Ms. Alia Tayyeb: I very much appreciate the question. I think it's an extremely important one.

I don't think that I'm the best placed to answer that question, given that I think the Canadian Armed Forces would be best placed to handle questions of that nature.

Mrs. Cheryl Gallant: Is CSE concerned about the ongoing research partnerships between Canadian universities and China's National University of Defense Technology, recently reported on in The Globe and Mail?

Ms. Alia Tayyeb: Indeed, as part of our foreign intelligence mandate, we do report on any foreign adversary activity that is directed towards Canadians, including approaches to our research work or intellectual property or economic investments, so that is absolutely a topic that we would be monitoring and reporting on to our government clients.

Mrs. Cheryl Gallant: How did you learn about the July 8 network-wide Rogers outage?

Ms. Alia Tayyeb: I think I would best turn that one over to my colleague, Sami.

Mr. Sami Khoury: Thank you for the question.

We monitored. We have good partnerships with all of the telecom operators, and shortly after the outage, we were in touch with Rogers to ascertain the nature of the outage.

Mrs. Cheryl Gallant: Did you call to ask, or did they initiate the conversation to let you know what was happening?

Mr. Sami Khoury: I called to ask.

Mrs. Cheryl Gallant: Okay.

The Vice-Chair (Mr. James Bezan): Ms. Lambropoulos, you have the floor.

Ms. Emmanuella Lambropoulos (Saint-Laurent, Lib.): Thank you, Chair.

Thank you to our witnesses for being here to answer some important questions with us today.

I understand that CSE is working with its partners in Ukraine in order to determine whether there are cyber-threats, if cybersecurity—

The Vice-Chair (Mr. James Bezan): Excuse me; we don't have interpretation. I've stopped the clock.

[*Translation*]

Ms. Christine Normandin (Saint-Jean, BQ): Mr. Chair, could you ask the member whether she's wearing the right headset?

We just received a directive from the House of Commons asking us to make sure we wear the proper headset in order to protect the health and safety of the interpreters.

[*English*]

The Vice-Chair (Mr. James Bezan): Ms. Lambropoulos, is that the correct headset that's been issued by the House of Commons? It is.

Can you just wrap it naturally around in front of your face? Try that, please.

Ms. Emmanuella Lambropoulos: Does this sound better and clearer?

The Vice-Chair (Mr. James Bezan): No. They're giving me a thumbs-down.

Ms. Emmanuella Lambropoulos: Can we pass it to another colleague? I'll try to get to a space that's a little bit easier to hear from.

The Vice-Chair (Mr. James Bezan): Okay, I appreciate that.

Ms. O'Connell, you can have the six minutes.

● (1555)

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

Thank you to our witnesses for being here.

I think the work that CSE does is really important, and most Canadians probably don't even realize the quality of our services here and the technology. I appreciate the opportunity to hear a little more and share with Canadians a little more about some of the work you do.

Some of the issues that are very topical, of course, in the media are private sector ransomware attacks. Where I'm from, outside of the GTA, SickKids hospital was in the news for sure, and we had a lot of reporting on that. Could you maybe speak to the process or what role CSE can play when there's a private sector non-governmental ransomware attack and how you try to work with clients, or the mandate or non-mandate you have in dealing with private sector attacks?

Mr. Sami Khoury: Thank you for the question. I'm happy to speak about that.

Regarding ransomware, when we issued our third national cyber-threat assessment, we continued to highlight the threat that ransomware poses to Canadians and Canadian organizations. It's a serious threat, as we can see in the health care sector, in critical infrastructure, in businesses and so on.

There are a number of ways that we work with the private sector to mitigate or to address the threat of ransomware. We constantly publish alerts and cyber-flashes to draw attention to what may be new vectors of ransomware or new techniques that cybercriminals are using in ransomware.

Every time we have an opportunity to speak to a business community, we speak about the threat of ransomware. Sometimes we get tips if our partners have seen precursors of ransomware being deployed in Canada, and we will tip the organization and tell them that they might want to look here because we have information to indicate that there might be a precursor to ransomware.

Unfortunately, sometimes we either hear through the media that there was ransomware, that a certain organization has fallen victim—

Ms. Jennifer O'Connell: I'm sorry. I don't mean to cut you off. I'm just limited in time.

Following up on that, is there any requirement for the private sector, for example, to notify the Canadian government of something. I could see that some businesses might not want to share that they've been vulnerable. Is there any sort of requirement? What do you do in that event? Is there something you can recommend to this committee as we take on this study in that area?

Again, you have my apologies for interrupting. I'm just limited in time.

Mr. Sami Khoury: Thank you. There is no requirement for the private sector to report to us ransomware incidents, and many of them don't report it. As a matter of fact, in 2021 we've only had reports of about 300 ransomware incidents to the cyber centre, which is probably under-reporting for a number of reasons.

As soon as we hear of an incident, we reach out to offer our assistance. Sometimes it's accepted, but more often it's declined.

Ms. Jennifer O'Connell: Thank you.

Following up on that, critical infrastructure is an area of particular importance. As my colleagues here know, I was in municipal government before and looking back at my role there, we really were not briefed. Municipalities or regional municipalities often hold a lot of the responsibility over water systems and critical infrastructure—it might be bridges in some cases—depending on the jurisdiction.

What work is being done to ensure all orders of government have the proper training or tools needed within their organizations to even be aware of what the threats might be, since they often hold the responsibility or authority over critical infrastructure?

Mr. Sami Khoury: Thank you for the question.

We have a number of programs or regular engagements with various critical infrastructure sectors, including municipalities. We hold regular calls with them. I personally get invited to speak at their annual events or at their conferences to share with them the latest threats that we are aware of, that we are seeing or that are affecting them.

We do have an outreach program with our partnership team, which is constantly out there talking to municipalities, to critical infrastructure operators, to the health care sectors and so on, to try, as much as possible, to make them aware of the services of the cyber centre.

● (1600)

Ms. Jennifer O'Connell: Thank you.

Just quickly, in terms of talent retention, CSE would be competing with cyber and technological experts—

The Vice-Chair (Mr. James Bezan): I will just pause you for a quick minute. We're getting French interpretation on the English channel.

Okay. Please try again.

Ms. Jennifer O'Connell: Thank you.

Just on retention or recruitment, I would assume we'd be competing in this space with Silicon Valley, etc. What is the strategy to ensure we continue to retain and recruit the best talent in this space?

Mr. Sami Khoury: Thank you again for this important question.

Recruitment is challenging, and it's a highly competitive space out there. We are trying to hire for a number of positions, for a variety of positions, and to ensure that we hire Canadians who represent the rich and diverse society in which we live.

Currently we are modernizing our multidisciplinary recruitment effort to attract the top talent and investing in a student program and a co-op program to make sure that our talent pool is rich. We are very engaged in communities to raise cybersecurity awareness in presentations to students to get them interested in the STEM field and are also investing in the retention of our current workforce. We have been named as a top employer three years in a row.

The Vice-Chair (Mr. James Bezan): Your time has expired.

[*Translation*]

Ms. Normandin, you may go ahead for six minutes.

Ms. Christine Normandin: Thank you, Mr. Chair.

Ms. Tayyeb and Mr. Khoury, thank you for being here.

My questions are along the same lines as Ms. O'Connell's.

Can you tell us about the similarities between what you do and what the Canadian Armed Forces does? We've heard from witnesses that there are problems.

My question is about human resources.

Does the challenge of recruiting people and the fact that the private sector is such a competitive employer create risks when it comes to security?

Mr. Sami Khoury: We are very mindful of the challenges associated with the current employment landscape. We endeavour to attract talent from all over Canada. We do not focus only on the national capital region. We try to hire people from all over the country with expertise in different areas. We also try to hire students, including those doing co-op placements. It's not only professionals who join our organization. We have employees who bring a lot of talent to CSE. That's where we are focusing our efforts.

We are also exploring the possibility of hiring people willing to live in regions in order to support cybersecurity activities. We aren't just hiring people willing to move to Ottawa. People can provide support locally.

Ms. Christine Normandin: Thank you.

I would be remiss if I didn't ask about the hot topic, McKinsey & Company. We've talked a lot about that firm in recent weeks. We've also talked a lot about IT and other services being contracted out to various private firms.

Does CSE engage in similar contracting?

If so, how do you ensure those services are delivered securely, knowing how many clients those firms have?

Mr. Sami Khoury: Thank you for your question.

To my knowledge, we don't have any contracts with that firm. I can send you more information in writing after the meeting, if you'd like.

As far as the security of contracts is concerned, each department is responsible for safeguarding its data. Our job is to establish security standards for various contracts, but not individually. Departments are responsible for adhering to those standards.

I hope that answers your question.

Ms. Christine Normandin: If I understand correctly, your organization doesn't have a contract with McKinsey & Company, specifically.

Do you have contracts with other firms, then?

Mr. Sami Khoury: As far as I know, we don't have contracts with other firms. Again, I'd be happy to follow up in writing.

● (1605)

Ms. Christine Normandin: I'd appreciate that. Thank you.

From time to time, you conduct defensive cyber operations, and that requires ministerial authorization. How quickly are you able to get that authorization?

Is there anything that would make the process more efficient and help you respond more quickly, for example, when you're dealing with issues related to a certain situation?

Ms. Alia Tayyeb: Thank you for your question.

We are always looking for ways to improve how we do things. We recently made a programming investment, and mainly, that helped us improve our ability to work with our foreign affairs colleagues. They play a very important role in our approval process.

[*English*]

I think what's important here is that we work very closely with our colleagues, both in the cyber centre and at Global Affairs Canada. They are responsible, with us, for providing assistance and advice in terms of our operational planning. However, we have been able to respond very quickly to threats as they have emerged.

[*Translation*]

Ms. Christine Normandin: Thank you.

Other challenges facing the Canadian Armed Forces have to do with procurement and security clearances. It takes too long for the armed forces to acquire the high-tech equipment it needs for a specific project and too long for prospective employees to receive their security clearance. I'd like you to comment on those issues.

Mr. Sami Khoury: I can answer that. Thank you.

The pandemic certainly disrupted the supply chain, and we are having just as much trouble as other departments when it comes to acquiring electronics and networking equipment to build our capacity. We are mindful of that. We try to work with companies to speed up the delivery of certain products, but we are just as affected by the situation as their other clients.

[*English*]

The Vice-Chair (Mr. James Bezan): Ms. Mathyssen, you get the last six minutes in this first round.

Ms. Lindsay Mathyssen (London—Fanshawe, NDP): Thank you, Mr. Chair.

Thank you to the witnesses for being here today.

I wanted to pick up where Ms. Normandin was in terms of discussing those contracts. They are certainly on a lot of our minds as of late.

Mr. Khoury, in terms of that information, those recommendations that you make to a lot of those departments, government departments, critical infrastructure and those contractors who are handling specific information, delicate information, private information and sensitive data on behalf of government, how do you provide them with those best practices? How do you monitor how they follow that in each department?

You said that they have to do it themselves, but do you play a role at all in that provision and monitoring?

Mr. Sami Khoury: Thank you for the question.

We come up with the various information security standards that are out there: protected A, protected B, protected C. We communicate those standards. They are sort of promulgated through Treasury Board. With each of these levels of classification, departments are aware of what information is classified as protected B or protected C, or what is secret and what is top secret. The departments themselves have to live by those standards. We don't audit them per se.

Sometimes we get pulled into specific projects. At that point, we provide some security advice to the project and ensure that the information security of the project is commensurate with the classification of the information. We don't review on a contract-by-contract basis what information is being provided to the contractor. I'm talking about it from an IT perspective, because my primary concern is cybersecurity and IT security.

Ms. Lindsay Mathyssen: In terms of those private contracts, they would have access to delicate information. Other than the department monitoring itself, do you or CSE not see any potential problems with that within departments? Do they not have any obligation or accountability to report to you?

● (1610)

Mr. Sami Khoury: Each department has a departmental security officer. We have a community of those who meet on a regular basis. Treasury Board is the policy arm of our community. We would work with them to ensure that the information is promulgated as much as possible, but we don't go and audit departments to understand how it is that they are handling the information at the proper classification level.

Ms. Lindsay Mathyssen: Do you see that as a potential problem, though? This may be something we could recommend going forward, so that there is more communication between those departments and CSE or your centre specifically, in order to have better information on problems that could be happening across departments with sensitive information.

Mr. Sami Khoury: Thank you again for the question.

I think departments know how to reach out, whether it's to Treasury Board or to us, if there is any clarity being sought on what is the proper classification of information. I personally have been in a number of conversations where we talked about the level of the classification of the information at hand and what is the proper security profile that we need to apply to the IT system in order to protect that information. Those forums exist today, and those channels exist today.

Ms. Lindsay Mathyssen: Quite literally, it's in your name. You're the centre. You're supposed to be bringing a lot of this information together. My concern is that, for some of these contractors, if you were to see patterns, it would be more helpful, I would assume, but in terms of those companies who may be repeat violators of those best practices in terms of cybersecurity for those departments, would you be able to see those patterns?

Also, we have seen in the United States, for example, that a company like Deloitte has actually been seen to release very sensitive information. In 2017, in that massive data breach, for the Department of Defense, Department of Homeland Security, the State Department and the National Institutes of Health, they leaked passwords, IP addresses and sensitive information.

When you see that happening internationally and then those same companies are being used here in Canada across the board within our own government, do you provide any of that feedback or any of those warnings? Do you recommend not using those companies that have had these problems? Do you monitor that? Do you track that? Do you provide those recommendations?

Mr. Sami Khoury: Thank you again for the question.

I would defer to PSPC on anything that has to do with contracting. Our role is very much to review the security architecture sometimes, and we would work with them.

Departments have the responsibility to do the SA and A of their systems. They review the security accreditation of their systems, and we get involved in those accreditations. Before the system goes live, obviously if it contains sensitive information the department will have to accredit that it has met the security baseline that the cyber centre has established. Sometimes we are part of the project, so we get involved in that.

On repeat offenders and contracting issues, I would respectfully defer that to PSPC.

The Vice-Chair (Mr. James Bezan): We're going to have to cut it off there. We're slightly over on our time.

Ms. Kramp-Neuman, you have the floor for five minutes, please.

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

Thank you to the witnesses.

Here's my first question. Due to the competitive nature of cyber-employment opportunities, is it safe to assume or accurate to assume that the Canada security establishment struggles in acquiring employees with the actual skills that are required for cybersecurity and to combat cyberwarfare?

Ms. Alia Tayyeb: Maybe I could take that one from the beginning. It's a great question. It's something that we talk about a lot at CSE and the centre for cybersecurity.

We're lucky, in a way. Statistics-wise, we do have a great deal of interest in our organization. We have an interesting mission. A lot of people are interested in this topic. With our cyber centre taking a more public profile, we have certainly developed greater inroads into the public in terms of awareness and that has translated into a great deal of interest in working here.

We hire a variety of people from different technical fields; it's not all one type of profession. We have engineers, mathematicians, cybersecurity experts, etc. We also have a wide variety of jobs available.

Having said that, as Sami indicated earlier, it is a competitive space, so we do need to innovate and we do need to make sure that we're keeping up with our competitors in this space. That's why some of the initiatives we have taken on are in terms of making CSE an excellent place to work and all the initiatives it takes to become a top employer in Canada, such as providing an environment for people to be innovative and, also, fostering an inclusive environment, where you can continually bring in new people to the sector who might not have considered it before, particularly women or individuals from different ethnic origins—

● (1615)

Mrs. Shelby Kramp-Neuman: Thank you for that. Just due to the nature of my time, I'm going to keep going.

Ms. Alia Tayyeb: Sure.

Mrs. Shelby Kramp-Neuman: We know there are a lot of remaining challenges with regard to financial compensation or what have you, but I'm going to move along.

As bodies are continuing to change their mandates, how do you see the relationship moving forward between cyber command and the Canadian Armed Forces? How can we ensure that we're optimizing both their areas of expertise and their resources?

Ms. Alia Tayyeb: Thanks very much. That's a fantastic question.

We've found an excellent partner in the Canadian Armed Forces in terms of what we call "force generation": developing a new workforce to be interested in the cyber domain.

CSE also works very closely with U.S. Cyber Command in this field. We do talk about workforce strategies in terms of building the expertise we need in order to have successful tools to meet the challenges of the future.

Mrs. Shelby Kramp-Neuman: Thank you.

We recognize that one of the CSE's central aims is to carry out active cyber-operations. Given the different bodies, such as Foreign Affairs and National Defence, would CSE be operating independently or in conjunction with these different bodies?

Ms. Alia Tayyeb: Thanks for that question.

Indeed, we definitely do not work independently. We work very closely with the Canadian Armed Forces and the Department of Foreign Affairs.

The Department of Foreign Affairs, in fact, is required for active cyber-operations. The Minister of Foreign Affairs is required to provide her consent for those operations. We work very closely in the planning and development of those operations and assessing the risks.

On the CAF, we essentially have a combined workforce, where we have embedded officers in both areas so that we continue to work effectively on this aspect of our mandate.

Mrs. Shelby Kramp-Neuman: Thank you.

Earlier in your testimony, there was a comment with regard to recruitment being highly challenging and that the retention of the current workforce is extremely difficult. Perhaps I'll allow you to continue with those comments.

Perhaps it was your colleague that was speaking to struggles with retention.

Mr. Sami Khoury: Thank you.

No, actually, I meant that we are investing in retention and making sure that we continue to be an employer of choice: to provide our staff with an environment where they can thrive, with the training opportunities they need. We are also, on retention—

Mrs. Shelby Kramp-Neuman: I'm sorry to cut you off. I have one last question.

Just so you're not repeating yourself, do we have enough personnel currently to fully meet the operational requirements?

Mr. Sami Khoury: Thank you again.

We're constantly hiring. The demand on our services is growing. We are busy hiring as much as we can.

Mrs. Shelby Kramp-Neuman: Thank you.

The Vice-Chair (Mr. James Bezan): Okay.

Ms. Lambropoulos, let's try this again. You have five minutes.

Ms. Emmanuella Lambropoulos: Thank you for being with us today to answer some of our questions.

As I was about to say earlier, the CSE is working with partners in Ukraine to monitor, detect and investigate any potential cyber-threats and to help them take measures to address any of these threats.

Have we seen Russia using cyber-operations in order to harm Ukraine during this war? Can you tell us if this has had an impact on Ukraine's ability to defend itself? Also, as Canadians, can we draw any lessons from this?

Mr. Sami Khoury: Thanks for the question. I'll take a first stab at it and maybe turn to my colleague Alia for a follow-up.

Before the invasion of Ukraine started, we had been communicating to our partners the threat of Russian cyber-activities. Russia is a formidable cyber-actor, and we have been communicating as much as possible for people to take the threat seriously.

From a Ukrainian perspective, they've been the victim of Russian cyber-aggression since 2015 and 2016, when it affected the power grid. Over the years, Ukraine has been building resilience. With the help of the west tipping them off, they have fended off a number of cyber-attacks that Russia unleashed on Ukraine in the early days of the war.

We have learned a lot from these cyber-attacks that Russia has unleashed on Ukraine. We have quickly turned around and published or issued cyber-flashes, so that, in case there is any spillover effect in North America, or at least in Canada, we are prepared to share as much as possible with critical infrastructure and businesses about what some of these indicators are.

● (1620)

Ms. Emmanuella Lambropoulos: Would you like to add to that, Ms. Tayyeb?

Ms. Alia Tayyeb: Yes, indeed. Maybe just further on the aspect of your question in terms of what we've seen Russia do in Ukraine, I think there has been a considerable amount of information—including in open sources—documenting Russia's use of cyber-tools against Ukraine in its most recent conflict and the use of those cyber-attacks and cyber-threats against Ukraine in conjunction with their kinetic attacks, the most prominent example being the disabling of satellite communications over Ukraine in the lead-up to the war.

For us, what we would call “hybrid warfare”, the use of cyber-tools along with kinetic tools, has been well documented in this conflict, both by the cyber centre and, in fact, by Microsoft, which did an excellent study on mapping out those two capabilities and how they were used together in this conflict.

Ms. Emmanuella Lambropoulos: Thank you.

Based on what you're telling me, Russia is of course a great actor in this regard. You mentioned in your opening remarks that cyber-crime is the most likely threat to impact Canadians, and that there are quite a few actors that pose a threat, including China, Russia, North Korea and Iran, which pose the greatest threats. How do these actors differ in their goals and their capabilities?

Mr. Sami Khoury: Thank you for this question.

We have called out those four nation-states in our third national cyber-threat assessment. They have a variety of motivations to go against Canada by targeting Canadian individuals, by compromising some technology through worldwide campaigns, by targeting Canada's economic value or by pursuing financial gains.

For example, we know that Iran is using cybercriminal tools to avoid attribution. This is one of their techniques. China is going after research, technical data, business intellectual property and military capabilities. North Korea is very much interested in enhancing its economic value by stealing credentials and then stealing funds.

They each have a motivation to conduct those activities or to at least go after a certain aspect of Canadian society to further their own interests.

Ms. Emmanuella Lambropoulos: Ms. Tayyeb, would you like to add to that? You have 30 seconds.

Ms. Alia Tayyeb: I think Sami described it well.

We are constantly surveying the space in terms of looking for new tactics and techniques that are used by ransomware actors to target Canadians. It is an evolving space, and it's something that requires a dedicated effort to follow up on to make sure that we continue to protect Canadian infrastructure.

Ms. Emmanuella Lambropoulos: Thanks to both of you.

The Vice-Chair (Mr. James Bezan): Thank you.

Now we'll go to our rounds of two and a half minutes.

Go ahead, Madame Normandin.

[*Translation*]

Ms. Christine Normandin: Thank you, Mr. Chair.

I'd like you to talk about co-operation between governments and information sharing. Canada is part of the Five Eyes alliance. Under an international cyberspace policy, Canada asks governments to report on malicious activity.

Is the co-operation between governments free-flowing, or is it more of a give-and-take relationship? For example, Canada will get information if it hands over information. Not getting information makes a partner reluctant to share any.

What does that co-operation between countries look like?

● (1625)

Ms. Alia Tayyeb: The information-sharing mechanism is very effective and very transparent, especially between the members of the Five Eyes alliance. We work in partnership to address all the threats we've discussed today.

We have very close relationships with our partners in those organizations. We have other allies all over the world that we share information with. These threats affect all of us. I would say that we have very good relationships in this sphere.

I'll pass it over to Mr. Khoury now.

Mr. Sami Khoury: I'd like to add a couple of things.

We belong to a number of communities that share information for the purposes of cybersecurity. The Five Eyes partners share a lot of information.

At a more global level, we share information with computer emergency response teams all over the world. When we receive information about malicious activity, we send them a note so that they can take steps domestically to neutralize the threat.

Ms. Christine Normandin: Does information sharing within the Five Eyes alliance involve all the partners, or do discussions happen on a more one-to-one level?

Ms. Alia Tayyeb: Broadly speaking, I would say both scenarios are possible. It depends on the type of threat affecting the partners. Mr. Khoury may have something different to say about that.

[*English*]

The Vice-Chair (Mr. James Bezan): We're out of time. We have to move on to our next two and a half minute question. I'm sorry about that.

Go ahead, Ms. Mathyssen.

Ms. Lindsay Mathyssen: Thank you.

Ms. Tayyeb, you mentioned in your opening statement the expanded powers that you have. A lot of folks were, of course, concerned about that expansion and the fact that your department can collect information on Canadians for research purposes, and then there's no requirement to release that information. It's there forever.

Of course, a lot of human rights and civil rights organizations were concerned about the use of that data and about it being used against folks when they're exercising their rights. There were also other concerns in terms of the oversight of that and the accountability of that, and how you're monitored continuously now that these laws have been in effect for several years.

Could you comment on that?

Ms. Alia Tayyeb: Thanks very much for that.

Allow me the opportunity to just clarify a point, if I misspoke earlier. To be clear, CSE is not permitted in any way, shape or form to target Canadians or any individuals in Canada. That's a basic prohibition. That extends to our foreign intelligence mandate and our cyber-operations mandate.

What I believe I was referring to was that, in that space, the interest would be on the foreign actor. If the foreign actor is targeting Canadians, we'd be interested in what that foreign actor is doing that would be harmful to Canada. That's a very specific prohibition.

In terms of review, absolutely we are reviewed. We have two review bodies, the NSIRA, the National Security and Intelligence Review Agency, and the NSICOP. We also have an intelligence commissioner who approves our ministerial authorizations to ensure that they're in keeping, on the foreign intelligence side, with our charter obligations, and to maintain and ensure the privacy of Canadians should any information on Canadians be collected incidentally.

We have both oversight and consistent review in all aspects of our mandate.

Ms. Lindsay Mathyssen: Within the CSE Act, you are allowed to research the activity of Canadians nationally and domestically—are you not?

Ms. Alia Tayyeb: No, we are not.

The Vice-Chair (Mr. James Bezan): Thank you very much.

Mr. Kelly, you have five minutes.

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

Mr. Khoury, less than a year ago at committee, you said, "the state-sponsored cyber programs of China, Russia, North Korea and Iran pose the greatest strategic threat to Canada."

First of all, is that still the case? Do you have any comments on non-state actors?

Mr. Sami Khoury: Thank you for the question.

The assessment that we've reiterated in our most recent national cyber-threat assessment is that those four countries—Russia, China, North Korea and Iran—continue to pose the greatest strategic threat to Canada.

As far as non-state actors are concerned, obviously cybercriminals are a threat that we have to address. As well, as a result of the Russia-Ukraine conflict, we've seen a number of state-aligned hacktivist groups. These are cybercriminals who have sort of flown the flag or taken sides. A number of ransomware affiliates have decided to align themselves with Russia in the conflict and taken sides. These are always things of concern.

● (1630)

Mr. Pat Kelly: Are you saying that these state actors avail themselves of mercenary-type services from international criminals?

Mr. Sami Khoury: In some cases, there's a close relationship between the state apparatus and some of these cybercriminal organizations.

Mr. Pat Kelly: Okay.

Also in the report there was a recommendation number 10, which followed from your last appearance. It recommended:

> That the Government of Canada invest in defensive and active cyber operations capabilities. As well, the Government should increase its recruitment and training of cyber specialists for the Canadian Armed Forces and the Communications Security Establishment, and ensure that all federal systems are adequately protected against cyber threats.

What action has been taken within your department on recommendation number 10 of the report?

Mr. Sami Khoury: Maybe Alia can take the first part of that.

Ms. Alia Tayyeb: I don't have that report in front of me, but indeed, on the first recommendation, in terms of investing in active and defensive cyber-operations, as I indicated, in the budget announced in 2022, we did [*Technical difficulty—Editor*].

The Vice-Chair (Mr. James Bezan): We have a cyber-hack here.

Voices: Oh, oh!

Mr. Sami Khoury: In the meantime, I can address the second part of that recommendation, which was defending government systems.

The Vice-Chair (Mr. James Bezan): Go ahead, Mr. Khoury.

Mr. Sami Khoury: We are constantly monitoring government systems. We are updating them with the latest threat indicators. We work closely with SSC and with Treasury Board on making sure that government IT is very well protected.

Also, as a result of the NSICOP recommendation, we are working with the small departments, agencies and Crown corporations, to bring them into the fold of the defensive capability of the cyber centre.

Mr. Pat Kelly: Okay. Thank you.

What about the Office of the Privacy Commissioner? In response to an earlier question, you mentioned that there is not a requirement for businesses to report ransomware, hacks or loss of data, but they are required to report that to the Privacy Commissioner. Do you take cues from or do you work with that office to determine threats in the furtherance of your work in your agency?

Mr. Sami Khoury: Thank you for the question.

No, we don't get tipped off by the Privacy Commissioner. Businesses have an obligation to report to a number of bodies. Sometimes it's the Privacy Commissioner. Sometimes it's regulatory bodies. We reach out as soon as we hear of an incident. We always reach out to the victims and offer our assistance.

Mr. Pat Kelly: You, on your own, just monitor the media. It seems like there must be a better way to ensure you are aware of hacks or ransomware attacks and these kinds of things as they happen.

Mr. Sami Khoury: We are made aware of incidents through a variety of means, media being one of them, but we also have partners who tip us off. Sometimes the victims themselves reach out to us to inform us that they've been a victim of a cyber-incident. We are aware of victims through a number of ways, but the coverage is not 100%, of course.

The Vice-Chair (Mr. James Bezan): Thank you. Your time has expired.

I'll just say that when you appear in person the screen never freezes up. Cyber-hacks can't get at you.

The final questions go to Mr. May.

● (1635)

Mr. Bryan May (Cambridge, Lib.): Thank you kindly, Chair. Your point is taken, as we had trouble hearing me today.

First of all, I want to thank the panellists for being here with us today and getting us off on the right foot on this study. My questions are going to be around Russia and Ukraine.

With the beginning of Russia's invasion of Ukraine, particularly as we're seeing significant material support from Canada, and, of course, many NATO allies, we've heard warnings that Russia may retaliate against NATO with cyber-like attacks. In your opinion, has that threat materialized in any way?

Mr. Sami Khoury: Thank you for the question.

The threat has not materialized in a direct way, but the threat has materialized through some spillover effects.

In the case that my colleague Alia brought up, Russia went after satellite communication against Viasat. As a result, for some western entities that were also users of that service, their communication got disrupted. Russia's intention was to disrupt Ukrainian communication, but the spillover effect was bigger than Ukraine. We've seen those kinds of threats materialize.

We've also seen those state-aligned hacktivist groups that have aligned themselves with Russia going after western governments, most notably through DDoS attacks in Germany and other places as a way of registering a message.

The Vice-Chair (Mr. James Bezan): Mr. May, you're not coming through.

Mr. Bryan May: For some reason, my little fob here isn't working very well. Can you hear me now, sir?

The Vice-Chair (Mr. James Bezan): We'll start again.

Go ahead.

Mr. Bryan May: Thank you.

Given that, can you spend a moment to share with this committee the strategies or how Russia uses cyberwarfare against Canada? Has that changed over the last year?

Mr. Sami Khoury: Thank you for the question.

We've seen, as I mentioned, that Russia is a formidable cyber-player. We've seen the extent of its capabilities in Europe, or at least in Ukraine, with the deployment of cyber-capabilities that are destructive in nature. We've seen it use them against Ukraine by shutting down the power grid over there twice.

We are very concerned about that, and that's why we work with critical infrastructure providers in Canada to make sure they are taking every precaution or every measure to protect themselves and their networks from those kinds of cyber-threats. Everything we learn, everything we see in Ukraine and everything we learn from what Russia is doing around the world we try to promulgate through cyber-flashes and other information bulletins to Canadian businesses.

Mr. Bryan May: In that regard, how does CSE assist the work of the Canadian Armed Forces, particularly in the areas of intelligence-gathering and counter-intelligence?

Ms. Alia Tayyeb: I can take that one.

We work extremely closely with the Canadian Armed Forces in terms of intelligence provision. We share with them all intelligence that we collect, whether it relates to threats to their armed forces' deployments abroad or internal threats to Canada that would affect the Department of National Defence, as we have a very close working relationship there.

In terms of other forms of co-operation, I spoke about foreign cyber-operations and how we work very closely with them on that mandate.

I would add that, under our act, we also have an assistance mandate. It is explicit that we can provide assistance to the Canadian Armed Forces and in so doing, we'll be operating under their mandate. However, we can use our technical skills, abilities and capabilities to assist them in their operations if they were to make such a request.

Thank you.

Mr. Bryan May: Thank you.

I think that's my time, Mr. Chair.

The Vice-Chair (Mr. James Bezan): Thank you, Mr. May.

To follow up on that and exercise a bit of my prerogative as chair, when you are assisting the Canadian Armed Forces in their activities, as well as what CSE is doing under its new mandate since 2019, does that include both defensive and offensive postures?

● (1640)

Ms. Alia Tayyeb: The nuance with the request for assistance part of the mandate is that we would act under the Canadian Armed Forces' mandate and authority, so it would be to the extent that they have the authority to do something. Whether it be active or defensive in nature, we could assist them insofar as their authorities permit.

The Vice-Chair (Mr. James Bezan): I'll also drill down a bit more into protecting Canadian infrastructure.

How much do you work with our public sector as well as private sector partners, like financial institutions, transportation hubs, health care systems and things along that line that would definitely be considered soft targets by our adversaries?

Mr. Sami Khoury: Thank you for the question.

We work extensively with the private sector and the public sector. We have a number of engagement fora through which we are briefing them regularly. For example, with the health care sector, we have a forum with them every two weeks to brief them on the latest threats. There are often over 500 people on a call.

We have more intimate collaboration, for example, with the banks, the electricity sector or the natural gas providers. We tailor our engagements to communities that share similar infrastructure, similar technologies or similar capabilities, but we are talking to almost all 10 critical infrastructure centres in Canada.

The Vice-Chair (Mr. James Bezan): Thank you very much.

I want to thank both Mr. Khoury and Ms. Tayyeb for joining us today. That was very interesting, and it was a great way to kick off our study on cybersecurity.

With that, we're going to suspend.

I would ask that the next round of witnesses please come to the table and log in online, so that we can continue in an expeditious manner.

● (1640)

_____(Pause)_____

● (1640)

The Vice-Chair (Mr. James Bezan): I call the meeting back to order. Here we go.

For our second hour, we have the Centre for International Governance Innovation. Joining us is Aaron Shull, managing director and general counsel, who is joining by video conference; and Dr. Wesley Wark, who is a senior fellow and is sitting with us at the table, which we really do appreciate.

Each of you has five minutes for your opening remarks. I have Mr. Shull going first.

● (1645)

Mr. Aaron Shull (Managing Director and General Counsel, Centre for International Governance Innovation): Thank you very much, Chair.

Thank you very much to the committee for having me. I'm honoured to appear before you today to discuss the critical issue of cybersecurity and the capabilities of foreign actors.

To effectively address the issue, I believe the government should take a multipronged approach. Now, I understand the urgency of the issue, so rather than discuss the current state of cybersecurity—we already heard from the previous two witnesses about the various threats we face as a country—let me begin at the end and offer a few thoughts about what I think you can actually do about it.

I've had the benefit of reviewing the comments of my colleague, Wesley Wark, so I will focus on a different set of prescriptions, although I will say that I agree with what he's going to offer.

First, I think the government should incentivize companies to adopt the latest security measures, such as the “CyberSecure” standard established by ISED and CSE for small and medium organizations. The standard provides a high level of protection, but its adoption—this is the problem—has been limited.

Implementing a tax credit system as an incentive to help increase the overall level of cybersecurity in the country and reduce the risk of cyber-attacks on businesses would be a way forward. These attacks result in significant financial loss, damage to reputation and disruption of operations. If we were to advance this, we could attract investment and increase productivity and profitability. The standards are already there, but too few companies are doing them. There's that old saying that you cannot herd cats but you can pick where you put the food out, so incentivize those businesses through a tax credit.

Second, the government should establish a clear and concise legal framework for dealing with cyber-attacks that includes guidelines for attribution, response and liability, but the governance structure should be nimble and responsive to the fast-changing environment. The regulations should be expert-driven, focusing on sound policy and not good politics. The Governor in Council should be able to approve standards, codes of practice and certification programs to act as an integrated compliance mechanism.

Third, the government should establish an annual multistakeholder platform for collaboration and engagement on cybersecurity issues. This platform should include participants from all levels of government, private sector, indigenous communities, academia, not-for-profits, law enforcement and industry leaders. In my view, cybersecurity is a whole-of-society concern for Canada. Everyone, including think tanks, needs to do more to address this issue.

As a consequence, my organization, CIGI, plans to host the first Waterloo security dialogue in June to bring together various stakeholders and focus on discussions and simulations to better understand the impact of cyber-incidents, response and recovery measures, and the roles and responsibilities of different parties.

Let's talk about the threats. As previous speakers have mentioned, there are active persistent threats, or APTs, in coordinated and highly targeted cyber-attacks often carried out by state actors who aim to steal sensitive information or disrupt critical infrastructure over a long period of time.

You have ransomware, which we've talked about already as well. That's malicious software that encrypts the victim's files and demands payment for a decryption key. There's also now something called double extortion, where they threaten to release very sensitive information. Not only is your information locked up, but they threaten to release sensitive things to either embarrass you or push you to payment.

Then we have supply chain attacks. Supply chain attacks occur when an attacker actually compromises the software or hardware of the supplier to deliver malicious code to its customers. Probably the best known of these in recent memory is the 2020 SolarWinds incident, where that popular IT management software was used to compromise thousands of organizations.

We also have election interference and foreign actors using cyber means to hack into voter databases, spread disinformation and manipulate social media, all with the view to influence public opinion.

We also then have critical infrastructure attacks. This was already talked about in terms of the Ukrainian power grid. This is a great example of a critical infrastructure attack having a real-world effect where, in 2015, 225,000 people were without electricity.

The full capabilities of states will certainly vary, but here's my view: In light of current geopolitical trends, I believe the safest operating assumption for Canada is that we will be existing in a grey zone for the foreseeable future.

As for what I mean by “grey zone”, I'm actually going to adopt the definition from Canada's defence policy, which I thought was the best definition I'd seen.

● (1650)

Here, it says:

> State and non-state actors are increasingly pursuing their agendas using hybrid methods in the "grey zone" that exists just below the threshold of armed conflict. Hybrid methods involve the coordinated application of diplomatic, informational, cyber, military and economic instruments to achieve strategic or operational objectives. They often rely on the deliberate spread of misinformation to sow confusion and discord in the international community, create ambiguity and maintain deniability.

In conclusion, my own view is that this is a whole-of-society concern for Canada. It's not just about government. It's actually about governance.

I believe it's our collective duty to better prepare the country for an existence in this grey zone.

Thank you, Mr. Chair.

The Vice-Chair (Mr. James Bezan): Thank you for your opening comments.

Please proceed, Dr. Wark.

Dr. Wesley Wark (Senior Fellow, Centre for International Governance Innovation): Thank you, Chair.

Chair and members of the committee, I'm grateful for this invitation to appear and give testimony.

The terms of reference of your study touch on many facets of the cyber-threat, but I will focus on just one here in the five minutes I have for this opening statement, and that's the Russian invasion of Ukraine, which has provided important real-world insights into the ways in which cyber-weapons can and will be used in wartime in conjunction with more conventional military attacks.

This alignment was first exemplified in the Viasat hack of satellite-based Ukrainian communications on the opening morning of the Russian invasion. You've heard previous speakers from CSE mention that attack.

What do we know of events since February 24, 2022? Let me take you to two open-source studies. I've provided links to these studies to the clerk of the committee.

In June 2022, CSE's Canadian centre for cybersecurity produced a threat bulletin that catalogued significant Russian cyber-activity in conjunction with military attacks on Ukraine for the period from February 2022 through to May 2022.

Among the key judgments in that CSE bulletin were that the scope and severity of Russian cyber-operations were more sophisticated and widespread than had been reported in open sources and that, beyond the Ukraine theatre itself, Russian cyber-threat actors were engaged in widespread cyber-espionage campaigns against NATO countries and looking to develop further cyber-capabilities against such targets, including Canada.

In January 2023, the Ukrainian cybersecurity agency released a report—translated, fortunately, into English—using a methodology very similar to that employed by CSE, which documented the scale of Russian cyber-attacks and their alignment with conventional bombardments from February through to November 2022.

A key finding in the Ukrainian report concerns the ways in which Russian cyber-attacks have targeted energy infrastructure in Ukraine as part of a ramped-up Russian effort to destroy Ukrainian sources of civil power supply and undermine morale. According to the Ukrainian security service—SBU—report, Russia carried out on average more than 10 cyber-attacks on Ukrainian critical energy infrastructure per day in November of 2022.

Ukraine's cybersecurity leadership wants the world to recognize the reality of cyberwarfare as they have experienced it. They urge a common approach to cyber-aggression, the use of sanctions to undermine the cyber-capabilities of an aggressor, the need for enhanced sharing of information about cyber-threats and a clear designation of cyber-attacks on civilian critical infrastructure as a war crime, along with a determination to pursue accountability for such crimes.

How should Canada respond to this set of appeals? I would suggest the following.

First, ensure that CSE is able to provide the maximum possible aid to Ukraine in terms of signals intelligence and cybersecurity support.

Second, the Government of Canada should continue to provide financial support to ensure the resilience of Ukraine's cyber-systems.

Thirdly, along with our allies, we should be using targeted sanctions to undermine Russian state and proxy cyber-capabilities. I think we should also continue to document and publicly call out Russian cyber-aggression against Ukraine and NATO. I would urge us to take a lead role in supporting Ukraine's call to designate cyber-attacks on critical infrastructure as a war crime in international law and assist Ukraine to pursue accountability.

Finally, we should ensure that we maintain a robust capacity to monitor and learn from the use of Russian cyber-weapons against Ukraine. This should include research support for Canadian academic and NGO studies and engagement with expertise in the private sector.

We have learned three things from the Russian cyberwar against Ukraine. First, civilians are prime targets. Second, cyber-weapons are not precision munitions, and third, that cyber-aggression knows no rules or bounds.

Worse still is what might be waiting in the wings: the looming possibility of another—I'm going to refer to this operation in Russian—NotPetya malware attack, with global ramifications. NotPetya was a Russian GRU—that is the military intelligence agency—hacker operation launched in June 2017 against Ukraine. It morphed out of control, as many of these malware attacks will do, crippling global container shipping. It was described by one Homeland Security adviser to the President of the United States as “the equivalent of using nuclear bomb to achieve a small tactical victory”.

● (1655)

The cyber-nuke outcome is one we must strive to avoid, just as we strive to avoid escalation to nuclear war over Ukraine.

Mr. Chair, I'll conclude by saying that I hope this doesn't sound too much like *Dr. Strangelove*.

Thank you.

The Vice-Chair (Mr. James Bezan): Thank you very much.

Those were very good opening comments. I appreciate both testimonies.

With that, we will go to our first round.

Ms. Kramp-Neuman, you have six minutes.

Mrs. Shelby Kramp-Neuman: Thank you, Mr. Chair.

Dr. Wark, thank you for your testimony. I'll start my questions with you.

In what ways do the tensions in Russia increase the need for more resources and military defence supports to ensure that Canada can effectively compete on the international stage?

Dr. Wesley Wark: Thank you.

Through you, Chair, I didn't quite catch it. I think the question is about defensive capabilities or armed forces capabilities. I think there would be.... I'd certainly agree.

The conventional view would probably be.... We shall see what the government decides in its upcoming defence review update, but I think the view will be that the armed forces need a lot of new equipment to be able to engage effectively in any future conflict, including along with allies in support of our own sovereignty. There is a great deal we have to do in that area.

I think we all recognize that the Canadian Armed Forces lacks a range of things, from sufficient manpower through to key military capabilities. Many of these have been called to attention.

I must say, as a private citizen, the fact that we were only able to supply four Leopard 2 tanks to Ukraine struck me as a terrible symbol of the ways in which our military has been allowed to be degraded over the years.

Thank you.

Mrs. Shelby Kramp-Neuman: Thank you. I'll continue.

There's a lack of manpower and a lack of morale. In addition to that, there are growing concerns that Canada is being left behind in the Five Eyes relationship as the U.K., U.S. and Australia continue to collaborate.

How has this worsened in the past 10 years, and how can Canada re-establish a relationship?

Dr. Wesley Wark: Thank you for that question.

I'll go in a slightly different direction. I'm not sure that I entirely agree. I would make a distinction between, perhaps, our military capabilities and the way that they have declined, and our intelligence capabilities, particularly on the signals intelligence side and our contribution to the Five Eyes.

I think that Canada, through the CSE, is regarded as a key actor in the Five Eyes, and it is regarded with respect. I am told by Five Eyes counterparts that we are regarded as being one of the leading countries in terms of our ability to provide cybersecurity for federal data infrastructure and communications. We're regarded, in that regard, with respect.

I think the challenge for Canada is keeping up in the face of a wide range of threats.

We are regarded as a key player in the Five Eyes. There are always things that the Five Eyes would like us to do more of. There has been consistent pressure for decades, for example, for Canada to create a foreign intelligence service and a humint agency, which we've already resisted. On the signals intelligence and cybersecurity side, I think we're a strong player.

Mrs. Shelby Kramp-Neuman: Thank you.

Switching gears, I'll address my next question to Dr. Shull.

There have been growing concerns over the use of social media and the information Canadians wilfully provide international companies on our cybersecurity. How does social media consumption make us easier targets for these international cyber-threats?

Mr. Aaron Shull: There is traditional cybersecurity, which is usually unauthorized access to systems and data. What you're talking about—and I really liked the question—goes a bit deeper, to societal resilience. We're talking about people and people's views of the world.

When we think about disinformation, misinformation or malinformation, the point is that people are persuadable. There are sophisticated influence campaigns that are taking place all the time to try to change our discourse, to sow societal division and to pull people in different directions, when we need to be uniting. The point here is that many of those capabilities are commercial and off-the-shelf. The highest profile example was the 2016 election in the United States, when the Russians got involved.

The point here is that the system didn't malfunction. It functioned as it was built. What we have is social intermediation with platforms sitting at the middle of our social discourse, and their incentive is profit. Their incentive is eyeballs. That's what we've built for ourselves.

It's a bigger conversation than just the cybersecurity stuff, but it's a great question.

● (1700)

Mrs. Shelby Kramp-Neuman: Thank you.

To add to that, what kind of access or power are consumers providing companies when agreeing to these terms and conditions?

Mr. Aaron Shull: That could be the subject of a Ph.D. dissertation.

I would say, to read all the terms of service that you've agreed to all year, there is some estimate that it would take the average individual something like 200 days.

I think the broader point is that we have built our entire system based on consent, which is a fallacy. It's a lie. The fact is that we don't know what we're consenting to. For a case in point, one company stuck in their terms of service that if you agreed to their terms, then they would own your soul forever, so now there's one company in San Francisco that just doesn't know what to do with all the souls that it owns.

Mrs. Shelby Kramp-Neuman: Going back to you, Dr. Wark, as we have you in the room, how do you see Canada's current investment in infrastructure compared with that of other countries like the United States, for example?

Dr. Wesley Wark: I'm sorry, but you're talking about investment in infrastructure...?

Mrs. Shelby Kramp-Neuman: I mean in comparison with that of other countries like the United States.

Dr. Wesley Wark: I would say we have a long way to go in deciding what we want to do about critical infrastructure. Let's put it that way.

We're waiting for a critical infrastructure strategy, which has been under study by the federal government. You will have seen a reference to Bill C-26, which refers to critical infrastructure. We have a list of critical infrastructure that dates back to 2009. In other words, it hasn't been updated since that time, which is the last time we had a critical infrastructure strategy.

The starting point is going to have to be to decide what we mean by “critical infrastructure”. Once we've done that—that will be an important but not an easy step—then we can think about regulating the terms under which critical infrastructure functions and what we expect of them in terms of, particularly, cybersecurity strategies.

There's some of that under way, obviously informally. Some aspects of critical infrastructure have done a terrific job in terms of ensuring they have very high levels of cybersecurity. The major banks are probably a key example of that. Across the board, the system is very diverse.

Mrs. Shelby Kramp-Neuman: That's excellent. Thank you very much.

The Vice-Chair (Mr. James Bezan): Mr. Sousa, you have the floor.

Mr. Charles Sousa (Mississauga—Lakeshore, Lib.): Thank you very much.

Thanks to both of you for your presentations. I appreciate them. I appreciate your highlighting some of the issues as they relate to the war in Ukraine and Russia and the various actors out there in foreign bodies who are creating stress for all of us.

You did talk a little bit about the cognitive warfare, the misinformation and those sorts of issues that are also prevalent and creating some havoc—tactics not necessarily to hold us ransom but rather to feed us misinformation.

Can you tell me, besides the foreign actors, how prevalent that is on our domestic soil?

Dr. Wesley Wark: Thank you for the question.

First of all, we're coming up with a more sophisticated understanding of what's going on in the information space. It's important to understand that we make distinctions among three different categories of information out there that may be troubling to us.

One is misinformation, which is defined by CSE, among others, as information that is false but not deliberately disseminated as being false. In other words, someone believes it even though it's untrue. There's, of course, a great deal of that and a lot of it circulating on social media channels. We saw its impact, for example, in the “freedom convoy” events in Ottawa and across the country last year.

Another form is disinformation, which is defined as information, often deliberately put out by foreign state adversaries, that is deliberately deceptive and untrue and designed, for various reasons, to undermine the state of a society. There are certain actors out there, including Russia and China, that are particularly good at disinformation. Russia has taken a lead, and we've seen a lot of that in the Ukraine war.

Then there's a third category, which I think really deserves a lot of attention, that CSE and its American counterpart have defined as malinformation. This is the grey area between disinformation and misinformation—the manipulation of information that's partly true and partly false to achieve certain objectives.

We're coming up with a more sophisticated understanding of how these different aspects of false information circulate and have an impact, but we're only at the beginning of a study of this. Frankly it's very difficult to know what to do about it other than trying to block foreign state actor activity.

● (1705)

Mr. Charles Sousa: The concentration is certainly on the foreign side. Are you not looking as much at what is happening domestically here?

Dr. Wesley Wark: In terms of intervening in the domestic space for political discourse, that raises important charter protection issues.

It's much more straightforward, although technically still very complex, to deal with something that is clearly improper and illegal, which is foreign state activity. This is why CSE, among other departments of the federal government, has a mandate to deal with foreign state disinformation.

Mr. Charles Sousa: How effective are AI and quantum technologies? Is this part of where these foreign state cybersecurity measures are being taken?

Dr. Wesley Wark: AI is certainly an enabler. Artificial intelligence has already been used already in various ways. Quantum computing and quantum applications are for the future, and I am no expert on them. Frankly, I hope not to be here when they're finally introduced. They are for the future. We can speculate a lot about what they might look like, but we're not there yet.

Mr. Charles Sousa: Are we winning against these cyber-threats from Russia and China?

Dr. Wesley Wark: That's a good question.

I think we are holding our own. The reason I think it's particularly important to pay attention to the Ukraine war is that it's a laboratory for cyberwarfare. It's really the first significant laboratory we've seen. Everything that's been used by Russia against Ukraine, and the way in which Ukraine has responded, is very important for us as a matter of study. We're in a fortunate position to be able to study this.

Mr. Charles Sousa: Is Ukraine being effective in their counter-attacks on this?

Dr. Wesley Wark: They are. I would say that they are partly because they have had long experience in this, going back to 2014 and the initial Russian incursion into Crimea and elsewhere. They've been ramping up their capabilities. They've not only been developing domestic capabilities and having popular support to do that. They've also had a lot of assistance from key allies in the west and from all the Five Eyes partners.

Mr. Charles Sousa: When you're looking at the infrastructure being deployed by Canada relative to some of these efforts by foreign players, are we partnering now with NATO and others to enable us to fight cybersecurity collectively? In so doing, are we exposing ourselves to yet other actors?

Dr. Wesley Wark: I think it's an interesting question.

I think the key alliance network in which Canada participates and where we're able to do significant work is the Five Eyes partnership. Many of the Five Eyes members, or at least some of them, are also members of NATO—Canada, the U.S., the U.K.—so it spills over into NATO. The Five Eyes is the key partnership for enhancing cybersecurity. A lot of work is going on there, I think, behind the scenes.

Very quickly, I would like to draw the committee's attention to one of the problems we have in Canada. CSE has a certain mandate. You see it in their cyber-threat assessment, which CSE officials have mentioned. They want to talk about strategic threats to Canada—that is, foreign state active threats—because that's in their mandate. There's a whole other world of threats to Canada and Canadians, including through cybercrime, which is not CSE's issue. It is the issue of the RCMP.

This is just a plea to the committee that, if you have the time in this study or in the future, we really need to have a look at how the RCMP is able to deal with this vast world of cybercrime and its impacts.

The Vice-Chair (Mr. James Bezan): Thank you.

[*Translation*]

Welcome to the Standing Committee on National Defence, Mr. Desilets.

You have 16 minutes. Please go ahead.

Mr. Luc Desilets (Rivière-des-Mille-Îles, BQ): Did you say "16 minutes", Mr. Chair?

● (1710)

[*English*]

The Vice-Chair (Mr. James Bezan): It's six. You have six minutes.

[*Translation*]

Mr. Luc Desilets: Thank you, Mr. Chair.

Thank you to the witnesses.

I sit on the committee from time to time. This is a fascinating subject, I must say. It's a source of concern, but also an area with tremendous potential.

I'd like to start with Mr. Shull.

I have a question about the cyber-attacks that we experience in small doses. In all likelihood, we will face more and more of them, so do you think we could go so far as to consider them war crimes?

[*English*]

Mr. Aaron Shull: That's a very good question. Indeed, senior members of the Ukrainian government have called for the offensive cyber-activities in the Ukraine to be considered war crimes. At present, it's likely not, but certainly it's not necessarily something that—

[*Translation*]

Mr. Luc Desilets: Excuse me, Mr. Shull.

The sound quality isn't good enough for the interpreter to do their job.

[*English*]

The Vice-Chair (Mr. James Bezan): Can you make sure your microphone boom is in the right place? Speak louder and try again, please.

Mr. Aaron Shull: Is it possible to interpret now, if I speak slowly?

The Vice-Chair (Mr. James Bezan): Unfortunately, we can't take any more testimony from you, Mr. Shull. The audio is not good enough for interpretation—unless you want to log out, exit the screen, log back in and see if you can get your audio working better so that we can hear you for proper interpretation here.

Monsieur Desilets, I stopped the clock. You can direct your questions toward Dr. Wark, if you want.

[*Translation*]

Go ahead, Mr. Desilets.

Mr. Luc Desilets: Are we carrying on with the same witness?

It doesn't look like it. Since he's still having technical issues, I'll switch to the other witness.

[*English*]

The Vice-Chair (Mr. James Bezan): You have to continue with Dr. Wark.

[*Translation*]

Mr. Luc Desilets: Mr. Wark, we've talked a lot about the firm McKinsey & Company lately. Since the firm also has ties with China, do you think it could affect Canada's national security?

[*English*]

Dr. Wesley Wark: Thank you.

I'm not an expert in contracting. I hesitate to answer. I think the answer that you had from CSE is probably the most appropriate one, which was that in terms of the security of contracting, it is a matter for PSPC. It's one that, in my experience as an occasional contractor—not on the scale of McKinsey—they take very seriously.

[*Translation*]

Mr. Luc Desilets: As a contractor, you're not on the same scale as McKinsey & Company. That's what I gather.

You mentioned the Five Eyes alliance. What do you have to say about Canada's position and participation in the alliance? Do you have any criticisms?

Is Canada's level of participation adequate?

Where are the gaps?

[*English*]

Dr. Wesley Wark: It's a very interesting question. It's hard to answer precisely for anybody who has an outsider status—like me—and who has not taken part in Five Eyes' meetings or communications.

My understanding is that Canada has been a member of the Five Eyes and was key to the expansion of the Five Eyes system. Our membership goes back to 1949, so we've been a part of this grouping for a very long time.

Our principal investment in the Five Eyes has always been in the signals intelligence and cybersecurity fields. We've expanded beyond those over the years as the Five Eyes expanded. I think there is a greater contribution that Canada could make to the Five Eyes in a variety of fields. That raises the perennial issue, for example, of a foreign intelligence service and what additional information it might provide to Canada.

There's also a role that other Five Eyes' partners look to Canada to play that we're able to play on occasion, but probably not to the strength that we should, which is in the assessment of global security threats. The threat assessment piece is an important piece with the Five Eyes, and Five Eyes partners like to get multiple perspectives on complex, developing global threat issues. We have some capabilities in that regard, but I think we could invest a lot more in the analytical side of the intelligence business, which often gets a lot less attention than the collecting side—the signals intelligence or the agent on the ground side.

● (1715)

[*Translation*]

Mr. Luc Desilets: That's interesting.

You said there were three types of false information out there. I really appreciated how you categorized them. The second type was disinformation, which is put out deliberately. It's a fairly new thing, if I'm not mistaken. We've probably experienced this type of false information on a different level.

Do you think there is anything we can do to counter false information that is deliberately put out by the Russians, the Chinese and, at times, perhaps even allies?

[*English*]

Dr. Wesley Wark: Thank you for the question.

We should probably be worried most about adversaries who are deliberating conducting disinformation campaigns and interfering in democratic practices. A lot of our attention has been paid, since 2016, on the possibility of election interference, because that's so fundamental to democratic practice. There's a lot of attention, as well, to the ways in which foreign state adversaries can use cybertools to try to impact diaspora communities in Canada and among our allies.

I think there are three effective things that we can do in that regard.

One—probably the most important thing—is to monitor and call them out publicly. Call them out as a form of deterrence for foreign state actors trying to use those tools, but also call them out to make sure that the Canadian public understands what's going on. We do that on occasion. We're doing it more often than we've done in the past. There are always sensitivities about calling out things because they can have diplomatic repercussions, so it can be complicated, but I think calling out is an important thing.

Public education is a critical part of the piece, but I will also say that trust in Canadians and trust in the ability of Canadians to make some common-sense decisions, ultimately, about what is clearly false and what is information that's being circulated on behalf of a foreign state is an important but, perhaps, underemphasized part of the equation. This may be the optimist in me, but I continue to have some faith in public sense.

I always like the example of what the French government did in response to its concerns about election interference in the national election in 2016. They created a special office in the president's office that was designed to introduce satirical commentary about clumsy Russian disinformation campaigns and to make fun of them. I think that's a great tactic.

The Vice-Chair (Mr. James Bezan): Ms. Mathyssen, the last six minutes go to you.

Ms. Lindsay Mathyssen: Thank you, Mr. Chair.

I'm glad to see Mr. Shull back online. I think my questions could be for both witnesses.

I'd like to continue on a bit from what Ms. Kramp-Neuman was discussing, Mr. Shull. I think you mentioned the discussion about the profit side of social media and the dangers of it, and of course the algorithms that are specifically used and written to bolster those profits, but really put forward more of that misinformation or sometimes online hate. We've seen that directly.

Could you comment in terms of what role the government needs to play in terms of the regulation of this and the responsibility of those private corporations to not use or not profit so much from those algorithms?

Mr. Aaron Shull: Sure. I'll just see if the translators are able to pick me up now. Not at all?

The Vice-Chair (Mr. James Bezan): Unfortunately, we're not getting the go-ahead.

Ms. Lindsay Mathyssen: Perhaps he could submit those responses.

The Vice-Chair (Mr. James Bezan): That's a good idea.

You could submit your answer in writing to the committee. Just forward it to the clerk and then we will have your feedback on that basis.

Ms. Mathyssen, let's move ahead.

Ms. Lindsay Mathyssen: I would actually offer the same question, then, to Mr. Wark.

Dr. Wesley Wark: Thank you for the question.

The fact that CIGI, which is at the heart of Canada's cyber-universe in terms of research, occasionally seems to have some difficulty connecting is actually a running joke between Aaron and me, but anyway....

Voices: Oh, oh!

Dr. Wesley Wark: I would say that I think one of the things that Aaron and I have discussed and focused some attention on—I offer this as a partial answer—is that the universe of social media communications is increasingly being affected by automated bots. These are simply machines out there that amplify, according to certain algorithms, certain kinds of messages, and they can be used for disinformation purposes by foreign state actors. We saw this with Russia in the 2016 election campaign against the United States. They can be used by social media companies to boost ratings.

I think the conclusion we've come to—without having the tools and necessarily suggesting how you do this—is that we have to tackle the automated bots issue in some form or another, to reduce their impact and the scale of the use that is made of them.

● (1720)

Ms. Lindsay Mathyssen: I was informed—and there was a presentation I received—about how we see personal information going forward and people's rights of usage of that personal information. It was suggested that, at whatever point, people be paid to surrender that personal information to Facebook, to social media or to any of those forums. Is that potentially a future way forward in terms of that compensation so that people know more of what they're getting and there's almost a contract?

Dr. Wesley Wark: Thank you for the question.

I would say this is something that successive privacy commissioners have been particularly keen on pursuing—and not just federal ones but provincial ones, including the previous Ontario privacy commissioner—to try to build a better model for consent that doesn't require us, as Mr. Shull suggested, to read through hundreds of pages of abstruse technical language, which none of us do.

We clearly need a better model for consent, and we clearly need better restrictions on efforts to use consent on the part of social media companies. I think there is a real role for the Government of Canada to play in that regard in terms of setting guidelines, as challenging as that might be, because the giant social media platforms will not like it, but it's something that I think we have to tackle.

Ms. Lindsay Mathyssen: If I could just switch a bit, there was discussion previously—and Mr. Shull, I know you can't contribute but we could have a discussion in terms of what you put in your written testimony—on providing more incentives for small businesses to up their game in terms of cybersecurity. In the previous panel today, Ms. O'Connell was asking about what municipalities needed to do as a tax on that infrastructure and how they are being provided with supports, advice and what have you.

Mr. Wark, would you argue that this support needs to be provided to municipalities and other levels of government as well?

Dr. Wesley Wark: I'm sorry that Aaron can't take that question. I'll try to answer for both of us to the best of my ability.

I think the suggestion that Mr. Shull made about tax incentives is certainly one way forward. Regulation, at least of what we might determine to be critical data infrastructure and communications, is another. Bill C-26 may have an interesting impact in that regard, depending on what Parliament does with it. It's certainly worthy of study.

I think the conclusion that we've come to, which CSE has also spoken to, is that, while there are pretty high levels of cybersecurity capabilities, awareness and implementation on the part of the major private sector actors in Canada, including the financial sector and other aspects of critical infrastructure, the real problem is with small and medium-sized enterprises. They have neither the resources nor, perhaps, even the understanding of the degree to which they are vulnerable to cyber-attacks

I think the small and medium enterprises are the area of focus, as well as figuring out ways to help them up their game in cybersecurity in ways that are affordable and understandable to them. That is the challenge.

The Vice-Chair (Mr. James Bezan): Again, thank you very much. Your time has expired.

We're going to move on to our five-minute round.

Ms. Jennifer O'Connell: Mr. Chair, I'm sorry.

Before you move on, could we ask the witness Mr. Shull if he can answer in writing to the committee? I think these are important questions.

● (1725)

The Vice-Chair (Mr. James Bezan): He's not online anymore. Is he?

The Clerk of the Committee (Mr. Andrew Wilson): He is. He's turned off his camera.

The Vice-Chair (Mr. James Bezan): He's listening in.

Mr. Shull, if you could respond to all of these in writing, that would be great.

Ms. Jennifer O'Connell: Yes, if he wishes.

The Vice-Chair (Mr. James Bezan): I know it's a bit more work, but we appreciate the input.

Moving on, Mr. Kelly, you have five minutes.

Mr. Pat Kelly: All right.

In addition to, or maybe in expansion of some of what you said in your opening remarks, can you give us some description of the impact of a potential successful cyber-attack on civilian life in Canada?

Dr. Wesley Wark: I thank you for the question.

Mr. Kelly, we've seen a few examples of attacks on Canadian holders of data and private information over the years. We haven't seen crippling attacks at this stage, I would say. Probably the worst of the attacks that we've seen goes back a number of years now. That was the hack into the National Research Council. It took a long time to rebuild systems in response to that attack.

We're learning as we're going, so I don't have an example to offer you other than these isolated incidents, but we're learning as we go.

Mr. Pat Kelly: During the study that took place less than a year ago—it was a broader study, but we looked at cybersecurity—there was discussion about the gaps that exist between the Canadian Armed Forces and the Canadian Security Establishment.

In the time since then, would you say that the gaps still exist? Have they been adequately filled? What are the gaps between our institutions?

Dr. Wesley Wark: Mr. Chair, I'd answer that question by saying it would be interesting to hear from CFINTCOM, in particular, on that, because that's the organization within DND that is most affected by developments.

What we've seen recently—it was highlighted in the defence "Strong, Secure, Engaged" strategy in 2017, and perhaps will be reinforced in the update, whenever that appears—is that the Canadian Armed Forces decided it needed a much enhanced capacity to engage in cybersecurity and have cyber-capabilities for its own offensive and defensive operations. It has been attempting to build up an independent, stand-alone capability in that regard under its own mandate. CSE has been able to assist it.

It's not so much that there are gaps between CSE and CFINTCOM, as I would understand it. It's more the question of how well the Canadian Armed Forces and, particularly, CFINTCOM have been able to build that cadre of cyberwarriors that they need.

Mr. Pat Kelly: You talked about resources, too, a bit in your opening statement. We're very familiar with the extraordinary cost of ships, jets, tanks and whatnot.

Is there a budget shortfall? Are there additional budget demands necessary to successfully undertake proper cybersecurity? Is it more a question of hiring the right personnel? Are there hardware and important budgetary items that cost money that we're deficient in or should budget for in the future?

Dr. Wesley Wark: Thank you.

I think the answer to that question is that probably everything comes into play. I think the key challenges for CFINTCOM in particular in building its capabilities are partly technological—having access to the best kinds of systems they'll need—and also in terms of human resource capability. It's about finding that kind of talented pool of either civilian or armed forces members who can contribute to a sort of cyber cadre within the Department of National Defence. In that respect, they face the same challenges, although perhaps magnified, that CSE faces in terms of maintaining the workforce, which was the subject of questions here and that CSE responded to.

I think it's a particular difficulty for CFINTCOM. It's also the case that armed forces are not necessarily institutions that change rapidly, culturally, and we've seen this in many respects.

Mr. Pat Kelly: Thank you. I have less than a minute left.

For these systems that you say we need access to, what kind of budget is necessary to ensure that we have adequate systems in place?

Dr. Wesley Wark: I couldn't really answer that question, to be honest. I'm not sure it's a huge price tag. It's just being able to identify the systems and acquire them. That is probably the key challenge.

● (1730)

Mr. Pat Kelly: The speed of procurement is a factor, then.

Dr. Wesley Wark: Yes.

The Vice-Chair (Mr. James Bezan): We're running out of time here. We have to be judicious in these last few minutes.

Go ahead, Mr. Fisher.

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

Thank you to our witnesses for being here today.

We've heard a fair bit today about critical infrastructure. Ms. O'Connell asked about it in the last panel, and I think Ms. Kramp-Neuman talked about it as well. I'm wondering particularly how certain sectors could be a target for state-sponsored cyber-attacks as a means to attack Canada without the use of conventional military means.

I am interested in thoughts from both of you, but perhaps one we'll get in writing and one we'll get from Mr. Wark. I am interested in the sectors that you see as being under the greatest threat. I think about the Rogers outage and I think about how that impacted people all across Canada. I think about natural disasters like Fiona. It outlined our reliance on power, telecoms, gas and ATMs. The fact is that the Internet was once a luxury, and now it seems to be a necessity. You can't do a thing when something like this happens.

I am interested in your thoughts, Dr. Wark, on which sectors you see as being under the greatest threat.

Dr. Wesley Wark: Thank you for the question.

I'm going to surprise you, perhaps, by saying that there is one sector that we have not typically considered being part of critical infrastructure but that we need to consider in the future, and that's space. Increasingly, we're going to rely on space-based platforms for critical infrastructure, communications, monitoring of climate change impacts and a whole range of things.

My hope is certainly that in the forthcoming critical infrastructure strategy the government is working on, they will include space as a new sector. I would say that is probably the most vulnerable area, because it is so new and because it is changing and developing so rapidly. There's a Canadian role to play there. Space is a big one.

The other thing I would say is that signals intelligence agencies, CSE and Five Eyes and other ones, have said that what we're facing are probing attacks at the moment by foreign state adversaries who are trying to figure out how our critical infrastructure systems work and where the vulnerabilities are. Will we actually see attacks on those systems, short of war? That's very hard to know. Probably, the answer is that it's not likely because it has such an escalatory impact, but there are certain aspects of it, in particular in terms of democratic practices and election infrastructure, for example, that can be vulnerable.

I would say that space and those critical infrastructure systems that feed our democratic needs around elections in particular are two key issues.

Mr. Darren Fisher: Thinking about Fiona and Atlantic Canada, does a natural disaster provide an opportunity for a cyber-attack, acknowledging the reliance on such things as the energy sector, the banking system and so on?

Dr. Wesley Wark: That's an interesting question. I don't really know the answer to it.

I think for those adversaries that might be paying attention, it would be a thing to look at to see how well a country can respond or recover and where the vulnerabilities might be exposed in terms of critical infrastructure, communications, services and so on. It's probably more in the field of study than anything else.

Mr. Darren Fisher: Okay.

We talked a little bit about conventional warfare. We always say that the war of the future won't look like what we're seeing in Ukraine on the ground. I don't want to put words in your mouth, but you mentioned “in conjunction”, or “hybrid” and those things. I think it was you who said that the scope of Russian cyber-threats is very “sophisticated”, but what we're seeing is a lack of success by Russia with regard to the war in Ukraine.

I'm wondering what your thoughts are on that hybrid warfare. We've said for years that it's not going to be the battlefields of yesterday where we see wars, yet we're seeing this little bit of a hybrid now with some cyber, some disinformation and some traditional conventional warfare.

Dr. Wesley Wark: That's a fascinating question.

I think the thing that the Ukraine war reminds us of is that at the moment a lot of it looks like the First World War. There's always that element of brute force, of machine on machine, man on man and woman on woman in combat these days, which we mustn't forget.

I think the expectation going into the outset of the Ukraine war was that the Russians would be more sophisticated actors in terms of both conventional military capabilities and cyber-capabilities. They haven't proven to be either—fortunately. That's not to say that they're not trying to learn and do better, and obviously the outcome of their war in Ukraine is very much up for grabs at this stage.

We have an inclination to over-invest in fears of the future of warfare and technological change and so on, but it's important to look at that.

● (1735)

Mr. Darren Fisher: Thank you.

The Vice-Chair (Mr. James Bezan): Thank you. Your time has expired, Mr. Fisher.

We have five minutes left. We're going to split that half-and-half between Monsieur Desilets and Ms. Mathyssen.

[*Translation*]

Mr. Luc Desilets: Thank you, Mr. Chair. By the way, your French was excellent earlier.

Given my fellow member's wonderful idea, I'd like Mr. Shull to get back to the committee in writing with the answers to three questions.

First, can a cyber-attack be considered a war crime?

Second, what type of response might we expect if a NATO country were the target of a major cyber-attack? Would it be considered an attack against NATO? Would NATO be at war?

This third one is pretty broad. Mr. Wark, earlier you mentioned certain recommendations you would like to see in the report.

Mr. Shull, are there recommendations you would like the committee to include in its report?

Mr. Wark, this one is for you. It ties in with my last question about disinformation, which I consider to be extremely dangerous. It's all over the place right now. I used to be a school principal, so young people and education come to mind. Schools need to work on prevention to help young people distinguish between real information and fake information.

Prevention aside, how much of the responsibility falls on the media and how much rests with us, as elected officials?

[*English*]

The Vice-Chair (Mr. James Bezan): You can answer that in one minute or less.

Dr. Wesley Wark: Thank you, Mr. Chair.

I would say that the media plays a huge role. Of course, the media as an institution has changed before our very eyes in the last couple of decades. There's the mainstream media, and there's everything else that's out there. I would say that the mainstream media has a strongly embedded code of practice and ethics to try to ensure that they are reporting, as they see it, truthfully and holding themselves to account. That is not, of course, the case for actors in social media, who have no such code of conduct.

At the end of the day, I think it really depends on the ability of ordinary Canadian citizens to decide where they want to get their sources of information from and, hopefully, it's not purely in an echo chamber kind of fashion, where they just get their sources of information from places that confirm pre-existing beliefs. My hope is that many Canadians ultimately will be able to do that.

The Vice-Chair (Mr. James Bezan): Ms. Mathyssen, the last question goes to you.

Ms. Lindsay Mathyssen: Thank you.

Interestingly, Mr. Wark, in a previous study we were talking about Arctic security.

We had Professor Byers here. He said that one of the biggest things we and the government have to focus on is the entire replacement of the RADARSAT Constellation system. That was one of his biggest points. Can you speak to that? Do you agree or disagree? It's a big point.

Dr. Wesley Wark: I'll be very brief and refer you to a recent Auditor General's report on Arctic surveillance. I think it made the very important point that the Canadian practice for procuring new satellite capabilities, particularly ones that can assist in monitoring our Arctic space, both for military purposes and for civilian purposes, is a very slow-moving one. We face a circumstance in which current satellite systems like RADARSAT and the trio of satellites may go out of operational capability before we're able to replace them.

There is this gap between long-term DND and Canadian Space Agency planning for the replacement of these systems and when they may run out of capabilities, and that gap I think clearly has to be closed. The RADARSAT Constellation is a very important attribute for Canada, and I think that, overall, Canada needs to invest much more heavily in satellite-based capabilities for our own needs.

● (1740)

Ms. Lindsay Mathyssen: To jump around a bit, we've talked a lot about needs in terms of having the right personnel, the people, within cybersecurity to do those jobs. Is Canada doing enough? Can the Government of Canada do more in terms of training those people?

I know that's a bit of a catch-up, but what can be done in terms of the government's investment in people coming into these jobs?

Dr. Wesley Wark: I think that would be an interesting follow-up question for CSE officials, who have their own training systems within CSE, about the extent to which they are able to migrate those training systems out to other federal government departments and agencies and out to the private sector.

I don't know. I suspect it's an important gap that you've identified.

The Vice-Chair (Mr. James Bezan): Thank you. The time has expired.

I apologize to Ms. Gallant and Ms. O'Connell that we weren't able to get their questions in.

Dr. Wark, as a Canadian who's proud of my Ukrainian heritage, I appreciate all your comments about the Russian invasion of Ukraine. I found it interesting that you said that a cyber-attack in Ukraine should be considered a war crime.

Just a quick yes or no, is a cyber-attack on a foreign nation an act of war?

Dr. Wesley Wark: I think the simplest answer is that it's not clear in the international law, but I think Canada can take a lead.

We've always taken a lead—or like to think we've taken a lead—in terms of international law developments, particularly at the International Criminal Court, and I would like to see the Government of Canada stand up and support the Ukrainian position on this and say that cyber-attacks on civilian infrastructure are a war crime.

The Vice-Chair (Mr. James Bezan): Thank you very much, Dr. Wark.

Mr. Shull, I thank you as well.

I'd like to remind committee members that our Friday meeting will be, again, on cybersecurity and cyberwarfare. It will be our study with academics, and next week we'll be meeting with DND and CAF officials.

With that, we're adjourned.