HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

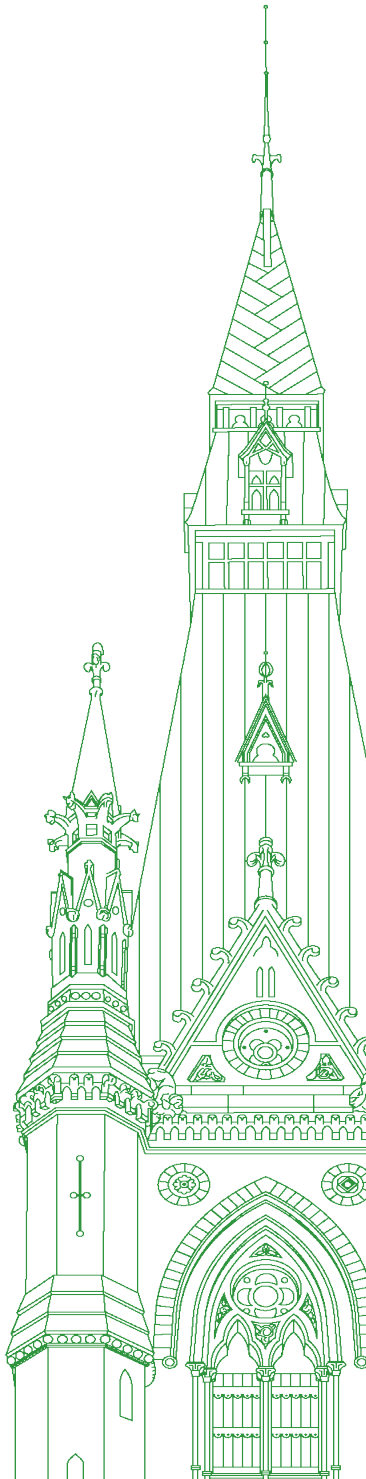
44th PARLIAMENT, 1st SESSION

Standing Committee on Access to Information, Privacy and Ethics

EVIDENCE

NUMBER 132

Tuesday, October 8, 2024



Chair: Mr. John Brassard

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, October 8, 2024

● (1545)

[*English*]

The Chair (Mr. John Brassard (Barrie—Innisfil, CPC)): Good afternoon, everyone.

I call this meeting to order.

[*Translation*]

Welcome to meeting number 132 of the Standing Committee on Access to Information, Privacy and Ethics.

Pursuant to Standing Order 108(3)(h) and the motion adopted by the committee on Tuesday, February 13, 2024, the committee is resuming its study on the impact of disinformation and of misinformation on the work of parliamentarians.

[*English*]

I would like to welcome our witnesses for the first hour today.

From the Royal Canadian Mounted Police, we have Richard Baylin, director general, cybercrime, and chief superintendent, federal policing, criminal operations.

Welcome.

[*Translation*]

We are also hearing from Denis Beaudoin, director general of national security and chief superintendent of federal policing.

Welcome to the committee, Mr. Beaudoin.

[*English*]

We also have Greg O'Hayon, director general, federal policing security intelligence and international policing.

I want to welcome you, sir.

You have up to five minutes for an opening statement to address to the committee.

[*Translation*]

Mr. Beaudoin, you have the floor for five minutes.

C/Supt Denis Beaudoin (Director General, National Security and Chief Superintendent, Federal Policing, Royal Canadian Mounted Police): Thank you, Mr. Chair.

My name is Denis Beaudoin, and I am a chief superintendent and the director general responsible for foreign actor interference for the federal policing national security program at the Royal Canadian Mounted Police, RCMP. I am joined today by Richard Baylin, chief superintendent of federal policing criminal operations on cybercrime, and Greg O'Hayon, director general of federal policing security intelligence.

First, I would like to thank you for the opportunity to discuss this issue. The malicious intrusion into Canada's democratic processes by hostile foreign actors is one of the RCMP's highest priorities.

To be clear, foreign interference affects every aspect of society. This includes the very foundations of our democracy, the fundamental rights and values that define us as a society, our economic prosperity, the critical infrastructure essential to our well-being, and our sovereignty.

Foreign actors seek to advance their objectives through several tactics, including state-backed harassment and intimidation of communities in Canada, manipulating the discourse at every level of our political system, and using malicious and deceptive tactics to influence our democracy.

Make no mistake—foreign governments are conducting campaigns of online disinformation to undermine our democratic processes and institutions, as well as to erode citizens' faith in democracy.

The RCMP has a broad mandate related to national security and cybercrime to ensure public safety by investigating, disrupting and preventing foreign interference. It draws upon provisions from various pieces of legislation, including those recently enacted in Bill C-70, as well as other offences under the Criminal Code. When investigating disinformation campaigns, the RCMP works closely with domestic and international partners to identify relevant evidence but sometimes disinformation campaigns may not constitute criminal conduct.

With these considerations in mind, I will briefly summarize the RCMP's role in contributing to the protection of Canada, its citizens, residents and elected officials from foreign interference activities.

[*English*]

In 2019, the Government of Canada announced its plan to protect democracy, to defend Canadian democratic institutions. This included measures to strengthen elections against various threats, including cyber threats and foreign interference. From the outset, the RCMP has been a committed contributor to these whole-of-government efforts.

Elected and public officials are central figures in our democracy's political system, as they shape our policies and laws. This role makes them key targets for foreign states, which may try to influence or coerce them to take policy positions that align with their interests. As such, the RCMP recently briefed parliamentarians, in partnership with other government agencies, on the threat of foreign interference. The RCMP is also leading initiatives to raise awareness with police forces across the country on the new legislation included in Bill C-70, as well as on the threat of foreign interference.

The RCMP is also an active member of the security and intelligence threats to elections task force—otherwise known as SITE—a working group that coordinates collection and analysis efforts concerning threats to Canada's federal election processes. This group is Canada's principal mechanism for monitoring threats of hostile state interference during elections and also consists of experts from CSIS, the CSE and Global Affairs Canada.

The RCMP's federal policing of cybercrime focuses investigative efforts on the highest level of cybercriminality and works closely with domestic and international partners to identify, disrupt and prosecute the most serious threats within the cybercrime ecosystem, which cause significant economic or other impacts to Canadian interests at home and abroad. The RCMP's federal policing cybercrime investigative teams and cyber liaison officers abroad focus on the prevention, enforcement and disruption of high-value threat actors and prolific cybercrime enablers who facilitate sophisticated crimes, such as malware, ransomware, espionage and foreign interference, as well as attacks against government institutions, key business assets and critical infrastructure of national importance.

As members of this committee are well aware, there has been an increase in threats to public officials in recent years. Because we recognize the personal impact of this trend, as well as the harm it causes to our democracy, this issue remains a key priority for the RCMP, and we will continue to counter these threats through our federal policing responsibilities, as well as through our engagement with other police forces and the diaspora communities.

With threats of this magnitude, collaboration between the public, the police of jurisdiction and the Government of Canada partners will continue to be an important aspect of protecting Canada against foreign interference.

The protection of Canada's democratic processes and the safety of its citizens and residents is paramount for the RCMP. It will be important for all aspects of society to work together to protect against foreign interference in this space.

Thank you.

● (1550)

The Chair: Thank you, Mr. Beaudoin.

I do want to thank the RCMP. Earlier this year, we, as a committee, had the opportunity to visit the academy in Ottawa, and through Deputy Commissioner Larkin, we got a pretty comprehensive briefing on the tools that are used for data extraction, for monitoring cybercrimes, etc., and foreign interference.

Were any of you at that session? No? Okay. Mr. Fisher was; I see his hand in the back.

We are going to start with our first round of questioning. It's six minutes on all sides; every party has six minutes. We are going to start with Mr. Barrett.

Go ahead, please, Mr. Barrett.

Mr. Michael Barrett (Leeds—Grenville—Thousand Islands and Rideau Lakes, CPC): Is the RCMP adequately funded to address the cyber-threats that Canada faces?

Chief Superintendent Richard Baylin (Director General, Cybercrime and Chief Superintendent, Federal Policing, Criminal Operations, Royal Canadian Mounted Police): Last week, Deputy Commissioner Flynn, I think, said quite clearly that you wouldn't be able to talk to a chief of police anywhere in Canada and not hear that there would be an interest in discussion around resourcing. However, I can tell you that the RCMP does have cyber teams across the country. We have worked to staff these teams, to build teams, to build training and to adapt to the threats, and we do surge resources to that. I do believe that we are, at this time, able to work at a level of criminality that is representative of a threat, yes.

Mr. Michael Barrett: Okay.

Other police forces need more resources, but the RCMP does not. That is what I'm extrapolating from your answer.

Are you properly resourced to address the threats facing Canada? A quick yes or no would be great.

● (1555)

C/Supt Richard Baylin: It's worth having a discussion about resources, absolutely.

Yes, I'll say we are resourced, right now, to deal with the threat.

Mr. Michael Barrett: Okay.

Could the government be doing more to deter foreign interference and protect Canadians from intimidation from hostile foreign states?

C/Supt Denis Beaudoin: It's hard for the RCMP to comment on the government, Mr. Chair.

What we can say is that we welcome the new legislation, Bill C-70, which was recently enacted on August 19. We look forward to working with our partners at PPSC and testing this new legislation.

Your earlier question was on cybercrime, national security and foreign-actor interference. We received funding recently through the SIAMACT. Nonetheless, with the rise of violent extremism in Canada, it's certainly competing with our ability.

Mr. Michael Barrett: What is operability like between the RCMP and CSEC when dealing with these types of issues? CSEC is self-described as being “responsible for foreign signals intelligence, cyber operations, and cyber security.” Is there a table that exists for addressing cyber-threats from hostile foreign states targeting Canadians?

I just need a very quick answer.

C/Supt Richard Baylin: The short answer is, yes, there is.

Mr. Michael Barrett: Okay. What is the name of that?

C/Supt Richard Baylin: It would be the NCRU, which is the national cybercrime coordination centre unit. There are a number of other committees and meetings that discuss threats as they occur.

Mr. Michael Barrett: If a Canadian were targeted by a hostile foreign state—a state-sponsored malware or hacking attack that was intercepted by you or your partners at the CSEC table—how would that Canadian come to learn what had happened? Would you notify the individual that a foreign state targeted them?

C/Supt Richard Baylin: It depends on the nature of what was found and who found it.

That committee would be where a discussion would take place, and where deconfliction would take place. Then a decision would be made, going forward, as to the nature of that threat and how to deal with it.

Mr. Michael Barrett: Of course, we had an example where parliamentarians across party lines were targeted by a foreign state-sponsored attack—APT31. It was revealed earlier this year. The individuals targeted were all legislators. None were notified by anyone who sits at that table. It's interesting to know that the conversation took place. I understand that paper got shuffled over to the House of Commons. That gives cold comfort to the affected individuals and leaves other Canadians wondering what would happen to them if they were being targeted. Would they be informed, or do they have to depend on their employer being notified, then informing them? Should they wait for the FBI to let them know? That is what took place in this case. It's how Canadians came to know this had occurred.

There are a couple of issues federal policing is addressing right now—investigations into a few issues dealing with the government.

Are you able to provide us with an update on the investigation dealing with the $60-million ArriveCAN scam?

C/Supt Denis Beaudoin: We're not going to comment on any investigation. Also, this is outside the national security portfolio, so I'm definitely not the right person to answer these questions.

Mr. Michael Barrett: Did he say that he's not able to answer the question? I can't hear what he's saying.

The Chair: That's what I heard.

Mr. Beaudoin, if you raise your voice a bit more, it would be helpful.

I'm having a tough time hearing, but he did say that, Mr. Barrett.

C/Supt Denis Beaudoin: I apologize.

The only thing I said is that we're not going to comment on any investigation. This one is outside of my responsibility, so I'm certainly not the right person to get these questions directed at him.

● (1600)

The Chair: Thank you, sir.

Thank you, Mr. Barrett.

Mr. Housefather, you have six minutes. Go ahead, please.

Mr. Anthony Housefather (Mount Royal, Lib.): Thank you, Mr. Chair.

Thank you, guys, for coming.

Is the RCMP investigating right now as to whether there are foreign countries that are involved in the university encampments that happened last year, the protests that are happening to glorify terrorism and glorify Iran and what Samidoun is doing? Are you investigating this?

C/Supt Denis Beaudoin: Again, we're not going to be able to comment on any specific investigation today.

Mr. Anthony Housefather: I'm not you asking to comment. I'm asking if you're looking into it.

C/Supt Denis Beaudoin: Well, you're asking me to comment on investigations, and I've just explained that we're not going to be able to provide any details on investigations today.

Mr. Anthony Housefather: I don't think a yes-or-no answer as to whether or not.... Are you concerned?

C/Supt Denis Beaudoin: Yes. We are definitely monitoring what is happening in Canada, and we have a number of folks looking at the current situation.

Mr. Anthony Housefather: When we have demonstrations like the one we had yesterday in Montreal, where McGill University buildings were damaged and where we had previous knowledge that these demonstrations were going to occur, what is the RCMP's role with respect to coordinating with local police?

C/Supt Denis Beaudoin: We engage with police jurisdictions early when we know some things will occur, and we're in touch with them. When something does occur, then we're going to liaise to see if there's a national security nexus to the incident.

Mr. Anthony Housefather: Prior to something actually occurring, are you investigating to see if there are national security nexuses to the planned demonstration and advising local law enforcement accordingly?

C/Supt Denis Beaudoin: Yes.

Mr. Anthony Housefather: Okay.

I understand why, in the question that Mr. Barrett had asked, there would be times when you would discuss whether an individual should be made privy to information in terms of a foreign threat if you thought that perhaps the individual was colluding with or was an agent of the foreign source, but in the event that you realized the person was blameless and was being made susceptible to threats from a foreign source, what would be the reason why the RCMP would not advise that individual?

C/Supt Denis Beaudoin: There's a variety of reasons, including when we are dealing with foreign states conducting this investigation. There could be caveats as to what we can do with the information. It could be a request from another agency to not act on them. There's a wide range of reasons why we wouldn't at some point.

Mr. Anthony Housefather: You understand, of course, that to a parliamentarian that's a very scary prospect, right? There's a threat against me, for example, or against anyone else, and you're aware of it, but I'm not.

There seems to be.... I don't know what the policing jargon would be, but it seems to be a disconnection between what the person being threatened by that foreign source would want to know and what you would be able or would want to tell them.

How do you protect somebody in the event that they're not aware of this impending threat from a foreign source, or an ongoing threat from a foreign source, if you can't tell them because, for example, your source in another country asked you not to do so?

C/Supt Denis Beaudoin: Yes. Like I said, we take the security of all Canadians, including parliamentarians, to heart. I briefed all parties earlier in June myself to ensure all parliamentarians are aware of the threats that may be upon you. The RCMP takes this extremely seriously.

On specific cases, like I said, we're not going to comment on investigations, but in general, as I said, there's a number of issues that come into play that we have to deal with. Sometimes we get to a resolution where we can advise a person. Sometimes there are reasons operationally why we don't, and sometimes we don't know either.

Mr. Anthony Housefather: Do I have any time left, Mr. Chair?

The Chair: You have a minute and a half.

Mr. Anthony Housefather: I want to come to communications, then, because from what I gather, in the United States law enforcement, the FBI is far more willing to disclose information more rapidly and more clearly than the RCMP. I see that with the Trump attempted assassination, for example, where there's information that I think in Canada wouldn't have come out for a significant amount of time, but that in the United States, after the attempted assassination in Pennsylvania, was very forthcoming. The law enforcement agencies were out there giving information.

I think there is a perception in Canada that the RCMP should communicate in a much clearer and more forthcoming way, particularly as it relates to threats. What are your thoughts on that?

● (1605)

C/Supt Denis Beaudoin: Privacy legislation in our two countries is extremely different. That's something we need to take into account as to what we do share. However, we're out there. We're in the public. We're doing many campaigns to assist Canadians at all levels to understand the threats to different diasporas. We're working to ensure that people are aware of the current situation and the threats that are happening from foreign states.

Mr. Anthony Housefather: Thank you, Mr. Chair.

The Chair: Thank you, Mr. Housefather.

[*Translation*]

Before giving the floor to Mr. Trudel, I want to tell the witnesses that each member has six minutes or less to ask questions. If a member interrupts you, don't take it personally. That's because time flies during questions and answers.

Mr. Trudel, you have the floor for six minutes.

Mr. Denis Trudel (Longueuil—Saint-Hubert, BQ): Thank you, Mr. Chair.

Gentlemen, thank you very much for being here today.

I'll go back to the last question that my colleague Mr. Housefather asked because I found it interesting. He was talking about the attack on Donald Trump. He mentioned that information was obtained more quickly in the United States than it would have been here in Canada. You answered that the laws were different in the United States.

What does that have to do with this particular file? What changes could Canada make to its legislation in order to have access to such information?

C/Supt Denis Beaudoin: First of all, I can't comment on the time the Federal Bureau of Investigation, or FBI, takes to provide information on a given situation. However, in general, Canada's privacy legislation is much more restrictive than that adopted in the United States.

If parliamentarians want to debate it, that's one thing, but right now, it's not possible to make certain information public because of privacy legislation.

Mr. Denis Trudel: It seems that, in the United States, the FBI doesn't feel the need to hide information, whereas that's the case here.

What can you tell us about that?

C/Supt Denis Beaudoin: I don't think it's a matter of hiding information, Mr. Trudel.

I can't speak to what the FBI does or doesn't want to do. The question should be put to them. At the RCMP, we're not there to hide information. As I said, we have a number of public awareness campaigns to inform people about…

Mr. Denis Trudel: The threat.

C/Supt Denis Beaudoin: That's the word I was looking for. The nature of the threat has changed in recent years.

At the RCMP, we try to be as transparent as possible, but when investigations are ongoing, we can't share certain information.

Mr. Denis Trudel: Correct me if I'm wrong, but you seem to be saying that the threat is worse now than it was five or 10 years ago.

Are you also implying that you don't have the tools right now to combat this threat?

C/Supt Denis Beaudoin: As I said, the nature of the threat has changed. We have to deal with the ideological nature of violence by individuals, which is new. Foreign interference is certainly a new threat, and we've seen it over the past decade or so.

Any investment by the government in programs related to these threats is welcome, and the RCMP will always be grateful for it. It certainly helps us do more for Canadians.

Mr. Denis Trudel: Are there active investigations involving parliamentarians in Canada right now?

C/Supt Denis Beaudoin: I can't comment on that today, Mr. Trudel.

Mr. Denis Trudel: Earlier, in your opening remarks, you said that interference wasn't always criminal conduct.

Can you explain to me exactly what you meant by that?

From what I understood, there could be legal and criminal interference. However, I imagine that you intervene only when it is criminal. So we have to make a distinction between the two.

C/Supt Denis Beaudoin: We were invited to appear before you to talk about misinformation and disinformation. That is why I will speak only on this subject.

If someone's opinion differs from that of other people, that's not necessarily criminal. According to the legislation that came into force in August, a criminal act is committed when the purpose of the disinformation is to influence an electoral or government process. So we have to prove that certain elements are present in order to investigate a criminal offence.

● (1610)

Mr. Denis Trudel: Earlier, you said that the new threats were more violent than before.

What were you referring to?

C/Supt Denis Beaudoin: I was referring to the ideologically motivated threat—the threat of ideologically motivated violent extremism, or IMVE.

Mr. Denis Trudel: You're not talking about physical violence.

Is that correct?

C/Supt Denis Beaudoin: No, it's ideologically motivated violent extremism. This type of threat has also increased. We need to redirect some of the existing resources within national security based on the type of threat and the intelligence that is shared with us.

Mr. Denis Trudel: All right.

I saw an article in The Globe and Mail this morning. It says that the RCMP is struggling to address the threat of foreign interference from countries such as China, India, Iran and Russia, because it operates under a muddled mandate.

Do you think your mandate is muddled?

What mandate would you need to effectively address threats from those countries?

What is the current legislation missing, and what tools do you need to deal with the issue?

C/Supt Denis Beaudoin: We got some new tools about six weeks ago. We're eager to study how they work and put them to use. Certainly, we will always need more resources.

As for having a muddled mandate, I don't think that's true. As threats evolve, we definitely have to adapt. Our investigators have to examine any new threat. Accordingly, we have to provide training. Since the situation is constantly changing, it's also important to educate the public on an ongoing basis.

Mr. Denis Trudel: An election may be called soon.

Are you doing anything specific to prepare should that happen?

Mr. Greg O'Hayon (Director General, Federal Policing Security Intelligence, Intelligence and International Policing, Royal Canadian Mounted Police): I'm the RCMP representative on the Security and Intelligence Threats to Election Task Force. We've been preparing for the next election for at least eight months precisely because we anticipate interference.

When it comes to threats—

The Chair: Please keep it brief, Mr. O'Hayon.

Mr. Greg O'Hayon: At the time, it was thought that—

The Chair: Unfortunately, the member's time is up.

You'll get a turn for two and a half minutes next time, Mr. Trudel.

[*English*]

Mr. Green, go ahead, please, for six minutes, and then maybe a little bit more after that.

Mr. Matthew Green (Hamilton Centre, NDP): Thank you.

As part of the committee study on the use of social media platforms for data harvesting and unethical or illicit sharing of personal information for foreign entities, Brigitte Gauvin, the acting assistant commissioner of federal policing for national security in the RCMP, noted that the RCMP's national security program investigates criminal activities, and if the activities pertain to foreign interference, an investigation takes place. However, she emphasized that the RCMP does not investigate social media for misinformation, disinformation or attempts to influence the platform. It investigates only if there is criminal activity.

Why is the RCMP not investigating misinformation, disinformation or attempts to influence on social media platforms?

C/Supt Denis Beaudoin: Like I said earlier, some instances of misinformation and disinformation may not be illegal in themselves, so the RCMP needs to look at whether a criminal offence has taken place. When we establish this, of course we will investigate, and it falls under the national security mandate. When it involves cybercrime, then my colleague, Mr. Baylin, would investigate.

Mr. Matthew Green: Thank you.

For the purpose of this committee, given the study that's before us, in what context, if any, could the spread of disinformation online be the subject of an RCMP criminal investigation?

C/Supt Denis Beaudoin: Like I mentioned earlier, it would be in relation to the goal of influencing government processes. That would make it illegal.

● (1615)

Mr. Matthew Green: When was the last time an investigation like that occurred? You don't have to give specifics, but give us a sense of how often this might be the case.

C/Supt Denis Beaudoin: It was when one of the new sections was just enacted a few weeks ago.

Mr. Matthew Green: Since this new section has been enacted, there's already been an investigation under the new parameters. Is that correct?

C/Supt Denis Beaudoin: No, the only thing I'm saying is that it's a very new law, so right now, I'm not aware of it being used, but again, there are many investigations across the country.

Mr. Matthew Green: Prior to that, there was nothing. Is that what I'm hearing?

C/Supt Denis Beaudoin: On disinformation, it doesn't mean that disinformation could come with threats, for example, and then we could use the Criminal Code. We need to look at all the facts and not just at the term “disinformation”. There's a wide range of the Criminal Code that we could use.

Mr. Matthew Green: I'm sorry. I need clarity because I'm not understanding the response, somewhat. I understood you to say that the criminal threshold is if there was evidence of an influence campaign or of foreign interference that would change the government's policy. Is that not correct?

C/Supt Denis Beaudoin: Yes, it's interference in government processes.

Mr. Matthew Green: Okay. With that being said, have you, in your career, ever had an investigation that met that threshold?

C/Supt Denis Beaudoin: Like I said, not personally because this is a new law; it was enacted about six weeks ago.

Mr. Matthew Green: Again, I'm sorry; I'm not trying to be stubborn here. Just to be clear, prior to that, there was no such investigation.

C/Supt Denis Beaudoin: For government processes.... No. However, what I was trying to explain is that there are other sections in the Criminal Code where disinformation itself may not constitute the offence, but a foreign state actor could have committed other offences in the Criminal Code that we could utilize.

Mr. Matthew Green: Okay. Again, in our study on social media platforms, Bryan Larkin, the deputy commissioner of the RCMP's specialized policing services, said that the RCMP has “ongoing relationships with all social media platforms” through its national cybercrime coordination centre and that the RCMP also has “protocols in place, particularly around [things like] child exploitation and harm to young people”.

Does the RCMP, given the new law, now have a specific protocol in place for dealing with foreign states spreading misinformation online in Canada?

C/Supt Denis Beaudoin: I'm not sure I understand the question, sir. Are you asking if we have contacts within the social media platforms, in regards to disinformation?

Mr. Matthew Green: Mr. Larkin said that you did.

C/Supt Denis Beaudoin: Yes, we do.

Mr. Matthew Green: I'm asking you this: Do you have specific protocols in place for dealing with foreign states spreading misinformation online in Canada, whether it's through the national cybercrime coordination centre or any other policy or protocol you might have within the RCMP?

C/Supt Denis Beaudoin: We maintain, especially on the major platforms, contacts with their security branch on a wide range of investigations because social media is used by all criminals, not just for disinformation, so we maintain contacts with them to obtain information—

Mr. Matthew Green: Sir—

C/Supt Denis Beaudoin: —when needed, so—

Mr. Matthew Green: I'm sorry. I'm going to ask this question, and it's for the purpose of the study. Can you please provide this committee with the specific protocols that you have in place when dealing with foreign states spreading misinformation online in Canada? Can you do that for us?

C/Supt Denis Beaudoin: I'm trying to answer the question, sir. What I was trying to explain is that we don't have specific.... We don't police the Internet. We don't have specific.... We need a victim, so when people come forward with allegations of disinformation and criminal offences that would have occurred on the platform, then we have protocols to engage with the social media companies to ensure we capture this disinformation.

Mr. Matthew Green: Can you give us some examples of how the RCMP engages with the public or with the private entities that you've just listed, or with vulnerable communities, to educate them about the risks of foreign interference activities?

C/Supt Denis Beaudoin: Yes. You're asking for examples. If we get a complaint from people who would have received threats online from a foreign state or actors of a foreign state, then we would engage the social media platform, sometimes on an urgent basis if there's threat to life, to obtain information on the perpetrator, to ensure public safety and to stop the threats to that person.

● (1620)

The Chair: You'll have another chance, Mr. Green. We're going to come back to you in a few minutes.

That concludes our first round. Mr. Cooper is going to start us off with our second round for five minutes.

Go ahead, Mr. Cooper.

Mr. Michael Cooper (St. Albert—Edmonton, CPC): Mr. Chair, on April 10 of this year, The Globe and Mail reported that in 2019 the then Liberal candidate and now the member of Parliament for Don Valley North was tipped off by a Liberal Party member that he was being monitored by CSIS.

It was confirmed at the public inquiry on foreign interference that only a select few top Liberals, closely connected to the Prime Minister, were present at a classified CSIS briefing where this information was communicated. Three top Liberals received the briefing, including Azam Ishmael, the national director of the Liberal Party. Mr. Ishmael then briefed Jeremy Broadhurst, who did have the requisite security clearance, Broadhurst being a top adviser to the Prime Minister. Broadhurst then briefed the Prime Minister.

What we know is that five top Liberals, including the Prime Minister himself, were briefed. That information resulted in a leak in which a candidate, now a member of Parliament, was tipped off that he was being monitored by CSIS.

Can you confirm that knowingly leaking classified information is an offence under sections 13 and 14 of the Security of Information Act?

C/Supt Denis Beaudoin: Yes. Leaking classified information is a criminal offence.

Mr. Michael Cooper: Would it be fair to say that it is a serious offence punishable by up to 14 years behind bars?

C/Supt Denis Beaudoin: Yes. I believe you're correct.

Mr. Michael Cooper: Following The Globe and Mail report, I sent a letter to the commissioner of the RCMP, dated April 12 of this year, bringing to his attention this apparent serious breach of national security whereby evidence points to five top Liberals, one of whom or more than one of whom may have betrayed their oath of secrecy and leaked classified information undermining ongoing national security operations. On May 3, 2024, I received a letter from the commissioner acknowledging my letter.

Since that time, has the RCMP opened an investigation?

C/Supt Denis Beaudoin: Mr. Chair, I won't be able to comment on any facts of whether we have or not an investigation.

Mr. Michael Cooper: Okay, fair enough: I understand that you might not be able to comment on it if an investigation has been opened, but the commissioner did say in his letter that the RCMP would examine this information.

Has the RCMP examined the information surrounding serious allegations contained in The Globe and Mail report about a major national security breach involving top Liberals close to the Prime Minister, perhaps even the Prime Minister himself?

C/Supt Denis Beaudoin: Mr. Chair, again, I'm not going to comment on this question.

Mr. Michael Cooper: Well, has the RCMP contacted any of these top Liberals?

C/Supt Denis Beaudoin: Mr. Chair, again, I'm not going to comment on—

Mr. Michael Cooper: Well, I think there needs to be a certain level of transparency. I know you can't comment on any ongoing investigation. I understand that. I respect that.

I'll put it to you this way: Has the Prime Minister contacted the RCMP? Has he referred this national security breach to the attention of the RCMP?

C/Supt Denis Beaudoin: Mr. Chair, it's the same answer: I'm not going to comment on it.

Mr. Michael Cooper: Well, it's interesting that you're not able to comment.

It's interesting further that the Prime Minister has been silent about it. He certainly hasn't said that he has referred the matter to the attention of the RCMP.

We have seen the Liberals at committee try to obstruct efforts to get to the bottom of this major national security breach. Frankly, what we've seen in terms of the Prime Minister's silence and obstruction by Liberal MPs—no doubt directed by the Prime Minister—is part of a pattern with this Prime Minister.

It's part of a pattern of a Prime Minister who has continually put his personal and partisan political interests and that of protecting top Liberals implicated in a serious crime—leaking classified information that may have compromised a CSIS investigation into Beijing's interference activities—ahead of our national security.

Canadians deserve better.

Thank you, Mr. Chair.

● (1625)

The Chair: Thank you, Mr. Cooper.

We're going now to Mr. Bains for five minutes.

Go ahead, sir.

Mr. Parm Bains (Steveston—Richmond East, Lib.): Thank you, Mr. Chair.

Thank you to our respective director generals for joining us today.

I want to talk about Bill C-70. I think you mentioned that it's a welcome legislative change with some measures that it brought in. Can you talk about cybersecurity and how it intersects with security of information and signals intelligence? Do you feel sufficient improvements have been made through that legislation? Does it allow you to have more powers and more ability to do the work of targeting misinformation, disinformation or any foreign threats through information specifically?

C/Supt Richard Baylin: I can comment on one aspect of that from a cyber perspective. Certainly, it does give us more than we had. As my colleague, Mr. Beaudoin, had mentioned, it's very early days. We will see where that takes us and how much more room that gives us, but absolutely, there is more there than what we had before.

Mr. Parm Bains: These changes have been brought in after decades of following the same measures, but for the new offences, do the resources that are now available to you satisfy your needs? I understand that it's new right now and you're probably working through it. I think you said that as of last week some new laws had just been enacted. Can you speak to the processes that have been in place and how much work you still need to do to really roll this out?

C/Supt Richard Baylin: I can speak to that, to a certain extent. Over the last year to 18 months or maybe even two years, the threat related to cyber has evolved. Initially, cyber was looked at much more as a tactical threat and a criminal threat. Most of the evolution of cybercrime and cyber investigative teams was focused on that aspect. It's only more recently that our focus has opened up to looking at things like we're talking about here today, such as disinformation aspects around more of a strategic threat from a national security perspective.

That's where this legislation has led us. We'll continue to work within the framework of that to see where it goes, but yes, absolutely, we do have more now than we did.

Mr. Parm Bains: Does this allow you to increase your work with other jurisdictions on transnational misinformation campaigns where they can be monitored with allies and things like that? Does that give you more abilities there?

C/Supt Richard Baylin: It gives us more aspects of criminality to speak to, because we're speaking beyond just, as I mentioned, that tactical threat, the criminal threat and working within this space. Yes, within our law enforcement and like-minded communities, these are the discussions that we do have now.

The "ecosystem" of cyber that the RCMP likes to refer to, as do our partners, is made up of many parts. Many of those parts actually cross paths from that criminal side into that national security side. It might be some of the same threat actors and some of that same ecosystem and infrastructure that we focus on, but we're now looking at it through a different lens, a national security lens, and that is helpful to us as well.

Mr. Parm Bains: On the threat actors piece, have you identified specific platforms? We've seen how toxic X has become. Are you monitoring more on the social media side? I know you said you don't police it, but are you noticing an increase in threats in certain spaces, like the dark web and these other spaces, that are available to people? Also, what actions you have taken to include into your processes?

● (1630)

C/Supt Richard Baylin: We certainly have seen, over the last number of years, an evolution in that. That has been well reported on in the public not just by the RCMP but by law enforcement writ large, and that, again, is one of the aspects of many of the things we look at.

You mentioned the dark web. Certainly, there are all sorts of different tools that enable criminality, and people who don't have sophisticated means, for example, to engage in things like ransomware and threats and so on are now able to obtain those with a very low level of sophistication and then conduct criminality.

I'm not sure if that answers your question.

The Chair: Thank you, Mr. Baylin.

Thank you, Mr. Bains.

[*Translation*]

Over to you, Mr. Trudel, for two and a half minutes.

Mr. Denis Trudel: Thank you.

Mr. O'Hayon, I'd like to pick up our conversation about the coming election—granted, it's as likely to be called in six months as it is in two weeks or a month.

I know you can't comment on ongoing investigations, but what worries you?

You said you've been preparing for eight months. What's the thing most likely to happen during the election campaign? In concrete terms, what could states such as Iran, China and Russia do?

Mr. Greg O'Hayon: The reason we've been preparing for months is that we face a range of threats, from violent extremism, as my colleague mentioned, to foreign interference.

Mr. Denis Trudel: Can you give me a concrete example?

Mr. Greg O'Hayon: It simply comes down to the fact that we're going to have to take in, analyze, and respond to, a greater amount of information than was the case during the 43rd and 44th general elections.

I can't really tell you what the thing most likely to happen is, but considering that we're here to discuss disinformation and misinformation, I'd say we'll certainly see those two things.

Mr. Denis Trudel: All right.

What kind of disinformation could we see?

For what purpose would a country like China undertake interference activities on social media? Would it be to benefit the Conservatives, the Liberals, the NDP or the Bloc Québécois? How does it work?

Mr. Greg O'Hayon: The strategy and goals vary depending on the country. The documents that have been made available through the public inquiry into foreign interference refer to the various strategic goals of countries such as China, Russia, Iran, Pakistan and India.

You have to put yourself in the enemy's shoes and think about what they want. According to the document summaries that have been released under the inquiry, Russia's goal is to stir up trouble, wreak havoc and create social polarization. China's goal, however, is quite different.

Mr. Denis Trudel: Thank you.

The Chair: Thank you, Mr. O'Hayon and Mr. Trudel.

[*English*]

Mr. Green, you have two and a half minutes. Go ahead, please.

Mr. Matthew Green: Thank you very much.

I want to go back to better understand how the RCMP prepared for this meeting, understanding that we're talking about foreign interference.

We've just had, I think, some major revelations vis-à-vis NSICOP. I'm wondering if, in preparation for this meeting, either of the witnesses had the opportunity to reflect on global comparators, other national police services akin to the RCMP that might also be dealing with these same types of situations.

C/Supt Denis Beaudoin: Mr. Chair, is the question how we prepared for the committee?

Mr. Matthew Green: The question is, in preparing for the committee and preparing for this work, for this study, did you take a look at best practices in other jurisdictions?

C/Supt Denis Beaudoin: Yes, we always do, and not just for this committee, Mr. Chair. We were part of the Five Eyes committee.

Mr. Matthew Green: Can you please provide what examples you would use from other jurisdictions that you would have as recommendations for this study?

● (1635)

C/Supt Denis Beaudoin: I'm not familiar with the study, but there are several best practices that we use. One of them that we're trying to do right now on foreign interference is breaking the silos between police services. When I say "silos", it's really raising awareness of transnational repression, because officers on the street may not realize that they're dealing with such a crime, and they may just see it as a threat. For example, we're trying to utilize some of these committees that are already in existence to spread this information, including Bill C-70, to all our colleagues across Canada. That's one example of sharing information.

Mr. Matthew Green: In your opinion, what were the learnings from the NSICOP report?

The Chair: I'm sorry, Mr. Green; I've stopped your time because I want to make sure that our witnesses are clear on what your demand is and what you're asking them. I think it's important for this study that we get an answer. Is there some other way that you want to rephrase it?

I've stopped your time to give you that opportunity.

Mr. Matthew Green: Thank you.

I would ask, because of the nature of the time, if the witnesses from the RCMP would provide to this committee, in writing, any notes they took or any preparation memos they had on examples from other jurisdictions that were dealing with this.

They mentioned that they're always looking at best practices. I'm keen to get recommendations from these witnesses here today for the purpose of our study. I don't know that I've necessarily gotten that, to this point. I just want to provide them the opportunity to provide in writing what direct recommendations they would take, based on best practices from other jurisdictions in law enforcement.

The Chair: I think I'm seeing some heads nod at the end of the table here. I think they understand what the request is.

I will ask, through the clerk, for a follow-up with the parliamentary affairs people in the RCMP to make sure we get a response to that.

Mr. Beaudoin, did you have anything you wanted to add?

C/Supt Denis Beaudoin: No. I just wanted to apologize if I'm not answering the question to the level you're seeking. It's certainly not our will.

The Chair: Okay.

C/Supt Denis Beaudoin: We'll happily provide a written response once we get a clear question and we fully understand the impact—

The Chair: That's why I wanted to have this interaction, so that all of us were clear on what the ask was.

Mr. Green, you still have 40 seconds. Are you good?

Mr. Matthew Green: I'm okay. I'm happy with that.

Thank you for the intervention, Mr. Chair.

The Chair: I'm sorry. I don't normally do that, but I wanted to make sure we had the information. Thank you.

We'll go now to Mr. Caputo, followed by Ms. Shanahan.

Go ahead, Mr. Caputo. You have five minutes.

Mr. Frank Caputo (Kamloops—Thompson—Cariboo, CPC): Thank you, Mr. Chair.

Thank you, Chief Superintendent Baylin, Chief Superintendent Beaudoin and Director General O'Hayon.

I want to pick up from where my colleague Mr. Barrett left off. He was speaking about appropriate resourcing. The Auditor General released a report in June of this past year. I'm not sure if you've read that report or are familiar with it.

Chief Superintendent Baylin, you're nodding your head.

C/Supt Richard Baylin: I think we're talking about the same report, but I'll wait for you to continue the question.

Mr. Frank Caputo: It was a pretty major report in June. It talked about the RCMP and resourcing. It talked about resourcing generally, and my colleague Mr. Barrett asked about resourcing.

I want to take a quote from that report and put it to you, sir. It says this:

> Overall, the Royal Canadian Mounted Police..., Communications Security Establishment Canada, and the Canadian Radio-television and Telecommunications Commission...did not have the capacity and tools to effectively enforce laws intended to protect Canadians from cyberattacks and address the growing volume and sophistication of cybercrime.

That's a direct quote, I believe, of the Auditor General. What do you say to that?

C/Supt Richard Baylin: Thank you for the question, Mr. Chair.

What I would say to that is that we've learned from that report that the evolution of cybercrime has required us to focus our efforts at a higher level. I mentioned the word "ecosystem" earlier. We are evolving our techniques. We are evolving tools.

I did also say that I'm always interested in having a conversation about resourcing and how we can better approach and deal with the aspects of cybercriminality. But I also said earlier as well, you will remember, that the Auditor General report did go back a number of years. When we talk about our initial approach to cybercrime and cyber-enabled crime, frauds and so on and so forth, and where we've now evolved to, that work still needs to continue, but moving away from an incident response-type aspect of cybercrime and working at a level of criminality that is about dismantling a system that enables cybercrime.

We're refocusing a lot of our efforts in that respect to make sure we can adequately deal with the issue.

● (1640)

Mr. Frank Caputo: I'm mindful of that, sir. Given what the Auditor General has said, and given the slow machinations of government and how long it takes, as someone who has prosecuted a great deal of cybercrime, I believe the Auditor General has put it quite clearly that resources are a problem. Resources are a problem. In this instance, the Auditor General highlighted one case with the CRTC where, in order to get around a warrant, I believe a device was essentially wiped or destroyed.

In any event, I will move on to the RCMP superintendents.

Can you confirm that there are no PRC police stations operating in Canada at this time?

C/Supt Denis Beaudoin: Again, I'm not going to comment on the ongoing investigation. It's been well-detailed that there are ongoing investigations on this, so I'm not going to provide any further comments.

Mr. Frank Caputo: With respect, I believe that Mr. Mendicino, when he was Minister of Public Safety, actually publicly commented on this issue in 2023, saying that the police stations had been shut down. I think that this is a matter that concerns Canadians greatly, particularly groups that are targeted. Candidly, I'm a bit surprised that we can't even hear, in Parliament, whether or not there are police stations. I understand that there are active investigations or there might be—I'm not sure whether there might be. How can we not just say yes or no, these things are or are not operating, and how does that jeopardize an investigation?

C/Supt Denis Beaudoin: There is active investigation. To your point, saying there might be, I think it was confirmed that is active investigation. Again, I'm not going to comment further on this subject.

Mr. Frank Caputo: From what I can understand, the RCMP said that they shut these down in 2023. If that's different in 2024, here we are as parliamentarians, studying foreign interference, so I think we should know whether or not there has been a change. Do you have any comment about that?

C/Supt Denis Beaudoin: I don't have any comments, Mr. Chair.

The Chair: Thank you, Mr. Caputo.

Ms. Shanahan, please go ahead for five minutes.

[*Translation*]

Mrs. Brenda Shanahan (Châteauguay—Lacolle, Lib.): Thank you, Mr. Chair.

Thank you to the witnesses for being with us today.

In my riding of Châteauguay—Lacolle, which will soon be called Châteauguay—Les Jardins-de-Napierville, social media platforms, particularly Facebook and other groups, are very popular. Everyone uses them.

Our study is about misinformation and disinformation. The definition of those two terms can lead to confusion.

Mr. Beaudoin, in your own words, can you tell us what those two terms mean?

C/Supt Denis Beaudoin: Misinformation is false information.

Disinformation is false information that is intentional.

Mrs. Brenda Shanahan: Misinformation is like a misunderstanding, whereas disinformation has an intent behind it. Intent is what sets them apart.

Can misinformation involve ill intent? In other words, someone might think misinformation is unintentional when, in reality, it isn't.

C/Supt Denis Beaudoin: Yes, it's possible.

I have to say that everyone has different definitions of the terms. They aren't in the Criminal Code. Disinformation and misinformation are not criminal offences, per se. The definitions people give the terms can vary as a result.

● (1645)

Mrs. Brenda Shanahan: I'd like us to raise that problem in our report. People aren't well informed. Even those of us in the public sphere struggle when it comes to having a proper understanding of the terms, so malicious actors can trick us.

Mr. Beaudoin, education is very important not only for the public, but also for private companies across all sectors. It's also important for vulnerable communities, including ethnic communities and communities at risk of being targeted by disinformation for malicious purposes.

Can you give us examples of education initiatives the RCMP undertakes?

C/Supt Denis Beaudoin: Let's look at misinformation activities targeting ethnic communities. As I mentioned, any such activities undertaken prior to an election or during the electoral process could be considered criminal.

We've publicized some of our community engagement activities. We try to educate communities and show them that Canadian police services are open and accessible. In other countries, the public can have a negative impression of police or a less favourable view of them.

We try to break the silo culture within communities. We try to educate them on new laws and criminal activity, which they can fall prey to. We also try to educate communities on Bill C-70.

Mrs. Brenda Shanahan: How do you do that? Do you put on workshops? Do you do engage with people in community centres?

In the business community, do you meet with chambers of commerce representatives?

C/Supt Denis Beaudoin: You did a good job of answering the question for me. Everything you said is true.

I can give you some examples. We went to Montreal in May or June to educate communities in the city.

We also give talks to police services across the country to educate them on foreign interference.

Foreign governments sometimes hire private security firms, so we've given many presentations to such firms. We encourage them to be watchful and help them to recognize the signs of interference, including through the use of social media.

We try to target a large audience. Of course, we don't have the resources to do everything we'd like to at the community level. We try to target certain groups to maximize the impact. We give in-person talks in some communities.

Right now, with the RCMP, we're working with Public Safety Canada and other agencies to deliver seven or eight presentations for specific communities in large Canadian cities. We try to go wherever we can to reach as many Canadians as possible.

The Chair: Thank you, Mrs. Shanahan and Mr. Beaudoin.

[*English*]

I have a question related to what Ms. Shanahan asked. You talked about disinformation and misinformation, and we've heard several definitions of those over the course of our study. I'm kind of old school. I remember when it used to be known as lying, to be quite frank. You mentioned the Criminal Code and that there was no distinction between or no identification of disinformation or misinformation in the Criminal Code.

What's the equivalent, in the Criminal Code, that police agencies would use for the spreading of lies, etc.? Would it be considered mischief in the Criminal Code? What would you use to apply that?

C/Supt Denis Beaudoin: I'm not sure misinformation in itself is a criminal offence, Mr. Chair.

The Chair: It could be a disagreement that you have or a difference of opinion; those are the definitions you stated earlier and what we've heard in previous testimony.

● (1650)

C/Supt Denis Beaudoin: Exactly. The biggest difference with Bill C-70 is that if it's a campaign of disinformation with the purpose of affecting government processes, it may become criminal. You won't find these terms under the Security of Information Act; they're not defined in there.

As the member alluded to, it may be something for the committee to see if there's value in defining them, but for police services, we're dealing with harassment, intimidation and threats. For disinformation, if somebody goes through this but at some point he crosses the path and there's a threat, then all of a sudden we investigate the threats, but not necessarily the "lying", as you called it, because oftentimes it may not be a crime.

The Chair: I appreciate all of your being here today and providing us with some valuable information.

There was a request by Mr. Green, so I'm going to make sure that the clerk follows up with parliamentary affairs. Generally, I try to put a timeline on the responses, so if you can, please supply those to the committee a week from today, perhaps at 5 p.m. I understand it's Thanksgiving weekend, but there should be ample time to address Mr. Green's questions.

Thank you, gentlemen, for being here today.

I'm going to suspend for a couple of minutes as we get ready for the next panel.

The meeting is suspended.

● (1650)

_____(Pause)_____

● (1655)

The Chair: Thank you for your patience as we switched over to the second panel.

I'd like to welcome our witnesses for the second hour today.

As an individual, we have Heidi Tworek, professor of history and public policy, University of British Columbia. Welcome, Ms. Tworek.

From CIVIX—which I'm familiar with from some local programs in Barrie, as I'm sure other members of Parliament are—we have Kenneth Boyd, the director of education.

In person from the Russian Canadian Democratic Alliance, we have Maria Kartasheva, the director, and Guillaume Sirois, who is counsel.

We're going to start with you, Professor Tworek. You have up to five minutes to address the committee with an opening statement.

Go ahead, please. Thank you.

Dr. Heidi Tworek (Professor, History and Public Policy, University of British Columbia, As an Individual): Thank you very much, Mr. Chair and the committee, for inviting me to discuss this important topic.

I'm a professor of history and public policy at the University of British Columbia, where I direct the Centre for the Study of Democratic Institutions, or CSDI. At CSDI, we aim to understand the past, analyze the present and train for the future, so I'll make three points today—one about the past, one about the present and one about the future.

First is the past. Misinformation and disinformation are a feature, not a bug, of the international system. So, too, is foreign interference in elections. The U.S. feared French interference all the way back in 1796. In the second half of the 20th century, the two Cold War superpowers, the U.S. and Soviet Union, intervened in around 11% of all national executive elections around the world.

The question is not if foreign interference will happen, but rather why some states engage in this practice at particular moments.

Some of my research examined why Germans tried to use the then-new technology of radio to influence global politics from 1900 to 1945. Germans wanted to interfere in foreign information environments because they felt boxed in politically and economically. Losing World War I accelerated those feelings. This obviously did not end well. The Nazis built on decades of experimentation to spread racist and anti-Semitic content, ending in a world war of words as well as weapons.

Without getting into more historical weeds, this shows that analyzing international relations actually helps to predict potential foreign disinformation campaigns. This phenomenon will not disappear, but will wax and wane, so we need systemic interventions to embed resilience through educational initiatives, platform interventions, transparency, research and other measures to strengthen democracy.

Second is the present. The current social media and AI environment has created new economic incentives for misinformation and disinformation. For understandable reasons, these committee meetings are focused on politics, but making money fuels the problem, too.

We need stronger enforcement of electoral regulations on platforms to guard against this during elections. Canada might also coordinate with other democracies facing the same problem. For example, an intergovernmental task force could coordinate on issues like demonetizing disinformation. This could draw lessons from other multilateral institutions like the Financial Action Task Force, or FATF.

More broadly, Canada has much to learn from other jurisdictions, like Finland on media literacy or Taiwan on transparency and combatting disinformation while preserving freedom of expression.

Third is the future. generative AI or gen AI is obviously at the top of most people's minds. I recently co-authored a report released by CSDI on the role of gen AI in elections around the world in 2024. We found that gen AI is currently pervasive, but not necessarily persuasive, yet it still creates problems. We find that gen AI threatens democratic processes like elections in three main ways.

First, it enables deception by lowering the barrier to entry to create problematic content. This accelerates problems that already existed on social media platforms.

Second, gen AI pollutes the information environment by worsening the quality of available information online.

Third, gen AI intensifies harassment. It's far easier to create deepfakes that may be used to harass female political candidates in particular. We should worry about this amplification of online abuse and harassment of political candidates, which is something that I've studied in Canada since 2019. This could target specific individuals or under-represented groups to force them out of politics.

To date, there is little evidence that beneficial use of gen AI in elections will outweigh these harmful ones. Multiple measures are needed to address the challenges of gen AI. Although not election-specific, for example, the British Columbia Intimate Images Protection Act offers one avenue to protect female political candidates from deepfakes. We should look for similar legislation to address other challenges posed by gen AI.

To sum up, the past tells us that disinformation is not going anywhere, but we do have power to mitigate it. The present tells us to grapple with the economic incentives, too. The future warns us to address issues with gen AI, like deepfakes, before they get out of hand.

Thank you very much.

● (1700)

The Chair: Thank you, Professor. You're under your time. We appreciate that.

Mr. Boyd, we're going to you next for five minutes, sir. Go ahead, please.

Mr. Kenneth Boyd (Director of Education, CIVIX): Good afternoon, members of the committee.

My name is Kenneth Boyd. I'm the director of education at CIVIX, a national non-partisan charity that is dedicated to building the skills and habits of active and informed citizenship. We work primarily with K-to-12 teachers from every province and territory in providing free programs both in English and in French on the themes of democratic engagement, civic discourse and digital media literacy.

Members of the committee may be most familiar with our student vote program, which is our parallel election program for students under the voting age, as well as our rep day program, which invites MPs and other elected officials into classrooms to engage directly with students.

We approach digital media literacy as a necessary component of informed citizenship. Engaging in the democratic process requires that citizens be able to identify reliable and trustworthy sources of information and have the skills to determine the difference between fact and fiction.

We know that the effects of mis- and disinformation online can interfere with engaged citizenship in ways that go beyond being merely misled. For example, in a recent survey that we conducted with 800 teachers from across Canada, we found that 81% of respondents said they believe that mis- and disinformation on social media contribute a “great extent” to the spread of hateful rhetoric in their schools.

Lacking the ability to engage critically with content online thus has downstream consequences in terms of people's ability to have constructive and meaningful conversations about important issues.

To address these problems, we created CTRL-F, our digital media literacy program that teaches empirically supported verification skills that have been proven to increase people's ability to determine the veracity of claims and identify the motives of unfamiliar sources online.

Since 2019, CTRL-F has been used by over 5,200 teachers who have taught the program to more than 300,000 students from all across Canada. We are consistently updating our program to address new kinds of mis- and disinformation online, including those produced by artificial intelligence, and are currently adapting our resources for use by adult learners.

While digital media literacy skills are necessary for everyone, it is especially important that students learn these skills at a young age. There are, however, a number of challenges in teaching effective digital media literacy to Canadians. I will note that while we recognize that education is a provincial issue, it is worth highlighting the issues we have seen in our work in schools and with teachers, as they are indicative of problems that all Canadians face.

First, our research has shown that the resources that are available to Canadian educators vary widely in terms of quality. Provinces can mention educational resources but not mandate their use, and many outdated resources are still used in classrooms and used by Canadians nationwide. In some cases, these resources were developed before the widespread adoption of the Internet, and others have even been shown to backfire, making people less trusting of credible sources.

Digital media literacy is also not a singular thing. It is an umbrella term that encapsulates many different concepts and competencies. However, educators and Canadians in general are given little guidance about which resources are available to them and which are of high quality and grounded in evidence.

Second, there is an overall dearth of digital media literacy training. For example, it is a common occurrence to find educators in charge of digital media literacy instruction who have no specific training in the subject matter or who received their last training when studying to become a teacher. Even for those who choose to inform themselves about the latest developments in digital media literacy, the online world moves and changes so quickly that it is difficult to keep up.

In response to these issues, we believe there needs to be a national strategy to facilitate digital media literacy training. Through our work, we have found that in terms of scalability it is most efficient to train educators, as well as civil society organizations and community leaders, to reach as many Canadians as possible.

We also encourage the committee to consider approaching the problems of mis- and disinformation as being a widespread skills issue rather than simply an awareness issue. Merely making people aware of the need to critically engage with content they find online will not help us make any progress. Canadians need access to and training in digital media literacy skills, and that requires a sustained investment from the federal government to ensure high-quality resources are available and programs can continue to operate effectively.

Finally, informed citizenship requires access to high-quality information. In our resources, we say that the online information environment is polluted. Trustworthy information can certainly be found, but mis- and disinformation are mixed in. Disinformation also tends to be free and easily accessible. Indeed, it is in the interest of the purveyors of such information for it to be as easily accessed as possible, so there is a real need to take steps to limit the degree of information pollution online. One way to address this problem is to support journalists, especially local journalists, who are able to provide reliable information and give Canadians better options to find important information online.

I'm happy to address any questions the committee has, and I thank you for your time.

● (1705)

The Chair: Thank you, Mr. Boyd.

We're now going to the Russian Canadian Democratic Alliance.

You have up to five minutes to address the committee. Go ahead, please. You're good to go.

Ms. Maria Kartasheva (Director, Russian Canadian Democratic Alliance): Honourable members of the committee, I am Maria Kartasheva, director of the Russian Canadian Democratic Alliance. I am accompanied by our counsel, Guillaume Sirois.

Thank you for your invitation and for addressing the national security threat posed by Russian propaganda and cognitive warfare.

The RCDA is a volunteer-led, non-profit organization created in the wake of Russia's criminal full-scale invasion of Ukraine. Our mission is to support the development of the Russian-Canadian community around the ideals of democracy, human rights and the rule of law. Opposing the invasion of Ukraine and Putin's regime is central to our work.

I want to begin by expressing my gratitude for your recognition of the serious threat that Russian information and influence operations pose to our democracy and society. Cognitive warfare aims to manipulate information and perceptions to influence thinking, to destabilize societies and to achieve strategic objectives without direct military confrontation. Russia employs these tactics as part of a broader strategy, viewing itself at war with the west, including Canada. Understanding this context is crucial for developing effective responses to safeguard our democracy.

I myself was a direct victim of this cognitive warfare. Russia sentenced me to seven years in prison for disseminating truthful information about the Bucha massacre while in Ottawa. I even faced the threat of deportation from Canada because of my political activism.

The RCDA, an organization that I co-founded, has been labelled an “undesirable” organization by the Putin regime. This designation puts all our partners and our collaborators, including me, at significant risk. One of our directors felt compelled to resign due to fears of persecution. This situation underscores the urgent need for decisive action to protect not only our democratic institutions but also the individuals who actively work to uphold them.

Meanwhile, despite Russia's long-standing disinformation campaigns in Canada, I have yet to see any individuals held accountable or facing consequences for their actions. Aside from public statements and ineffective sanctions, it appears that Canada is doing little to prevent Russia from gaining the upper hand in its cognitive war against Canadians.

As we have learned, notably in the course of the foreign interference commission, there are four key ways that Russian propaganda is impacting the work of parliamentarians.

First, Russian disinformation is shaping how Canadians, and by extension, members of Parliament, think about, and vote on, pivotal issues, including the support for Ukraine, NATO and even domestic issues, such as inflation.

Second, disinformation fuels fear and hostility, contributing to threats and violence against MPs, undermining their ability to perform their duties safely.

Third, the saturation of disinformation contributes to growing political apathy among the general population, weakening democratic participation.

Fourth, these disinformation campaigns aim to destabilize the very foundations of our democracy by spreading doubts about the integrity of elections, and of our democratic processes.

In response, the Government of Canada must do the five following things:

First, annually assess the scope of Russian and other state-sponsored disinformation targeting Canada, and report the findings to Parliament for transparency and accountability.

Second, adopt a strategy to combat Russian propaganda, focusing on protecting the work of members of Parliament and the Russian diaspora from such disinformation campaigns.

Third, establish an independent body similar to the CRTC or Elections Canada to monitor, to assess and to respond to foreign propaganda, ensuring the integrity of democratic processes is upheld.

Fourth, engage with the Russian diaspora and civil society organizations to help identify and combat Russian propaganda.

Fifth, enforce a decisive foreign policy that curbs Russia's disinformation, with diplomacy and global partnerships ensuring accountability for Russia's actions in Canada.

In conclusion, Russian interference in Canada's democratic processes, as exemplified by the ongoing disinformation campaigns, represents a significant threat that must not be ignored. For decades, Russia has been conducting destructive operations, such as the Tenet Media operation, with relative impunity. By recognizing the gravity of this threat and by committing to serious action, we can protect our democracy for future generations.

Thank you for your attention. I am happy to answer all of your questions.

● (1710)

The Chair: Thank you.

Thank you to all of our witnesses for very interesting opening statements.

We're going to go to six-minute rounds for each party, and we're going to start with Mr. Barrett.

Go ahead, Mr. Barrett, for six minutes.

Mr. Michael Barrett: Mr. Boyd, I've had the opportunity to engage with your organization on rep days, and I'm aware of how I fared in the local student vote. I'm as pleased with that result as I am with the general election and by-election results that I've had. I'll give a shout-out to St. John Bosco in Brockville and St. Edward in Westport, which invited me to take part in rep days there. I think it's a great program. There are always great questions that demonstrate the understanding these students have as a result of the efforts of your program. That's certainly commendable.

You talked about education being a provincial responsibility. I wonder if you could quickly tell us about your funding. How much federal funding have you received, and how much provincial funding does your organization receive?

● (1715)

Mr. Kenneth Boyd: I can't tell you the exact percentages off the top of my head. We are a registered charity, so all of our funding information is of course on the public record. I would say that for our digital media literacy programs especially, we receive a combination of funding from the federal government, the digital citizen initiative, private organizations and donors, research centres and provincial governments.

As for this program, I would say that we've mostly received funding from Canadian Heritage and the digital citizen initiative.

Mr. Michael Barrett: I believe you've expanded your offerings overseas to Colombia and Chile. How are those initiatives funded?

Mr. Kenneth Boyd: Those initiatives are funded through independent grants that have been applied for by our teams in Colombia and Chile. They received a grant recently from the EU to continue funding their projects. They have taken the work we've done in Canada, especially on digital media literacy programs, and adapted it for an audience in both Colombia and Chile.

Mr. Michael Barrett: You're teaching children how to navigate, I think you described it as, digital pollution. There's definitely lots of pollution online. Thinking critically and being able to discern what's real and what's not become more and more challenging all the time.

What is one tangible recommendation you could make for us to include in this report? What do you think could improve digital media literacy of children across Canada?

Mr. Kenneth Boyd: I think there needs to be an investigation into the kinds of resources that are effective, based in evidence and can be made.... As I mentioned before, we understand that education is more of a provincial responsibility. However, in terms of being able to make a recommendation, some tools have been shown to be effective. Understand what those are and make them known, not just to students but also to Canadians more widely.

There are effective digital media literacy strategies out there that can be learned. I think that would be something concrete the committee could pursue.

Mr. Michael Barrett: Give me an understanding of the uniformity of material being delivered across Canada in the space of civic literacy and digital media literacy. Is there any standard across provinces and territories? If so, what is it? If not, is there even consistency within each province on the material being delivered across school boards?

Mr. Kenneth Boyd: With regard to the different provinces, it's common to find, in curricula, requirements that digital media literacy or source evaluation be taught in some capacity. Provinces are able to make recommendations or list possible resources, but they do not mandate the use of any particular resource. That is to say, you might find different digital media literacy education happening across provinces and territories.

There is no unified, consistent mandate to use some resources and not others.

Mr. Michael Barrett: What do you think is the most important way that your organization will protect its credibility going forward? What steps are in place, whether it's for board selection or for screening funding sources, to ensure that, as an organization that's charged itself with these important educational initiatives, you are ensuring that you remain credible and unimpeachable in a very murky landscape of information providers?

Mr. Kenneth Boyd: I'm sorry; could you rephrase the question in terms of credibility? I missed the first part of that question.

The Chair: You have 10 seconds left.

Mr. Michael Barrett: Really, I was just looking at what you're doing to protect your credibility, whether it's with the selection of individuals to your board or screening funding sources, based on the murky information landscape that's out there. How are you protecting your credibility as a source for teaching people?

● (1720)

The Chair: I'm going to need a really quick response, Mr. Boyd.

Mr. Kenneth Boyd: Very quickly, as I mentioned, we are a charity, so we are very transparent about all of our funding sources. That is, I think, one way that we maintain credibility.

The Chair: Thank you.

[*Translation*]

Mrs. Shanahan, you have six minutes. Go ahead.

[*English*]

Mrs. Brenda Shanahan: Thank you very much, Chair.

I'd like to thank all of the witnesses for being here, but I want to particularly turn my attention to a story that came out in the last month, which I'm sure the witnesses are familiar with. It is the story about Tenet Media. There is a connection to my home province of Quebec in that there were two people in our West Island locality, Lauren Chen and someone else, who were named in a U.S. indictment. They are alleged to have been spreading misinformation. It could have been that they were, as I think the technical term goes, "useful idiots", but it could be that they were very knowingly doing what they were doing. I don't know, but let's talk about what was going on there.

According to the U.S. indictment:

> After Russia invaded Ukraine in February 2022, RT was sanctioned, dropped by distributors, and ultimately forced to cease formal operations in the United States, Canada, the United Kingdom, and the European Union.

That's a very big market right there.

The indictment continued:

> In response, RT created, in the words of its editor-in-chief, an "entire empire of covert projects" designed to shape public opinion in "Western audiences."

The indictment goes on to allege that Tenet Media is one of RT's covert projects.

How does the RT empire of covert projects hurt Ukrainian Canadians? I'm asking that of Madam Kartasheva.

Ms. Maria Kartasheva: I feel that asking that question of Ukrainian Canadians would be better, as I am a representative of Russian society in Canada, but I feel that Russian propaganda in general is hurting everyone. Specifically, if we're talking about Ukrainians in Canada, I was talking with one of the directors of the UCC, who was telling me that, after the war and because of Russian propaganda, they've seen a horrendous increase in hate crimes against Ukrainians, whether it will be insults or just some symbols outside universities or just on the street.

We know that there are a lot more Ukrainians now in Canada, because when the war started, Canada opened its doors to them. I imagine that, for them, it's got to be very traumatizing to come from the war and see these hateful symbols around them. In my understanding, Canada doesn't do enough to protect them or even react to these crimes.

Mrs. Brenda Shanahan: Thank you very much for that answer and, in fact, for enlarging the question.

I want to point out that my riding of Châteauguay—Lacolle, which will soon be named Châteauguay—Les Jardins-de-Napierville has a wonderful agricultural region. We go right out to the American border.

We have a large number of Russian speakers of mixed Russian-Ukrainian heritage. We were very proud, even the small city of Châteauguay of 50,000 people, to be able to receive over 100 Ukrainian families who were displaced after Russia's invasion of Ukraine. It was all hands on deck and a wonderful community project. Indeed, the group has since been disbanded insofar as the Ukrainians have completely integrated, are working and are looking after themselves and their families, although the friendships are forever. It has very much sensitized our community to this disinformation, misinformation and how harmful it can be. How can we best fight back?

Ms. Maria Kartasheva: Well, it's a very important question, and I guess that's why we are all gathered here. There has to be some kind of independent body that will investigate these kinds of disinformation and provide recommendations on how to react to that or maybe even, sometimes, enforcing some solutions to that. Obviously, it is a very complex issue, and the problem concerns not just, for example, media like Russia Today. The strategy of Russian propaganda is very complex: It includes social media; different “experts” who do interviews on different media, including normal and respected media; and different professors. It is a very complex issue that has to be treated on all of these levels, and that's why I was proposing this independent body that will coordinate this activity, because if everyone is solving the issues, no one is solving the issues. There has to be one body that's monitoring all that.

● (1725)

Mrs. Brenda Shanahan: Thank you for that.

Thank you for the work that you're doing in sensitizing Canadians that, indeed, there are Russians here in Canada who are actively fighting for democracy, even at their own risk. I appreciate the work you are doing. Do you know of any other RT projects that are seeking to influence western audiences?

Ms. Maria Kartasheva: I am not familiar with the RT on that level because, personally, it just pains my brain to watch what they show and whatever they're doing. However, I know their strategies are very complex and, as I said, they do it on multiple levels. I'm familiar with it because they do, honestly, pretty similar things in Russia as well, with the goal of spreading disinformation and doubt amongst people so as to not trust each other, the government or anyone, and so—

The Chair: Thank you. It's okay, Maria. It's fine.

I'm sorry, but we're almost 45 seconds over there.

[*Translation*]

Mr. Trudel, you may go ahead for six minutes.

Mr. Denis Trudel: Thank you, Mr. Chair.

Ms. Tworek, disinformation, AI, social media, and how to counter disinformation and misinformation give rise to very serious issues.

This year, a think tank within Employment and Social Development Canada released a report listing the top 35 global disruptions we currently face. Disinformation is the biggest one facing the world today, according to the report.

Do you agree with that, Ms. Tworek?

[*English*]

Dr. Heidi Tworek: What I would say is that it underlies so many other threats. Whether those are questions around war, climate change, etc., we see that disinformation is a part of all of those problems, so that's how I tend to think about it. What we also see is that abuse and harassment are a key part of disinformation. We never know quite who it's going to strike, depending on the issue. I see it as an underlying foundation, and that's why I think it's such an existential threat.

[*Translation*]

Mr. Denis Trudel: When you think about it, AI is somewhat terrifying. It can duplicate my face and voice, and make me say just about anything on social media. That's pretty awful.

How do we deal with that phenomenon? What can we do legislatively to prevent problematic situations during the next election campaign? Say there's a video in which I'm supposedly singing the praises of the Conservative Party of Canada's agenda and it's going around social media.

[*English*]

Dr. Heidi Tworek: What we say in our report is that this is obviously something that has to be taken on in multiple dimensions. There are the companies that are themselves thinking about things like watermarking to see whether something is AI-generated or not, so ensuring something like that is implemented.... We need the kinds of programs like civics, not just for schools but also for those who are not of school age, and we also need to think about different kinds of regulations. We have a whole host of recommendations within that report, and I'm happy to share the report with the committee so that you can delve into those. However, I think that the clear bottom line is there's no one responsible party here. We need a range of different measures to deal with this.

● (1730)

[*Translation*]

Mr. Denis Trudel: You said in your opening statement that AI had been used during election campaigns in other countries.

What happened exactly, and how did they detect that the content was AI-generated, not genuine political content?

[*English*]

Dr. Heidi Tworek: In some cases, for example, in Slovakia, there was a deepfake audio. The person themself obviously said that it was a deepfake. We've seen some in India as well.

It's always very difficult to identify if this changes someone's mind or not, but we have these kinds of singular examples that we point out in the report from countries all around the world to show this kind of generative AI is at least being used.

For now, we don't find a lot of evidence that it's persuasive. That's why I say we need to get ahead of the problem before it becomes something that we can't really get a grip on.

[*Translation*]

Mr. Denis Trudel: In the countries you've studied, did the attack or threat come from a foreign country or from other political parties domestically?

[*English*]

Dr. Heidi Tworek: That was, unfortunately, something that we couldn't identify. We didn't engage in those kinds of investigations.

Sometimes it can indeed be very difficult. The example of Tenet Media shows us that, in that case, it actually wasn't about who was creating the content; it was about the financing behind it. That's why I made the recommendations about thinking about financing as well as looking at the content itself, because you can have, in a way, things that happen off of the platforms that are actually influencing what kind of content is being created.

We need to combine not just thinking about the content but also thinking about the actors and their behaviour.

[*Translation*]

Mr. Denis Trudel: Do you think certain political parties in Canada are currently spreading disinformation for partisan purposes?

[*English*]

Dr. Heidi Tworek: That's a very difficult question to answer.

As far as we know, political parties are obviously going to be pushing for themselves to win, but we haven't looked into specifically assessing what political parties are doing internally. That's obviously something that's very difficult for us to get at.

[*Translation*]

Mr. Denis Trudel: Thank you.

Mr. Boyd, I have the same question for you.

Do you think there are political parties in Canada that have spread disinformation in the past for partisan purposes, that are doing so now or that plan to do so in the future?

[*English*]

Mr. Kenneth Boyd: I'll give the same answer Professor Tworek gave, which is that it is very difficult to determine if political parties themselves are internally creating this kind of information. I certainly have no sense of what the intentions would be going forward, so I don't have a good answer for you. I'm sorry.

[*Translation*]

Mr. Denis Trudel: All right. Thank you.

The Chair: Thank you, Mr. Trudel.

[*English*]

Mr. Green, go ahead for six minutes, sir.

Mr. Matthew Green: My questions in this round are going to be for Ms. Tworek.

In a 2023 conference briefing note entitled “Media/Digital Literacy in an Era of Disinformation”, you reflected on a presentation you had made in 2022; it was published in the Journal of Intelligence, Conflict, and Warfare.

During this presentation, you talked about the fact that misinformation and disinformation often overlap with online abuse—in fact, you referenced it in the previous round of questions—that is directed towards professional groups, and marginalized groups like, for example, women, as I think you referenced. You said it's the foundation.

Why do you think that is?

Dr. Heidi Tworek: Part of what we've seen in studies that we conducted since 2019 is that often these kinds of identity-based attacks and that kind of harassment can have disproportionate effects on people from racialized communities, 2SLGBTQ+ people or women. This can often overlap with some sort of disinformation about those individuals.

The distinction here is that, of course, you can have vigorous and rigorous discussion about issues, but we often see with these groups that is melded with attacks on their identities.

This has an influence on the political candidates themselves and also, I'd like to add, on their campaign teams. That's really important, because those are often people who are thinking about going into politics and potentially becoming candidates. They see the kind of online abuse and harassment directed at a candidate, and they think, “Maybe politics is not for me.”

If we're thinking about having a diverse legislature that represents the diversity of Canadians, we do need to address this issue.

● (1735)

Mr. Matthew Green: It's interesting that you raise that. I know, for instance, that this point was raised by one of our previous committee members, Ms. Pam Damoff, who talked at length about the way in which political violence expresses itself.

From your perspective, at what point do these campaigns cease being merely misinformation and disinformation and cross over into the rubric of political violence or, dare I say, a proto-fascist approach to dismantling democracy in the country?

Dr. Heidi Tworek: That's obviously a big question that political theorists can debate. I think I'd take it in a slightly different direction, which is to say that these are often actual threats against people's physical or psychological safety. There are all sorts of ways that we need to think about addressing this.

A report I co-wrote with Chris Tenove in 2020 gives a whole host of recommendations for how we can try to address these kinds of things so that we can continue to have a democracy and, hopefully, build on a democracy that has a diverse group of political candidates and representatives. I'd be happy to submit that report to the committee.

Mr. Matthew Green: That would be good, because my next question is how we look to minimize that type of online abuse.

The two challenges you highlighted during that 2022 presentation were the lack of explanatory journalism and the lack of social media expertise for some professional communicators trying to publish high-quality information online. Can you explain these two challenges and whether there are initiatives in Canada to meet them?

Dr. Heidi Tworek: In terms of the lack of explanatory journalism, another way of thinking about this is that we need to think about what journalism looks like in the 21st century, who can supply that information and so on. There are obviously a whole host of initiatives.

I'll just highlight one, which is The Conversation Canada, which was co-founded by a couple of my colleagues at UBC. The idea of that is pairing academics who are very bad at writing op-eds mostly with journalists who are able to edit. What we get there is academic expertise, but packaged in ways that most people can understand it. This can be freely reprinted. That's just one example of how we can amplify journalism and have it coming from experts.

In terms of social media expertise, this is quite a problematic area now because we see that social media platforms, even since 2022, have increasingly been shutting down the ability for researchers to access any data from platforms, whether it's CrowdTangle from Meta or X, which is now prohibitively expensive. It's made it harder and harder for us, as researchers, to be able to access the sort of data we need to answer a lot of the fundamental questions that this committee is proposing. That's why bills like Bill C-63 embed ideas around transparency for researchers within them.

Mr. Matthew Green: That's algorithmic transparency to understand how people are fed information. Is that what you're referring to?

Dr. Heidi Tworek: Part of it is algorithmic transparency. Some of it is also questions around getting access to posts at all, because we're not able to access large numbers of posts from many social media platforms. There were a lot of questions, for example, about X—then Twitter—that we could ask in our study on political candidates in 2019 but I can no longer ask because I simply don't have access to that level of data.

Mr. Matthew Green: What I'm getting here is the commodification of information. I know that machine learning and AI are able to go on and check the mood of the people on the platform in significant ways. Of course, this was referenced in the 2016 election under Trump in the way in which Cambridge Analytica and others targeted people.

From your perspective, what ways can we decommodify this kind of information capitalism to make it more democratic and transparent, as you suggested?

Dr. Heidi Tworek: It's a great question. I don't think there are any silver bullets, but researchers suggest a variety of ways.

Some are looking at antitrust. There's obviously a lot of that happening in the U.S. Others are suggesting things around data privacy so that companies simply don't have access to so much information. Others are talking about whether we need public AI. That's Mozilla's suggestion, for example.

I don't think there's one silver bullet, but there are a whole host of different potential options that we could explore.

Mr. Matthew Green: Okay. Thank you very much.

The Chair: Thank you, Mr. Green.

That concludes our first round.

We have enough time for five minutes for the Conservatives and five minutes for the Liberals.

[*Translation*]

Mr. Trudel will have two and a half minutes.

[*English*]

We'll have two and a half minutes for you, Mr. Green, and that will take us up to the allotted time.

I am going now to Mr. Caputo for five minutes.

Go ahead, sir.

Mr. Frank Caputo: Thank you, Mr. Chair.

I'd like to thank the witnesses who are here in person, and Mr. Boyd and Professor Tworek who are on video conference.

I note, professor, that you are from UBC. As an SFU grad, I have to put in a friendly jab about the superiority of SFU.

● (1740)

The Chair: That's a "point of order", Mr. Caputo?

An hon. member: Oh, oh!

Mr. Frank Caputo: In all seriousness, one of the things that has really bothered me about foreign interference, especially surrounding elections, is the amount of time it takes for the government to act. In other words, the people on the ground know exactly what's happening, yet there is a significant lag time between that information getting to security forces in Canada and action being taken.

Would either of you, Mr. Boyd or Professor Tworek, have any input on that?

Dr. Heidi Tworek: I'll just say briefly that one of the things I advocated for is thinking about transparency and how that can happen appropriately.

The Chair: Mr. Boyd, do you have any response to that?

Mr. Kenneth Boyd: As you mentioned, there is potentially, or inevitably, going to be some lag time in these kinds of cases, but I think that points to the need to approach these problems from multiple angles. In terms of Canadian citizens having the ability to help identify when information is false or misleading, that would be something that can help fill the gap before there is action taken by any sort of federal agency.

Mr. Frank Caputo: Let's build on that.

I'm sorry. Mr. Sirois has something to add here.

Thank you.

Mr. Guillaume Sirois (Counsel, Russian Canadian Democratic Alliance): Russian propaganda, especially, has been an issue for a very long time, for at least a decade or maybe more. We've learned through the Foreign Interference Commission today that the strategy to address this foreign interference is at a nascent stage. This is a very long delay to address a national security issue like foreign interference. We've seen the consequences of that with the Tenet Media operation. Had we had a strategy sooner—for instance, after the 2016 interference during the presidential election—maybe we wouldn't be here today talking again about foreign interference.

Mr. Frank Caputo: I certainly agree with you, Mr. Sirois. If I have to be candid—which I believe I should be in these committees and in Parliament generally—I have seen a lack of political will to address this head on. Frankly, that falls at the feet of the government. I've said this at just about every committee meeting we've had. We have 11 people who have wittingly or semi-wittingly, according to our security forces, worked with hostile foreign states.

You talk about confronting this and confronting it early. I believe the term you used was “a nascent stage”. This is information that we know that our security forces know, but that we, as Canadians, don't know. We've asked so many times of our security apparatuses, yet it feels like we get no further information.

Is that just not completely the opposite of the approach we should be taking of shining the light, shining it brightly and shining it early?

Mr. Guillaume Sirois: I think we both agree that transparency is the key to answering to foreign propaganda, such as the Russian interference we're discussing today. Transparency allows for the beginning of the conversation on how we can address this issue. If we don't know what the government is doing behind closed doors, we cannot have a proper discussion about what it should be doing or about what the government is doing wrong.

Mr. Frank Caputo: Ms. Kartasheva, you mentioned something at the beginning that caught my ears, that you were sentenced to seven years in jail in Russia in absentia.

Do you want to talk about that? This is your time if you want to discuss that, any of the impacts of that and what other people in your position go through. Feel free. The floor is yours.

Ms. Maria Kartasheva: The worst part for me was that I didn't receive support from Canada in time. I received it later, after I managed to get media attention. For months, I was struggling to get any attention, even from my MP. She apologized later because apparently there was some mistake on her assistant's part. For months, I felt completely abandoned by Canada, and I'm very worried that this might happen to someone else.

In short, what happened is that I had my citizenship application being processed at the time when I was sentenced in Russia. First, I was obviously arrested; then I was sentenced. I informed IRCC about this, which IRCC basically ignored, and my first citizenship ceremony was cancelled. Then I received a letter half a year later saying that I might not become a citizen because I'm a criminal in Russia.

● (1745)

Mr. Frank Caputo: Just so that's it's clear to me: You got something from IRCC saying—

Ms. Maria Kartasheva: It was half a year later. I wrote to them several times, asking if there was any progress. They said that they were reviewing my case and that everything was fine. Then they sent me a letter saying that I had a month to send them all the documents that I might want to provide. They sent the letter to me at the beginning of December, just so you understand. It was months, and it was the holidays. No one was responding to my requests to send me any documents. It was a not a great time. Oh, oh!

The Chair: Okay. The worst part of my job is having to cut off somebody who's telling their story.

Mr. Frank Caputo: I'm sorry.

Perhaps one of my Liberal colleagues will allow you to continue, because I think this is worthy of hearing.

The Chair: Let's see if Mr. Bains will take you up on that offer.

Mr. Bains, you have five minutes. Go ahead, please.

Mr. Parm Bains: Yes, I will, if you want to continue.

Ms. Maria Kartasheva: Basically, my biggest issue and the fear of my colleagues in the organization and a lot of Russian citizens in Canada is that they will have problems in Canada when their citizenship or other immigration documents are processed, and that if they were persecuted in Russia, it will affect their stay in Canada. The biggest fear I had was that I would be deported. I had to live with that fear every day for a month, because I didn't know how this would end.

Again, no one apologized to me. I don't know why this happened. Maybe there is someone in IRCC who was interested in stopping me from becoming a Canadian citizen. Maybe there was someone there who wanted to get me back to Russia to end up in prison. I don't know. There was no investigation, to my knowledge, and I don't know if there would be any investigation.

I created a petition to prevent these cases from happening, by making a list of foreign laws that would not be preventing people from becoming citizens or getting visas, and IRCC responded that their system is perfectly fine and is working in the interests of people like me. You might be the judges of that, because I don't agree. I feel gaslighted by IRCC and, I guess, by the Minister of Immigration, and I'm not happy with that.

Mr. Parm Bains: Thank you for sharing. I apologize on behalf of the government. I wish there were some resolution that we could find. Some recommendations that you've made right now are on record, and they will be looked at and reviewed for sure, and maybe we can look at your case further.

I'll continue with you and Mr. Sirois, please.

Could you share with us what are the most common platforms or channels through which you believe Russian disinformation is being spread in Canada now? I know there's a long history of it. Quite frankly, we've heard from several experts in this matter that Russia was like the originator of this kind of almost like modern-day warfare, an information warfare.

Could you tell us what you know or what you monitor today with respect to which platforms or channels are being used right now?

Ms. Maria Kartasheva: It depends on what kind of public they're targeting.

For younger people, that would be Telegram. For older people, maybe, or people who are not very confident with Telegram, there's Facebook. You can see so many bots on Facebook spreading Russian propaganda, and you can tell that those are not real people because they don't post anything else.

There are also Canadian Canadians, right, or immigrants in Canada from other countries. That would be other different media or also experts and professors in universities in Canada who spread Russian propaganda and visit Russia on obviously Kremlin-sponsored trips and then tell how great everything is in Russia and on occupied territories. Then they tour Canada and spread this information among Canadians.

There are definitely several strategies they use for different groups of people, but I can tell that those are working.

Mr. Parm Bains: Primarily it's bots that are being used.

Ms. Maria Kartasheva: I think this is one—

Mr. Parm Bains: Is that the primary operational tool?

● (1750)

Ms. Maria Kartasheva: It's one of the tools they use, but certainly it's not the only one.

Mr. Parm Bains: Okay.

I'd like to go to Mr. Boyd quickly, if I have some time here.

Just today, there were reports of TikTok being sued by more than a dozen attorneys general in the United States who are alleging the following:

> ...the social media platform is misleading the public about its safety. The app, they say, is harming children's mental health, with some kids getting injured or even dying because of TikTok's viral “challenges”.

Do you have the capacity to monitor trends on TikTok or other platforms? I know that other youth-based platforms that are used could impact young people.

Mr. Kenneth Boyd: We do keep a general track of what kinds of platforms are being most used by young people. We conduct surveys with teachers and students from across the country to learn about their digital media habits.

Certainly, TikTok is still one of the major platforms that is being used by young people. That is something that we are aware of. A lot of times when we use examples of the kinds of misinformation and disinformation that young people might come across, we use examples from TikTok and give students the ability to try to verify and see what's actually true and what's not in the platform.

The Chair: Thank you, Mr. Boyd.

Thank you, Mr. Bains. I appreciate that you allowed your time to be used for Ms. Kartasheva to conclude the story.

[*Translation*]

Mr. Trudel, you have two and a half minutes. Go ahead.

Mr. Denis Trudel: Thank you, Mr. Chair.

Your story is very moving, Ms. Kartasheva. It's actually quite troubling. I hope the government will follow up to get to the bottom of what happened, because it's outrageous.

You said in your remarks that analysts working for Russia were asked to comment in traditional media venues.

Can you give us names?

[*English*]

Ms. Maria Kartasheva: I'm sorry. Can you repeat the question?

[*Translation*]

Mr. Denis Trudel: You said in your remarks that analysts working for Russia had been asked to comment in traditional media venues, not just on social media platforms. You said that was one of the methods Russia used to engage in foreign interference, including in Canada. These are experts who are asked to talk about certain situations, like the war in Ukraine, and they're paid to spread the propaganda of the Russian government.

Can you give us their names?

Mr. Guillaume Sirois: It's tough to give specific names without risking defamation. All we can do is talk about allegations and things we've heard, without providing a clear answer as would be the case in a court of law, say.

That said, there are definitely people spreading the Kremlin's messaging. Some have collaborated on articles posted on Russia Today, including a professor who was asked to testify as part of the public inquiry on foreign interference. He said we should pull back on aid for Ukraine and was spreading the Kremlin's narrative. His name is Paul Robinson. It's a matter of public record.

Those kinds of comments can be very dangerous when it comes to the Russian diaspora.

Mr. Denis Trudel: Understandably, Russia is interested in countries such as the United States, China, Germany and France, but let's be clear, Canada isn't a major world power.

What is Russia trying to achieve here? Generally speaking, what is its strategy?

Mr. Guillaume Sirois: I can answer that question.

[*English*]

Maria can add something, if she feels the need to.

[*Translation*]

Canada is an important ally in many international alliances. Just think of NATO or the Five Eyes, an intelligence alliance that brings together five countries. Obviously, Canada is a very close partner of the United States.

It's not hard to imagine that hostile foreign actors—not just Russia, but also China and Iran—would want to gain access through the back door, so to speak, in order to undermine organizations like those that play an important role in international security.

The Chair: Thank you, Mr. Trudel and Mr. Sirois.

[*English*]

Mr. Green, go ahead for two and a half minutes.

Mr. Matthew Green: Thank you very much.

For my question, I'll go back to Dr. Tworek.

In the book you published in 2019, *News from Germany: The Competition to Control World Communications*, you uncovered how the Germans fought to regulate information at home and used new technology to magnify their powers abroad, showing that information warfare has existed for a long time. You referenced that in your opening statements. I recall the documentary on Edward Bernays called *The Century of the Self*, in terms of propaganda. This is an age-old political tool.

What lessons can we learn from history and draw on to find solutions to the current problems of disinformation and misinformation we face today?

● (1755)

Dr. Heidi Tworek: Thank you very much.

I think there is a whole host.

The first, as I said, is about looking broadly at international relations to try to predict which countries are going to engage in this. This is probably much cheaper than some other modes of foreign interference. We need to be on the lookout for that, using our international-relations hat.

The second is about being on the lookout for how new technologies get used. There are stories of the Germans seizing on a new technology, whereas others, like the British, were relying on older technologies and didn't see it coming to a certain extent. We need to be forward-thinking in that regard.

The third lesson is that there's a lot we can do. We're not powerless in this regard. We have faced similar situations before with new technology, so we shouldn't just throw up our hands and say, “The Internet and generative AI are unprecedented, so there's nothing we can do.” There's actually a lot that has precedent. We can look at examples of how we've tried to deal with this before, in order to see what's worked and what hasn't.

Mr. Matthew Green: You mentioned that we need to be predicting which companies will use.... I'm sorry. It's “countries.” I slipped up. I said, “companies” because there are also a host of non-state actors.

Can you speak about ways non-state actors also use these tools online? I talked about the commodification of information, and you spoke a bit about data sovereignty. Could you speak more about that? Also, can you talk about how ubiquitous this is?

Really, I think it's safe to say that all countries are, in some way or another, accessing this type of disinformation tool.

The Chair: We have very limited time for the answer.

Go ahead, please.

Dr. Heidi Tworek: There are obviously a very small number of companies, so we need to pay attention to how they're making money—mainly through advertising—and think about how we might regulate that and what public options could look like, which is what we did in the past with radio and television.

Mr. Matthew Green: Thank you.

The Chair: Thank you, Mr. Green.

That concludes our panel for today. I want to thank everyone for appearing.

Professor, I understood you to say that you were going to supply the committee with a copy of a study you had done. Could you do that? I'll make sure the clerk follows up with you.

I want to thank the Alliance for being here. I understand that you've been very busy appearing before parliamentary committees over the last little while. Thank you for again for taking the time to come before our committee.

Mr. Boyd, thank you as well.

Before we go, I'm just about to publish Thursday's agenda.

Mr Bains, your witness will be here on Thursday. I apologize because the way it was formatted, we actually didn't see the name on the Excel spreadsheet, but it was there after we went back. I know you brought that up in the last meeting. He will be here on Thursday.

The other thing I have to mention to the committee as well is that the social media companies have agreed to come after the Thanksgiving break, which means that we would have to extend this study for another two meetings. Given the level of interest and, quite frankly, given the important information the committee has been provided by our witnesses, I'm going to propose that we extend this by another two meetings so that we have the social media companies. They include TikTok, Google and Meta. They're all coming the week after Thanksgiving.

Do do I have agreement among committee members?

[*Translation*]

Are you fine with that, Mr. Trudel?

Mr. Denis Trudel: Yes.

The Chair: All right.

[*English*]

We're going to do that. We'll see everybody on Thursday. Thank you for all of your contributions.

To our witnesses, thank you on behalf of Canadians for being here today and providing us with some valuable information.

The meeting is adjourned.