EVIDENCE

OTTAWA, Monday, April 15, 2024

The Standing Senate Committee on National Security, Defence and Veterans Affairs met with videoconference this day at 4 p.m. [ET] to examine and report on issues relating to national security and defence generally.

Senator Tony Dean (*Chair*) in the chair.

[*English*]

The Chair: Welcome to this meeting of the Standing Senate Committee on National Security, Defence and Veterans Affairs. I'm Tony Dean, senator from Ontario, the chair of the committee. I'm joined today by my fellow committee members, whom I will ask to introduce themselves, beginning with our deputy chair.

[*Translation*]

Senator Dagenais: Jean-Guy Dagenais, Quebec.

[*English*]

Senator Oh: Victor Oh, Ontario.

Senator White: Judy White, Newfoundland and Labrador, replacing Senator Anderson for today.

Senator M. Deacon: Welcome. Marty Deacon, Ontario.

Senator Cardozo: Andrew Cardozo from Ontario.

Senator McNair: Hello. John McNair from New Brunswick, replacing Senator Kutcher today.

Senator Yussuff: Hassan Yussuff, Ontario.

Senator Dasko: Donna Dasko from Ontario.

The Chair: Thank you, colleagues.

On my left is the committee's clerk, Ms. Ericka Dupont, and to my right are the Library of Parliament analysts Anne-Marie Therrien-Tremblay and Ariel Shapiro, who support us so well.

Today, we welcome three panels of experts who have been invited to provide a briefing to the committee on disinformation and cyber operations in the context of Russian's war against Ukraine. We're continuing our focus on Ukraine, but specifically now on cyber operations.

TÉMOIGNAGES

OTTAWA, le lundi 15 avril 2024

Le Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants se réunit aujourd'hui, à 16 heures (HE), avec vidéoconférence, pour examiner, pour en faire rapport, les questions concernant la sécurité nationale et la défense en général.

Le sénateur Tony Dean (*président*) occupe le fauteuil.

[*Traduction*]

Le président : Bienvenue à la réunion du Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants. Je m'appelle Tony Dean et je suis un sénateur de l'Ontario et président du comité. Mes collègues du comité se joignent à moi aujourd'hui, et je les invite à se présenter, en commençant par notre vice-président.

[*Français*]

Le sénateur Dagenais : Jean-Guy Dagenais, du Québec.

[*Traduction*]

Le sénateur Oh : Victor Oh, de l'Ontario.

La sénatrice White : Judy White, de Terre-Neuve-et-Labrador. Je remplace la sénatrice Anderson aujourd'hui.

La sénatrice M. Deacon : Je vous souhaite la bienvenue. Marty Deacon, de l'Ontario.

Le sénateur Cardozo : Andrew Cardozo, de l'Ontario.

Le sénateur McNair : Bonjour. John McNair, du Nouveau-Brunswick. Je remplace le sénateur Kutcher aujourd'hui.

Le sénateur Yussuff : Hassan Yussuff, de l'Ontario.

La sénatrice Dasko : Donna Dasko, de l'Ontario.

Le président : Je vous remercie, chers collègues.

À ma gauche se trouve la greffière du comité, Mme Ericka Dupont, et à ma droite se trouvent les analystes de la Bibliothèque du Parlement, Anne-Marie Therrien-Tremblay et Ariel Shapiro, qui nous appuient avec une grande efficacité.

Aujourd'hui, nous accueillons trois groupes d'experts qui ont été invités à informer le comité au sujet de la désinformation et des cyberopérations dans le contexte de la guerre de la Russie contre l'Ukraine. Nous continuons à nous intéresser à l'Ukraine, mais en nous concentrant maintenant particulièrement sur les cyberopérations.

I'll begin by introducing our first panel of witnesses. From Global Affairs Canada, I'd like to welcome Tara Denham, Director General, Office of Human Rights, Freedoms and Inclusion, and Kelly Anderson, Director, International Cyber Policy. From the Communications Security Establishment, we welcome back Mr. Sami Khoury, head of the Canadian Centre for Cyber Security.

Thank you all for joining us today. We now invite you to provide your opening remarks. We'll begin with Tara Denham, who will speak on behalf of Global Affairs Canada.

Ms. Denham, whenever you're ready, please commence.

[*Translation*]

Tara Denham, Director General, Office of Human Rights, Freedoms and Inclusion, Global Affairs Canada Mr. Chair, members of the committee, thank you for your invitation to discuss disinformation and cyberoperations in the context of Russia's war against Ukraine. It's been two years since Russia invaded Ukraine.

As we enter the third year of Russia's illegal aggression against Ukraine, the Kremlin continues its efforts to reduce Ukraine's ability to defend itself. Moscow also continues to use all available means to try to reduce international support for Ukraine. These tools include cyberoperations and disinformation.

[*English*]

Cyber has been a domain of conflict since before the invasion, and it will remain a contested domain when the hostilities end. However, in both peacetime and war, there are rules that states are expected to follow for responsible state behaviour in cyberspace.

Russia has been, and continues to be, a particularly egregious actor in cyberspace. It has repeatedly disregarded the United Nations framework for responsible state behaviour in cyberspace, which makes clear how international law applies in cyberspace and promotes the UN norms for state behaviour.

Global Affairs Canada works diligently to promote and defend the framework at the UN and in our bilateral and regional engagements. We also make clear what is and what is not acceptable by calling out unacceptable behaviour.

Je commencerai par présenter notre premier groupe de témoins. Je souhaite la bienvenue à deux membres du personnel d'Affaires mondiales Canada : Tara Denham, directrice générale du Bureau des droits de la personne, des libertés et de l'inclusion, et Kelly Anderson, directrice de la Direction de la politique internationale. Nous avons également de nouveau avec nous M. Sami Khoury, dirigeant principal du Centre canadien pour la cybersécurité, du Centre de la sécurité des télécommunications.

Merci à tous de vous être joints à nous aujourd'hui. Nous vous invitons maintenant à présenter votre déclaration préliminaire. Nous commencerons par Tara Denham, qui parlera au nom d'Affaires mondiales Canada.

Madame Denham, si vous êtes prête, vous avez la parole.

[*Français*]

Tara Denham, directrice générale, Bureau des droits de la personne, des libertés et de l'inclusion, Affaires mondiales Canada : Monsieur le président, mesdames et messieurs les membres du comité, merci de votre invitation à discuter de la désinformation et des cyberopérations dans le contexte de la guerre menée par la Russie en Ukraine. Nous venons de marquer les deux ans de l'invasion de l'Ukraine par la Russie.

Alors que nous entrons dans la troisième année de l'agression illégale de la Russie contre l'Ukraine, le Kremlin poursuit ses efforts en vue de réduire la capacité de l'Ukraine à se défendre. Moscou continue également d'utiliser tous les moyens disponibles pour tenter de réduire le soutien international à l'Ukraine. Au nombre de ces outils figurent les cyberopérations et la désinformation.

[*Traduction*]

Le cyberespace était déjà un domaine de conflit avant l'invasion, et il restera un domaine contesté après la fin des hostilités. Toutefois, en temps de paix comme en temps de guerre, les États sont censés suivre des règles de comportement responsable dans le cyberespace.

La Russie a été et est toujours un acteur particulièrement outrancier dans le cyberespace. Elle a agi à plusieurs reprises au mépris du cadre de l'ONU pour un comportement responsable des États dans le cyberespace, qui précise que le droit international s'applique dans le cyberespace et qui vise à promouvoir les normes de l'ONU relatives au comportement des États.

Affaires mondiales Canada s'efforce avec diligence de promouvoir et de défendre le cadre à l'ONU autant que dans ses contacts bilatéraux et régionaux. Nous faisons également savoir ce qui est acceptable et ce qui ne l'est pas en dénonçant les comportements inacceptables.

Canada, along with partners, including the United States and the United Kingdom, have called out malicious cyber activity by Russia seven times in the last four years. Most recently, in December 2023, the Minister of Foreign Affairs issued a statement of support to the U.K. condemning electoral and political interference against the U.K. by Russia.

In addition, Canada, along with the U.S., the U.K. and the European Union, attributed malicious cyber activity against commercial satellite communications networks to disrupt Ukrainian command and control during the February 2022 invasion. Those actions had extensive spillover impacts in other European countries not involved in the conflict.

Canada also works to lessen and mitigate the impact of Russian cyber operations against Ukraine by helping Ukraine build its cyber resilience. In February 2024, the Prime Minister announced further funding for cyber assistance to Ukraine to strengthen Ukraine's ability to deter and counter cyber-enabled threats from Russia and Russian affiliated non-state actors.

Canada has also been a leading voice in creating and shaping the civilian platform that organizes cyber assistance to Ukraine, which is called the Tallinn Mechanism. The Tallinn Mechanism provides a platform to enable cyber capacity building to be coordinated, avoid duplication and meet Ukraine's priority needs. It complements similar work that takes place in the military domain.

Along with malicious cyber activities, Russia has long employed state-sponsored disinformation as part of a broader hybrid tool kit to achieve its geopolitical and military objectives globally. In the case of Ukraine, Russia conceals, blurs and fabricates information to gain military advantage, demoralize Ukrainians, divide allies and garner domestic and international support for its illegal invasion.

Russia has also increased its targeting of the broader international audiences, notably in Africa and Latin America. For example, narratives about Ukraine being at fault for the global food crisis are spread by Russian political figures and furthered on social media and in state-owned media articles.

In response, Canada has adopted a strong posture to counter Russia's efforts to manipulate false information and narratives in their favour. We have publicly called out the Kremlin on its disinformation tactics related to Ukraine, including through campaigns on Russia's illegal annexation of Donetsk, Kherson, Luhansk and Zaporizhzhya oblasts of Ukraine. We have issued

Avec ses partenaires, dont les États-Unis et le Royaume-Uni, le Canada a dénoncé des cyberactivités malveillantes de la Russie à sept reprises au cours des quatre dernières années. La dernière fois, en décembre 2023, la ministre des Affaires étrangères a publié une déclaration de soutien au Royaume-Uni qui condamnait l'ingérence électorale et politique de la Russie dans ce pays.

De plus, avec les États-Unis, le Royaume-Uni et l'Union européenne, le Canada a attribué à la Russie des cyberactivités malveillantes menées contre des réseaux commerciaux de communications par satellite dans le but de perturber le commandement et le contrôle ukrainiens au cours de l'invasion en février 2022. Ces actes ont eu des répercussions considérables, y compris dans d'autres pays européens qui ne participent pas au conflit.

Le Canada s'efforce également de réduire et d'atténuer les répercussions des cyberopérations de la Russie contre l'Ukraine en aidant l'Ukraine à développer sa cyberrésilience. En février 2024, le premier ministre a annoncé un financement supplémentaire pour la cyberassistance à l'Ukraine afin de renforcer la capacité de l'Ukraine à prévenir et à contrer les menaces de nature cybernétique venant de la Russie et d'acteurs non étatiques proches de la Russie.

Le Canada a également été un chef de file dans la création et l'établissement de la plateforme civile qui organise la cyberassistance à l'Ukraine : le mécanisme de Tallinn. Le mécanisme de Tallinn procure une plateforme qui vise à permettre la coordination du renforcement des cybercapacités, à éviter les doubles emplois et à répondre aux besoins prioritaires de l'Ukraine. Il complète des efforts comparables déployés dans le domaine militaire.

Outre ses cyberactivités malveillantes, la Russie a depuis longtemps recours à la désinformation cautionnée par l'État dans le cadre d'une panoplie hybride plus large d'outils pour atteindre ses objectifs géopolitiques et militaires à l'échelle mondiale. Dans le cas de l'Ukraine, la Russie dissimule, obscurcit et fabrique des renseignements pour obtenir un avantage militaire, démoraliser les Ukrainiens, diviser les alliés et obtenir du soutien en Russie et à l'étranger pour son invasion illégale.

La Russie cible également plus qu'avant le public au sens large à l'international, notamment en Afrique et en Amérique latine. Par exemple, des discours qui font porter à l'Ukraine la responsabilité de la crise alimentaire mondiale sont diffusés par des personnalités politiques russes et propagés dans les médias sociaux et dans des articles publiés par la presse d'État.

En réaction, le Canada a adopté une position ferme pour contrer les efforts déployés par la Russie afin de manipuler en sa faveur de fausses informations et histoires. Nous avons publiquement dénoncé les tactiques de désinformation du Kremlin concernant l'Ukraine, notamment au moyen de campagnes sur l'annexion illégale par la Russie des oblasts

video exposés, highlighting Kremlin tactics on the exploitation of social media platforms, state-sponsored media and disinformation.

We work with allies to monitor, report and share assessments of Russian disinformation, such as through the G7 Rapid Response Mechanism, which was announced in 2018 in Charlevoix as part of Canada's presidency.

Canada has deployed sanctions to target entities and individuals involved in Russian disinformation operations. To date, we have sanctioned seven individuals and three entities for their roles in disseminating disinformation targeting Ukrainian audiences. We also fund projects to support whole-of-society counter disinformation efforts.

We've long acknowledged that no government can tackle this issue alone, so it's important to work with civil society and academia. For example, Canada is providing $2.5 million to the International Institute for Democracy and Electoral Assistance to increase the capacity of civil society organizations to more effectively counter foreign information manipulation.

With that, I think I'll close my opening comments and look forward to your questions.

The Chair: Right on the button. Thank you, Ms. Denham.

We now go to Mr. Sami Khoury. Welcome back. Please go ahead whenever you're ready. We're looking forward to hearing from you.

Sami Khoury, Head, Canadian Centre for Cyber Security, Communications Security Establishment: Good afternoon, chair and members of the committee. Thank you for the invitation to appear today. I'd like to begin by providing an overview of the cyber-threat landscape, focusing on threats emanating from Russia. Following this, I will provide an overview of how the Communications Security Establishment, or CSE, has worked to support a unified global response to Russia's invasion of Ukraine.

[*Translation*]

With technology advancing at a rapid pace, the cyberthreat landscape in Canada is also constantly evolving. In a global environment marked by destabilizing events, threat actors are adapting their activities and using emerging disruptive

ukrainiens de Donetsk, de Kherson, de Louhansk et de Zaporijjia. Nous avons publié des vidéos qui mettent en lumière les tactiques du Kremlin dans les domaines de l'exploitation des plateformes de médias sociaux, des médias d'État et de la désinformation.

En collaboration avec des alliés, nous surveillons et signalons la désinformation russe et nous échangeons des évaluations à ce propos, par exemple dans le cadre du Mécanisme de réponse rapide du G7, qui a été annoncé en 2018 à Charlevoix dans le cadre de la présidence canadienne.

Le Canada a appliqué des sanctions contre des entités et des personnes impliquées dans des opérations russes de désinformation. À ce jour, nous avons infligé des sanctions à sept personnes et trois entités pour leur rôle dans la diffusion de désinformation ciblant des auditoires ukrainiens. Nous finançons également des projets pour appuyer des efforts pansociétaux pour contrer la désinformation.

Nous reconnaissons depuis longtemps qu'aucun gouvernement ne peut régler seul ce problème, c'est pourquoi il est important de collaborer avec la société civile et le monde universitaire. Par exemple, le Canada verse 2,5 millions de dollars à l'Institut international pour la démocratie et l'assistance électorale afin de renforcer la capacité des organismes de la société civile de contrer avec efficacité la manipulation de l'information par des acteurs étrangers.

Sur ce, je pense que je vais conclure mes observations préliminaires. Je me ferai un plaisir de répondre à vos questions.

Le président : Vous êtes pile dans les temps. Je vous remercie, madame Denham.

Nous passons maintenant à M. Sami Khoury. Nous sommes heureux que vous soyez de nouveau parmi nous. Si vous êtes prêt, vous avez la parole. Nous avons hâte de vous entendre.

Sami Khoury, dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications : Bonjour, monsieur le président, mesdames et messieurs les membres du comité. Je vous remercie de m'avoir invité à comparaître aujourd'hui. Pour commencer, j'aimerais donner un aperçu des cybermenaces en concentrant mon propos sur les menaces qui viennent de la Russie. Je donnerai ensuite un aperçu des efforts entrepris par le Centre de la sécurité des télécommunications pour encourager une réaction mondiale unifiée à l'invasion de l'Ukraine par la Russie.

[*Français*]

La technologie progressant à un rythme rapide, le contexte des cybermenaces évolue lui aussi constamment au Canada. Dans un environnement mondial marqué par des événements déstabilisants, les auteures et auteurs de menaces adaptent leurs

technologies, such as generative artificial intelligence, to achieve their financial, geopolitical and ideological goals.

[*English*]

Cybercrime, including ransomware, continues to be the cyber-threat activity most likely to affect Canadians and Canadian organizations. However, the state-sponsored programs of Russia, China, Iran and North Korea continue to pose the greatest strategic cyber-threat to Canada.

Russia's invasion of Ukraine in February 2022 gave the world a new understanding of how cyber activity is used to support wartime operations. Russian-sponsored malicious cyber activity against Ukraine has disrupted or attempted to disrupt organizations in government, finance and energy, often coinciding with conventional military operations. Cyber and military activities have also been supported by coordinated disinformation operations.

The Centre for Cyber Security's *National Cyber Threat Assessment* unclassified report outlined how nation-states are increasingly willing and able to use misinformation and disinformation to advance their geopolitical interests.

Furthermore, AI-enabled technologies are making fake content easier to manufacture and harder to detect. Adversary states are constantly circulating and amplifying false content that supports their interests.

[*Translation*]

Since the Russian invasion of Ukraine, we have seen numerous Russian-sponsored online disinformation campaigns aimed at spreading false information about Canada's involvement in the Russia-Ukraine conflict and about NATO allies in order to discredit them.

For example, the controlled media have been ordered to include doctored images of members of the Canadian Armed Forces deployed on the front line and to publish false allegations that the Canadian Armed Forces are committing war crimes.

[*English*]

Beyond disinformation, state-sponsored actors are targeting critical infrastructure to collect information through espionage, to pre-position in case of future hostility and as a form of power projection and intimidation.

activités et utilisent des technologies perturbatrices émergentes, comme l'intelligence artificielle générative, pour atteindre leurs objectifs financiers, géopolitiques et idéologiques.

[*Traduction*]

La cybercriminalité, y compris les rançongiciels, reste la cybermenace à laquelle les Canadiens et les organismes canadiens sont les plus exposés. Toutefois, les programmes d'État de la Russie, de la Chine, de l'Iran et de la Corée du Nord demeurent la principale cybermenace stratégique pour le Canada.

L'invasion de l'Ukraine par la Russie en février 2022 a donné au monde une nouvelle perspective sur le recours à des cyberactivités pour appuyer des opérations de guerre. Les cyberactivités malveillantes contre l'Ukraine cautionnées par la Russie ont perturbé ou tenté de perturber les activités d'organismes du secteur public, du secteur des finances et du secteur de l'énergie, souvent en parallèle avec des opérations militaires conventionnelles. Les cyberactivités et les activités militaires ont également été appuyées par des opérations coordonnées de désinformation.

Le rapport non classifié *Évaluation des cybermenaces nationales* du Centre pour la cybersécurité a mentionné que les États-nations ont de plus en plus la volonté et la capacité d'avoir recours à la mésinformation et à la désinformation pour promouvoir leurs intérêts géopolitiques.

En outre, avec les technologies de l'intelligence artificielle, il est plus facile de créer de faux contenus et ceux-ci sont plus difficiles à détecter. Les États adversaires font constamment circuler et amplifient de faux contenus pour appuyer leurs intérêts.

[*Français*]

Depuis l'invasion russe en Ukraine, nous avons observé de nombreuses campagnes de désinformation en ligne qui ont été parrainées par la Russie et qui visent à transmettre de la fausse information sur la participation du Canada dans le conflit entre la Russie et l'Ukraine et sur des alliés de l'OTAN, dans le but de les discréditer.

Par exemple, les médias contrôlés ont reçu l'ordre d'inclure des images trafiquées de membres des Forces armées canadiennes déployés en première ligne et de publier de fausses allégations selon lesquelles les Forces armées canadiennes commettent des crimes de guerre.

[*Traduction*]

Au-delà de la désinformation, les acteurs parrainés par les États ciblent les infrastructures essentielles pour recueillir de l'information à la faveur d'activités d'espionnage, pour se prépositionner en cas d'hostilités futures et comme une forme de projection de puissance et d'intimidation.

The invasion of Ukraine has demonstrated that Russia is increasingly willing to use cyber activity against critical infrastructure as a foreign policy lever.

Closer to home, foreign cyber-threat actors, including Russian-backed actors, are attempting to target Canadian critical infrastructure networks, as well as their operational and information technology.

While I can't speak to CSE or the Cyber Centre's specific operations, I can confirm that we have been tracking cyber-threat activity and have been working with Ukraine to monitor, detect and investigate potential threats, and to take active measures to address them.

The Cyber Centre has also been working closely with domestic partners and international allies to support a unified global response to Russia's invasion of Ukraine. Specifically, we have monitored for malicious Russian cyber activity against Canada, Ukraine and NATO; bolstered the Government of Canada's defences against known Russian-backed cyber-threat activity and countered Russian disinformation; shared cyber-threat information with key partners in Ukraine, NATO allies and Canadian critical infrastructure; and provided intelligence and cybersecurity support to Operation UNIFIER, the Canadian Armed Forces training mission in support of Ukraine;

At the request of our Latvian allies, the Cyber Centre has also deployed personnel to help defend against cyber-threats on Latvia's critical infrastructure and government network.

[*Translation*]

These deployments are part of a joint mission involving cybersecurity specialists from the Canadian Armed Forces, the Canadian Centre for Cyber Security and its Latvian counterpart.

This joint mission helped defend a NATO ally against hostile cyberthreats.

[*English*]

Last week's defence policy update, *Our North, Strong and Free*, highlights the need to respond to significant global shifts and an evolving threat landscape.

L'invasion de l'Ukraine a montré que la Russie est de plus en plus disposée à se servir de cyberactivités contre des infrastructures essentielles pour exercer des pressions en politique étrangère.

Plus près de chez nous, des auteurs étrangers de cybermenaces, dont des acteurs appuyés par la Russie, tentent de cibler les réseaux d'infrastructures essentielles du Canada ainsi que leurs technologies opérationnelles et technologies de l'information.

Bien que je ne puisse pas donner de détails concernant les opérations du Centre de la sécurité des télécommunications ou du Centre canadien pour la cybersécurité, je peux confirmer que nous avons suivi des cybermenaces et que nous collaborons avec l'Ukraine pour assurer la surveillance et la détection des menaces potentielles, mener des enquêtes et prendre des mesures actives pour faire face à ces menaces.

Le Centre canadien pour la cybersécurité travaille également en étroite collaboration avec des partenaires canadiens et des alliés étrangers pour encourager une réaction mondiale unifiée à l'invasion de l'Ukraine par la Russie. Plus précisément, nous avons mené une surveillance axée sur les cyberactivités malveillantes de la Russie contre le Canada, l'Ukraine et l'OTAN; nous avons renforcé les défenses du gouvernement du Canada contre les cybermenaces connues appuyées par la Russie et nous avons contré la désinformation russe; nous avons échangé des renseignements sur les cybermenaces avec des partenaires clés en Ukraine, avec nos alliés au sein de l'OTAN et avec les responsables des infrastructures essentielles du Canada; et nous avons fourni des renseignements et un appui en matière de cybersécurité à l'opération Unifier, la mission d'instruction des Forces armées canadiennes en soutien à l'Ukraine.

À la demande de nos alliés lettons, le Centre canadien pour la cybersécurité a également déployé du personnel pour contribuer à la défense des infrastructures essentielles et du réseau du gouvernement de la Lettonie contre les cybermenaces.

[*Français*]

Ces déploiements s'inscrivent dans une mission conjointe faisant appel à des spécialistes de la cybersécurité des Forces armées canadiennes, du Centre canadien pour la cybersécurité et de son équivalent letton.

Cette mission conjointe a aidé à défendre un allié de l'OTAN contre des cybermenaces adverses.

[*Traduction*]

La mise à jour de la semaine dernière de la politique de défense, *Notre Nord, fort et libre*, met en lumière la nécessité de réagir à des changements majeurs à l'échelle mondiale et à l'évolution des menaces.

As you heard from the minister, the government has announced a commitment of $8.1 billion in further investment into Canada's defence capabilities over the next five years. This includes a $1 billion commitment to CSE's foreign cyber operations program and to increase foreign intelligence collection capabilities.

In total, the defence policy update commits $2.8 billion over 20 years for cyber capabilities. These investments will enable Canada to take action through cyberspace that counter threats, advance foreign policy interests and support military operations.

[*Translation*]

In conclusion, as we adapt to an ever-changing threat environment, we will continue to work closely with our Five Eyes partners and leverage our unique technical and operational expertise and capabilities to confidently ensure Canada's resilience to cyberthreats and disinformation.

[*English*]

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

The Chair: Thank you, Mr. Khoury.

Colleagues, our panellists are with us for one hour. To ensure each member can participate fully, we're limiting the question and answer to four minutes. Please keep your question succinct and identify the person you're addressing the question to.

[*Translation*]

Senator Dagenais: My first question is for Mr. Khoury. The war in Ukraine has been going on for over two years. There's the year leading up to the war and the time since the invasion. The Russian disinformation surely began well before the start of the conflict.

Can you tell us to what extent Russian cyberoperations have changed or evolved over time? Also, in general, how long does it take to spot and distinguish between the real and the fake?

Mr. Khoury: Thank you for your question.

Comme vous l'avez entendu de la bouche du ministre, le gouvernement a annoncé un engagement de 8,1 milliards de dollars en investissements supplémentaires dans les capacités de défense du Canada au cours des cinq prochaines années. Cela comprend un engagement de 1 milliard de dollars pour le programme des cyberopérations étrangères du Centre de la sécurité des télécommunications et pour renforcer les capacités de collecte de renseignements étrangers.

En tout, la mise à jour de la politique de défense prévoit 2,8 milliards de dollars sur 20 ans pour les cybercapacités. Ces investissements permettront au Canada de prendre des mesures dans le cyberespace pour contrer les menaces, promouvoir ses intérêts en politique étrangère et appuyer des opérations militaires.

[*Français*]

En conclusion, à mesure que nous nous adaptons à un environnement de menace qui évolue sans cesse, nous continuerons de travailler étroitement avec nos partenaires de la collectivité des cinq et de tirer avantage de notre expertise et de nos capacités techniques et opérationnelles uniques, pour assurer en toute confiance la résilience du Canada par rapport aux cybermenaces et à la désinformation.

[*Traduction*]

Sur ce, je vous remercie de me donner l'occasion de comparaître devant vous aujourd'hui. C'est avec plaisir que je répondrai à vos questions.

Le président : Je vous remercie, monsieur Khoury.

Chers collègues, les témoins sont avec nous pour une heure. Pour que la participation pleine et entière de chaque membre soit possible, nous limitons la question et la réponse à quatre minutes. Veuillez poser des questions succinctes et mentionner à qui vous les adressez.

[*Français*]

Le sénateur Dagenais : Ma première question s'adresse à M. Khoury. La guerre en Ukraine dure depuis plus de deux ans. Il y a un an avant la guerre et maintenant un an depuis le début de la guerre. La désinformation russe avait sûrement commencé bien avant le début du conflit.

Pouvez-vous nous dire dans quelle mesure les cyberopérations russes ont changé ou évolué dans le temps? De plus, en général, combien de temps faut-il avant de repérer et de différencier le vrai du faux?

M. Khoury : Je vous remercie pour la question.

Indeed, Russia has been obsessed with Ukraine since 2014 or 2015. There has been a series of cyberactivities that began at that time; some have been quite damaging in terms of critical infrastructure.

We are well informed through our intelligence teams and through the partnership we have with our Five Eyes colleagues about what is happening in Ukraine. We have seen the evolution of Russian tactics and a fairly rapid adaptation of these tactics. So, as soon as we detect something, we issue a bulletin to help our communities defend themselves. We've seen that the Russians will often adapt or modify their techniques within 24 hours to try and get round what we're doing. So they are quite agile in adapting to our measures.

Along with Ukraine and our Five Eyes partners, we have a good pulse on their activities and we are helping our Ukrainian colleagues. In addition, we are learning about ways to defend Canada and we are increasing the resilience of our organizations.

Senator Dagenais: My second question is for Ms. Anderson. I'd like to talk to you about the government's decision-making in relation to the disinformation spread by the Russians. Have the reports of Russian cyberoperations by the Canadian Centre for Cyber Security led to changes in decision-making? Have the reports sometimes come too late to give you a more accurate picture of the situation?

Kelly Anderson, Director, International Cyber Policy, Global Affairs Canada: Thank you for the question. I would say that we work very closely with Mr. Khoury and his team. So we obtain information fairly quickly to decide what we need to do about cybersecurity issues.

That said, the process for deciding whether to make a public attribution of cybersecurity issues is fairly lengthy, because we want to be really sure, within the federal community, that we know the nature of the event and that we take into account the effects that relate to the framework for responsible state behaviour in cyberspace.

This includes the impact on international law, but also certain standards of responsible behaviour.

[*English*]

Senator Oh: Thank you, witnesses, for being here.

My question for the panel is how do cyber operations, such as hacking and misinformation campaigns, overlap with Russia's military action in Ukraine? What risks does this intersection pose for Canada's cybersecurity?

Effectivement, la Russie a une obsession avec l'Ukraine depuis 2014 ou 2015. Il y a eu une série de cyberactivités qui ont commencé à ce moment-là; certaines ont été assez dommageables sur le plan de l'infrastructure critique.

Nous sommes bien informés par nos équipes de renseignement et par le partenariat que nous avons avec nos collègues de la collectivité des cinq pour savoir ce qui se passe sur le chantier ukrainien. On a vu l'évolution des tactiques russes et une adaptation assez rapide de ces tactiques. Donc, dès qu'on détecte quelque chose, on émet un bulletin pour aider nos communautés à se défendre. On a constaté que souvent, en moins de 24 heures, les Russes adaptent ou modifient leurs techniques pour essayer de contourner un peu ce que nous faisons. Donc, ils sont assez agiles pour s'adapter à nos mesures.

Nous, avec l'Ukraine et avec nos partenaires de la collectivité des cinq, nous avons un bon pouls de leurs activités et nous aidons nos collègues ukrainiens. De plus, on s'informe sur les manières de défendre le Canada et nous augmentons la résilience de nos organisations.

Le sénateur Dagenais : Ma deuxième question s'adresse à Mme Anderson. J'aimerais parler avec vous des prises de décisions du gouvernement en relation avec la désinformation véhiculée par les Russes. Est-ce que les signalements des cyberopérations russes par le Centre canadien pour la cybersécurité ont entraîné des changements dans les prises de décisions? Est-ce que les signalements sont parfois arrivés trop tard pour vous donner un éclairage plus réel de la situation?

Kelly Anderson, directrice, Direction de la politique internationale, Affaires mondiales Canada : Merci pour la question. Je dirais qu'on travaille très étroitement avec M. Khoury et son équipe. Donc, on a de l'information assez rapidement pour décider ce qu'on doit faire concernant les questions de cybersécurité.

Cela dit, le processus pour déterminer si on va faire une attribution publique concernant les questions de cybersécurité est assez long, parce qu'on veut être vraiment certain, au sein de la communauté fédérale, de connaître la nature de l'événement et qu'on prend en considération les effets qui ont trait au cadre des activités responsables des États dans le cyberespace.

Cela inclut l'impact sur le droit international, mais aussi certaines normes de comportement responsable.

[*Traduction*]

Le sénateur Oh : Je remercie les témoins d'être ici.

Ma question au groupe de témoins concerne l'éventuelle concordance entre les cyberopérations, comme le piratage et les campagnes de désinformation, et l'action militaire de la Russie en Ukraine. Quels risques cette concordance représente-t-elle pour la cybersécurité du Canada?

I want to add one more question: Does the Canadian government provide enough funding to counter cybersecurity operations in Canada?

Mr. Khoury: Thank you for the question. I can answer the first part of your question.

Since the invasion of Ukraine, we've seen a synchronization between Canadian cooperation and cyber operations. Russia's goal was to weaken civil society and the government through cyber operations and also inflict some damage that has impacted, for example, the telecommunications infrastructure in Ukraine.

We learn a lot from all of these cyber activities. We monitor them closely through our foreign intelligence mission, but also through the partnership we have with our allies. As quickly as we can, we turn what we learn from these into alerts, cyber flashes and advisories to promote resilience. Those started even before Russia invaded Ukraine. We had a sense that these activities were going on, and we issued a number of alerts even before Russia invaded Ukraine to ask that organizations be vigilant and on top of their IT.

Ms. Denham: On disinformation, again, Russia uses a whole slew of tool kits, and they use them very strategically to align one with the other. On disinformation, specifically, what we saw before the invasion was one of the narratives — and you'll probably all be familiar with it — but at the time you heard that Ukraine was being overrun by Nazis. Probably people in the room heard that narrative. That started over a year before going through Russian disinformation campaigns. In 2021, when you looked at Russian state-sponsored media, the citation of Nazism was at about 3%, and then just before the invasion, it was up to over 20% in the narrative. So you can see how they start to flood the narrative space.

That's one of the tactics.

When you combine it with cyber activities, laying the foundations, having not only Ukrainians but also the international community question what actions are and will be taken — and, in fact, hopefully they're trying themselves to sow support for that illegal invasion.

We have to be more and more aware of how the military operations are completely tied into and often preempted by some of the disinformation and other activities that are being laid out, which could be months and years in advance.

Senator Oh: How about the government funding? Do we need more funding for a counteroffensive?

J'aimerais ajouter une autre question : le gouvernement du Canada fournit-il un financement suffisant pour contrer les opérations de cybersécurité au Canada?

M. Khoury : Je vous remercie pour votre question. Je peux répondre à la première partie.

Depuis l'invasion de l'Ukraine, nous assistons à une synchronisation entre la coopération canadienne et les cyberopérations. L'objectif de la Russie était d'affaiblir la société civile et le gouvernement par des cyberopérations et aussi d'infliger des dommages qui ont touché, par exemple, les infrastructures de télécommunication en Ukraine.

Toutes ces cyberactivités nous en apprennent beaucoup. Nous les surveillons de près dans le cadre de notre mission de renseignement étranger, mais aussi dans le cadre du partenariat avec nos alliés. Nous transformons le plus vite possible ce que nous apprennent ces cyberactivités en alertes, en bulletins et en avis pour promouvoir la résilience. Ces efforts ont commencé avant même l'invasion de l'Ukraine par la Russie. Nous avions l'impression que ces activités avaient lieu, et nous avons publié plusieurs alertes avant même l'invasion de l'Ukraine par la Russie pour demander aux responsables d'organisme d'être vigilants et de surveiller leurs technologies de l'information.

Mme Denham : Concernant la désinformation, encore une fois, la Russie utilise toute une panoplie d'outils, et elle les utilise de manière très stratégique pour les faire concorder. En ce qui concerne la désinformation, plus précisément, ce que l'on a vu avant l'invasion était l'un des discours — et vous le connaissez probablement tous —, à l'époque, selon lequel l'Ukraine était aux mains des nazis. Les personnes présentes ont probablement entendu cette histoire. Tout cela avait commencé plus d'un an plus tôt dans les campagnes de désinformation russes. En 2021, quand on examinait les médias d'État russes, le nazisme était mentionné dans environ 3 % des cas; juste avant l'invasion, il était mentionné dans plus de 20 % de ce qui se racontait. On voit donc l'inondation de l'espace du discours.

C'est l'une des tactiques.

Combinée à des cyberactivités, elle correspond à la pose de fondations; il s'agit que non seulement les Ukrainiens, mais aussi la communauté internationale, s'interrogent sur les mesures prises et sur celles qui le seront — et, en fait, il y a, espérons-le, une tentative de susciter l'appui pour cette invasion illégale.

Nous devons prendre conscience du fait que les opérations militaires sont complètement liées à certaines des activités de désinformation et autres préparées, et souvent devancées par elles, parfois de plusieurs mois et années.

Le sénateur Oh : Qu'en est-il du financement par le gouvernement? Faut-il relever le financement pour mener une contre-offensive?

Ms. Denham: We're always reviewing the support that's required. We just had the Defence Policy Update and funding announced. There's always a recurring review.

For our disinformation team, there was an announcement after we were created in 2018 — an acknowledgement on the strength of Russian-specific disinformation. That team was expanded in 2022.

We're always going through revisions. Of course, if there are more capabilities, we're able to work on those. But we're continuing to review those requirements.

Senator M. Deacon: Thank you to all of you and your teams for being here today. It's very much appreciated.

Ms. Denham, you mentioned how Canada is assisting Ukraine in its cyber defences. I'm wondering how deep this cooperation can go. Mainly, does it extend to offensive operations as well? I'm wondering about the norms of war when it comes to cyber operations. Is it more of a grey area if we assisted Ukraine's cyber operations, or would it be akin to sending Canadian troops on the ground? I'm trying to distinguish those differences.

Russia for instance — you talked about it — is constantly at work online here in Canada. I think it's fair game if we assisted Ukraine in trying to shut down a power station with a cyberattack, for instance. Or would that be similar to declaring war on Russia?

I'm trying to make the distinction between cyber and boots on the ground.

Ms. Denham: Maybe I'll start, and if my colleagues want to add in, they may. Again, I'm not placed to speak specifically to military operations. A lot of the work we do and that I was referencing is building up civilian cyber capabilities with Ukraine. That's the Tallinn Mechanism that we referenced. There are the military operations — and National Defence or others are more engaging in those discussions — but just as important is to build up the resilience of Ukrainian civil society and organizations to respond to the cyber incidents when they're happening. That is separate from, as you're indicating, a specific military operation.

The other part that is important that we are always focused on is, as was referenced, the UN norms of responsible state behaviour in cyberspace. So for any actions that we would be taking or advocating be taken, Global Affairs Canada would be advising in terms of whether the actions aligned with what has been agreed within a UN framework.

Mme Denham : Nous examinons en permanence le soutien nécessaire. La mise à jour de la politique de défense et un financement viennent d'être annoncés. Il y a toujours un examen récurrent.

En ce qui concerne notre équipe chargée de la désinformation, il y a eu une annonce après notre création en 2018, une reconnaissance de la puissance de la désinformation propre à la Russie. Cette équipe a été élargie en 2022.

Nous procédons en permanence à des examens. Bien entendu, s'il y a plus de ressources, nous pouvons les mettre à profit. Toutefois, nous examinons en permanence ces besoins.

La sénatrice M. Deacon : Je remercie chacun d'entre vous ainsi que vos équipes d'être ici aujourd'hui. Je vous en suis très reconnaissante.

Madame Denham, vous avez mentionné que le Canada aide l'Ukraine à se défendre dans le cyberespace. Je me demande à quel point cette coopération est poussée. Surtout, s'étend-elle à des opérations offensives? Je m'interroge sur les normes de guerre en ce qui concerne les cyberopérations. Appuyer les cyberopérations de l'Ukraine, est-ce une zone grise ou cela équivaudrait-il à envoyer des troupes canadiennes sur le terrain? J'essaie de faire la distinction.

La Russie, par exemple — vous en avez parlé —, agit constamment en ligne ici, au Canada. Je pense qu'il serait légitime que le Canada aide l'Ukraine à essayer de mettre hors service une centrale électrique en menant une cyberattaque, par exemple. Ou cela reviendrait-il à déclarer la guerre à la Russie?

J'essaie de faire la distinction entre le cyberespace et les troupes sur le terrain.

Mme Denham : Je vais peut-être commencer, et si mes collègues souhaitent ajouter quelque chose, ils le feront ensuite. Encore une fois, je ne suis pas en mesure de donner des détails sur les opérations militaires. Une grande partie du travail que nous effectuons et auquel je faisais référence consiste à développer les cybercapacités civiles avec l'Ukraine. C'est le mécanisme de Tallinn que nous avons mentionné. Il y a les opérations militaires — et la Défense nationale ou d'autres participent davantage à ces discussions —, mais il est tout aussi important de renforcer la résilience de la société civile et des organismes ukrainiens pour qu'ils puissent réagir aux cyberincidents qui se produisent. C'est distinct, comme vous le dites, d'une opération militaire.

L'autre élément important auquel nous prêtons toujours attention, comme nous l'avons mentionné, concerne les normes de l'ONU pour un comportement responsable des États dans le cyberespace. Donc, chaque fois que nous prenons ou que nous préconisons une mesure, Affaires mondiales Canada donne un avis concernant sa conformité avec ce dont il a été convenu dans le cadre adopté par l'ONU.

That's a lot of where we're having the conversations with our whole-of-government colleagues in terms of the capabilities that we're supporting and where some of the advice and advocacy are in terms of the behaviour in cyberspace.

I'm not sure if Sami would like to add more.

Mr. Khoury: Thank you for the question.

We've been a strong supporter of Ukraine and have been working through the Canadian Forces. I will defer to the Canadian Forces as to what they do on the ground, but we've worked through them to pass to Ukrainian partners over there either intelligence or cyberdefence tips to have them build some resilience in their society. We've also worked with neighbouring countries, like Latvia, to also build that layer of resilience on the perimeter.

We know that Russia has pretty impressive cyber capabilities, and they haven't hesitated to use them in 2015 and 2016 to shut down the electric grid in Ukraine. We are very mindful of that. Whenever we see something funny or suspicious in Ukraine, we want to learn from it, because we don't want those capabilities to make their way to Canada.

From a team perspective, we're very concerned about cyber defence and how to build national resilience in Canada against all of these threats.

The Chair: That was a question that was on all of our minds, Senator Deacon, so thank you for asking it.

Senator Boehm: Thank you to our witnesses for being here. It's always great to see former colleagues appear as witnesses.

Ms. Denham, you mentioned the G7 Rapid Response Mechanism, or RRM, as it was established by leaders in 2018 and first discussed by foreign ministers and then at the leaders' table. As I recall from those discussions, because I was there, there was some concern about the viability of the Rapid Response Mechanism and whether it would continue through to other G7 presidencies, how it would be funded and whether it was nimble enough to expand.

I met with the Latvian ambassador this afternoon. We talked a lot about Canadian-Latvian cooperation. It is not that Latvia is looking to join the G7 or anything like that, but is there enough space within the mechanism, first of all, to expand cooperation with countries that are not in the G7? Is it being sufficiently

C'est en grande partie le sujet de nos discussions avec nos collègues du reste du gouvernement en ce qui concerne les capacités que nous appuyons ainsi que la teneur des avis et recommandations concernant le comportement dans le cyberespace.

Je ne sais pas si M. Khoury souhaite ajouter quelque chose.

M. Khoury : Je vous remercie pour votre question.

Le Canada est un ardent défenseur de l'Ukraine et il agit par l'intermédiaire des Forces canadiennes. Je laisse aux responsables des Forces canadiennes le soin d'expliquer ce qu'elles font sur le terrain, mais nous avons collaboré avec elles pour transmettre par leur intermédiaire des renseignements ou des conseils en matière de cyberdéfense à des partenaires ukrainiens sur place, pour qu'ils acquièrent une certaine résilience dans leur société. Nous avons aussi collaboré avec des pays voisins, comme la Lettonie, pour mettre en place cette dimension de résilience également sur le périmètre.

Nous savons que la Russie a des cybercapacités assez impressionnantes, et elle n'a pas hésité à en faire usage en 2015 et en 2016 pour paralyser le réseau électrique en Ukraine. Nous en sommes bien conscients. Chaque fois que nous voyons quelque chose d'inhabituel ou de suspect en Ukraine, nous voulons en tirer les leçons, parce que nous ne voulons pas que ces capacités soient mises en œuvre au Canada.

Dans la perspective de l'équipe que nous formons, nous nous préoccupons beaucoup de la question de la cyberdéfense et de l'amélioration de la résilience nationale au Canada face à toutes ces menaces.

Le président : C'est une question que nous nous posions tous, sénatrice Deacon; je vous remercie de l'avoir posée.

Le sénateur Boehm : Je remercie les témoins d'être ici. C'est toujours un plaisir de voir d'anciens collègues comparaître en tant que témoins.

Madame Denham, vous avez mentionné le Mécanisme de réponse rapide du G7, qui a été mis en place par les chefs d'État et de gouvernement en 2018 et discuté pour la première fois par les ministres des Affaires étrangères, puis par les chefs d'État et de gouvernement. Si ma mémoire est bonne, car j'ai assisté à ces discussions, il y avait une certaine inquiétude quant à la viabilité du Mécanisme de réponse rapide et quant à sa pérennité au fil des présidences du G7, quant aux modalités de son financement et quant à savoir s'il aurait l'agilité nécessaire pour permettre son élargissement.

J'ai rencontré l'ambassadeur de Lettonie cet après-midi. Nous avons beaucoup parlé de la coopération entre le Canada et la Lettonie. La Lettonie ne cherche absolument pas à se joindre au G7, mais, tout d'abord, y a-t-il suffisamment de place au sein du mécanisme pour élargir la coopération à des pays qui ne font pas

financed? Finally, is it really rapid? Because with bureaucracies, rapid response is not usually associated in the same sentence.

Is it working effectively?

Ms. Denham: Thank you for your question and for your work at the time when this was being created. I'll go through and hopefully touch on all of your points.

In terms of how to actually maintain the interests or the momentum behind the structure, typically, in G7, when initiatives are announced, it can be announced by a presidency and then perhaps the next presidency doesn't see the same importance or relevance of the issue. It can dip then in terms of concentration of energy.

At the time, it was actually decided that Canada would maintain a secretariat of the rapid response mechanism. That is not going by how we would traditionally set up these. I think it was an excellent decision at the time, because by maintaining the secretariat, we were maintaining Canadians' focus and Canada's leadership on the issue, and we've also been able to maintain the focus since 2018 and continue to build and push the RRM, to be more responsive and agile, and to expand beyond the G7 members.

That flows well into the other question: We do go beyond the G7 members. I would think of it in this way: The response is a core part, and when there's a need to respond, it would be led and coordinated by the G7 members. For example, the power of a G7 statement can be very impactful in having those G7 countries sign on. When we do need to call something out, that's where we would want to keep the focus with the G7. However, we've actually built and have other countries that participate in the conversations that we've created linkages with non-governmental academics. I believe you have Marcus Kolga coming later.

So we've tried to expand that network not only to the G7 countries, but, for example, Australia, New Zealand, other countries that are interested in the issue, they participate in the information sharing, which is at its core.

Senator Boehm: Do they participate in the financing as well, or is that strictly on our side, since we have the secretariat?

Ms. Denham: Canada finances the secretariat. Respective countries are responsible for setting up whatever structures they require in their domestic entities, as do observers. Different countries may have a different level of focus on a particular issue, and that correlates into how many resources they have invested in it.

partie du G7? Le mécanisme est-il suffisamment financé? Enfin, est-il vraiment rapide? Parce que, dans les administrations, « réponse » et « rapide » sont des termes qui ne sont habituellement pas associés l'un à l'autre.

Est-ce que cela fonctionne efficacement?

Mme Denham : Je vous remercie pour votre question et pour le travail que vous avez effectué à l'époque où cela se mettait en place. Je vais m'efforcer d'aborder un à un tous les points que vous avez évoqués.

En ce qui concerne le maintien de l'intérêt ou de la dynamique qui sous-tend la structure, habituellement, au G7, quand des initiatives sont annoncées, elles le sont par une présidence, et il arrive que la présidence suivante estime que la question n'a pas la même importance ou la même pertinence. Il arrive qu'une partie de l'énergie consacrée à la question se dissipe.

À l'époque, il a été décidé que le Canada maintiendrait un secrétariat du Mécanisme de réponse rapide. Il a été décidé de ne pas procéder de la manière habituelle. C'était à mon avis une excellente décision, à l'époque, parce que, maintenir le secrétariat, c'était maintenir l'attention des Canadiens et le leadership du Canada sur la question, et nous avons également pu maintenir l'attention depuis 2018 et poursuivre le développement et la promotion du Mécanisme de réponse rapide, pour qu'il soit plus réactif et plus agile, ainsi que l'élargissement de l'initiative à des pays qui ne sont pas membres du G7.

Cela m'amène à l'autre question : l'initiative ne se limite pas aux membres du G7. Je l'envisagerais de la façon suivante : la réaction est un élément essentiel, et quand il faut réagir, la réaction est dirigée et coordonnée par les membres du G7. Par exemple, une déclaration signée par les pays du G7 peut avoir un impact considérable. Quand il faut dénoncer quelque chose, nous voulons que l'attention se concentre sur le G7. Toutefois, nous avons bâti des relations : d'autres pays participent aux discussions; nous avons noué des liens avec des universitaires qui ne travaillent pas pour un gouvernement. Je crois que Marcus Kolga comparaîtra plus tard.

Nous avons donc essayé d'élargir ce réseau au-delà des pays du G7; par exemple, l'Australie, la Nouvelle-Zélande et d'autres pays qui s'intéressent à la question participent à l'échange de renseignements qui est au centre de l'initiative.

Le sénateur Boehm : Participent-ils aussi au financement, ou le financement nous incombe-t-il strictement étant donné que le secrétariat est au Canada?

Mme Denham : Le Canada finance le secrétariat. Les pays respectifs sont responsables de la mise en place des structures, quelles qu'elles soient, dont ils ont besoin au sein de leurs entités nationales, tout comme les observateurs. Différents pays peuvent porter un intérêt différent à une question donnée, et cet intérêt est corrélé aux ressources investies.

To date the RRM has been most prominently focused on information manipulation and disinformation, that's where we started, that's been the prominence of our focus.

To your question as to are we nimble, we have also recognized the issue of transnational repression as being a major concern. We've established a working group within the RRM, and we are working with colleagues in that area. Again, the RRM was about threats to democracy. Disinformation was the paramount focus at the time, but we have to continue to expand and be nimble to meet those challenges. And transnational repression is one we're tackling.

Finally, to close out on the rapidity with which bureaucrats can respond. There were two elements to it, one is we are all based on unclassified, open-source information; and therefore, the ability to be rapid is that we can share that quickly. We don't have to declassify intelligence; it can be passed beyond the Five Eyes. That has proven quite successful in building our understanding of the issues.

The collective response is where we've had the challenges, and that's where, as the secretariat, we've noted that it is a challenge. We are reaching out to our G7 colleagues, because it is very difficult to agree as a collective, as the G7, when we're going to call out certain actions. We have all done it individually. At times we've done it with a few of the members, but our focus is we need to be more active in the response now that we've built the entities that it's based on.

Senator Boehm: Thank you very much.

Senator Cardozo: I wonder if I could ask you to share with us a little bit more about the range of attacks that take place. Ms. Denham, you had talked about disinformation, and I think you mentioned the issue of food production, in Ukraine. Is there truth to that, in as much as Ukraine produces a large amount of wheat, that is, as I understand it, a lot of it exported to Africa? So what is truth there and what is disinformation in that issue? In general, what other kinds of cyber attacks are we seeing beyond disinformation? Is there actual warfare techniques taking place?

Ms. Denham: Maybe I'll speak first quickly to the disinformation and ask Mr. Khoury to speak more on the cyber.

À ce jour, le Mécanisme de réponse rapide a été axé avant tout sur la manipulation de l'information et la désinformation; c'est là que nous avons commencé, là que notre attention s'est portée.

Pour répondre à votre question quant à notre agilité, nous avons également reconnu que la question de la répression transnationale est une préoccupation majeure. Nous avons mis sur pied un groupe de travail à l'intérieur du Mécanisme de réponse rapide, et nous travaillons avec des collègues dans ce domaine. Encore une fois, le Mécanisme de réponse rapide concernait les menaces pour la démocratie. La désinformation était le principal sujet de préoccupation à l'époque, mais nous devons continuer à élargir le champ et à faire preuve d'agilité pour relever ces défis. La répression transnationale est l'un des défis auxquels nous nous attaquons.

Enfin, pour conclure à propos de la rapidité avec laquelle les fonctionnaires peuvent réagir, cette question touche deux dimensions : une de ces dimensions est que nous nous fondons tous sur des renseignements non classifiés, de sources ouvertes; par conséquent, nous pouvons agir promptement, puisque nous pouvons les diffuser rapidement. Il n'est pas nécessaire de déclassifier les renseignements; ils peuvent être diffusés en dehors du Groupe des cinq. Cette approche a renforcé notre compréhension des problèmes.

La réponse collective est la dimension dans laquelle les défis ont surgi; c'est là que le secrétariat a constaté une difficulté. Nous communiquons avec nos collègues du G7, parce qu'il est très difficile de se mettre d'accord pour parler d'une seule voix, en tant que G7, quand nous nous apprêtons à dénoncer certains actes. Tous les pays ont réagi individuellement. Parfois, le Canada a réagi avec quelques-uns des membres, mais la priorité pour nous, c'est que nous devons être plus actifs dans le domaine de la réponse maintenant que nous avons mis en place les entités sur lesquelles elle repose.

Le sénateur Boehm : Je vous remercie.

Le sénateur Cardozo : Puis-je vous demander de nous en dire un peu plus sur les différentes attaques qui ont lieu? Madame Denham, vous avez parlé de la désinformation, et je pense que vous avez mentionné la question de la production alimentaire en Ukraine. Dans quelle mesure ces histoires sont-elles vraies, puisque l'Ukraine produit une grande quantité de blé dont une grande partie, si j'ai bien compris, est exportée vers l'Afrique? Où est la vérité et où est la désinformation dans ce dossier? En général, en plus de la désinformation, quels autres types de cyberattaques observe-t-on? De véritables techniques de guerre sont-elles mises en œuvre?

Mme Denham : Je vais peut-être d'abord dire un mot à propos de la désinformation et demander à M. Khoury d'en dire plus sur les cyberattaques.

It's an excellent example of how the Russian narrative was blaming Ukraine for the global food crisis after the invasion, but what had actually been happening for a number of years is that there had been a building global food crisis in terms of making sure that there was sufficient wheat production and that it was moving to different parts of the world. That was amplified and made worse through COVID. So there is actually a build-up of these issues.

Then with the Russian invasion, Russia was blaming Ukraine for not getting the wheat out, but Russia had actually done the blockades and was not letting the boats, the transport, actually leave. So they take a piece of truth, which is there is a global food crisis — Ukraine has been traditionally one of the major exporters — but they manipulate it to make it sound like it was Ukraine's fault that there was a food crisis, when, in fact, Russia invaded Ukraine and put the blockades on and was damaging farmers' crops and targeting different infrastructure. So it was Russia that amplified, through the invasion, the food crisis.

That's an illustration of how information is manipulated to actually undermine the credibility of other countries.

Senator Cardozo: The other part is they were just getting that information out in large quantities?

Ms. Denham: I'll speak quickly. Cyber and digital often get intermingled. People say it's a cyber operation and, of course, we have particular definitions.

One of the easy ways to think about it is if you think of hack and leak, the hack is the cyber, using the infrastructure, breaking something, breaking and getting in and taking information; the leak is the disinformation, the manipulation of information. So the cyber infrastructure, when you talk about cyber incidents, they're targeting infrastructure or breaking something if I think of it that way; and disinformation is the manipulation of the information that may have come from a cyber incident, but not always, if that is helpful.

Mr. Khoury: Thank you for the question. If I can add, so we've seen a gradation of sophistication of cyber activity in Ukraine that Russia has done, everything from defacing websites to doing denial of service attacks against websites. That is to preclude people from achieving that. At the other extreme, we've seen many waves of — at the time it was the wiper malware. Wiper essentially is they would release this code on a network, and the sole purpose of that code is to delete all information on that network, so I would put that in the destructive category.

C'est un excellent exemple de discours construit par la Russie pour faire porter à l'Ukraine la responsabilité de la crise alimentaire mondiale après l'invasion, mais, en réalité, depuis plusieurs années, une crise alimentaire mondiale se profilait, liée à une production insuffisante de blé et à des difficultés d'expédition du blé dans différentes régions du monde. Le problème a été exacerbé et aggravé par la COVID. Les difficultés sont donc apparues progressivement.

Ensuite, avec l'invasion russe, la Russie a pointé du doigt l'Ukraine, l'accusant de ne pas expédier le blé hors du pays, alors que c'était la Russie qui était responsable des blocus et qui ne laissait pas sortir les navires, les transports. Donc, la Russie prend une part de vérité, l'existence d'une crise alimentaire mondiale — l'Ukraine est depuis longtemps l'un des principaux exportateurs —, mais elle la manipule pour donner l'impression que la crise alimentaire est imputable à l'Ukraine, alors que, en réalité, la Russie a envahi l'Ukraine, mis en place des blocus, dévasté les cultures agricoles et pris pour cible différentes infrastructures. C'est donc la Russie qui, par son invasion, a exacerbé la crise alimentaire.

Cet exemple illustre la manipulation de l'information pour miner la crédibilité d'autres pays.

Le sénateur Cardozo : L'autre élément, c'est la diffusion de cette information à grande échelle?

Mme Denham : Je vais donner une brève réponse. Le cyberespace et le numérique sont souvent mêlés. On dit qu'il s'agit d'une cyberopération et, bien sûr, il y a des définitions précises.

Une façon simple d'envisager la question est de penser à un piratage et à une fuite : le piratage est la cyberattaque; il s'agit de viser les infrastructures, de détruire, de pénétrer par effraction et d'accéder à l'information; la fuite est la désinformation, la manipulation de l'information. Donc, quand il est question de cyberinfrastructures, quand on parle de cyberincidents, les pirates prennent pour cible les infrastructures ou détruisent quelque chose, dans cette perspective; et la désinformation est la manipulation de l'information qui vient peut-être d'un cyberincident, mais pas toujours, si cette explication est utile.

M. Khoury : Je vous remercie pour votre question. J'ajouterais que nous avons observé une hausse du degré de sophistication des cyberactivités de la Russie en Ukraine, du vandalisme ciblant des sites Web aux attaques par déni de service contre des sites Web. Il s'agit d'empêcher d'y avoir accès. À l'autre extrême, on a assisté à de nombreuses vagues, à l'époque, du maliciel effaceur. Ce que l'on entend au fond par effaceur, c'est un code introduit dans un réseau et dont la seule fonction est d'effacer toutes les données sur ce réseau; il s'agit donc d'un programme destructeur.

There's been multiple waves of wiper malware that the Russians have tried to unleash on Ukrainian government infrastructure. Many of them were caught. Countermeasures were developed so that they became ineffective, but that was a bit of a cat-and-mouse game where they would release something, it gets detected. We adapt and then they tweak it, and so on.

At the other extreme, they've demonstrated they have the capability, for example, to shut down the electricity grid as early as 2015-16. So that is the gradation from just defacing websites to shutting down the electricity in a particular part of the country using cyber means.

Senator Cardozo: Can they do things to tanks, for example, to cause them to not work or turn in the opposite direction or things like that?

Mr. Khoury: I'm not knowledgeable when it comes to military technology, so I would defer to somebody maybe at National Defence. But we live in a connected world, so is it possible? Maybe.

Senator Dasko: Thank you for being with us today. Ms. Denham, you mentioned that seven people were sanctioned. Can you elaborate on that, because I think you just said it. How much can you tell us? I think that will help us understand what is considered to be sanctionable, tell us something about the situation.

Ms. Denham: Sure. On the sanctions that Canada has applied — and there's been a number of sanctions since the illegal invasion, I don't have the exact number with me. In terms of the disinformation, let me start by saying that within our sanctions regime, which we need to apply very judiciously, to be able to apply sanctions, there are a few criteria. One is that we need to be able to back it up, with the information, so that's open-source information to provide evidence of the issue; two, indications of gross human rights violations; three is — .

Ms. Anderson: International corruption.

Ms. Denham: Thank you, international corruption. Sorry, I always forget the third one.

Those are the areas for which we can apply sanctions and that the team would actually be reviewing to see if individuals that have been suggested or recommended to be sanctioned fall under one of those categories. Currently, cyber activities do not fall within those three areas. What we have been able to do is do sanctions on disinformation. There have been other sanctions about which you have heard — very public releases about

Les Russes ont tenté de faire déferler plusieurs vagues de maliciels effaceurs sur les infrastructures publiques ukrainiennes. Bon nombre de ces maliciels ont été interceptés. Des contre-mesures étaient mises au point pour les rendre inefficaces, mais c'était un jeu du chat et de la souris : les Russes lançaient un maliciel, qui était détecté; nous nous adaptions, ils le modifiaient, et ainsi de suite.

À l'autre extrême, les Russes ont montré, dès 2015-2016, qu'ils ont la capacité, par exemple, de mettre hors service le réseau électrique. Il y a donc une gradation, du simple vandalisme contre des sites Web à la panne d'électricité dans une région donnée du pays en utilisant des moyens cybernétiques.

Le sénateur Cardozo : Peuvent-ils s'en prendre avec succès à des chars, par exemple, les empêcher de fonctionner, leur faire faire demi-tour ou d'autres choses du même ordre?

M. Khoury : Je ne suis pas au fait des technologies militaires; quelqu'un de la Défense nationale pourrait peut-être vous en dire plus. Toutefois, nous vivons dans un monde connecté. Est-ce possible? Ce l'est peut-être.

La sénatrice Dasko : Je vous remercie d'être parmi nous aujourd'hui. Madame Denham, vous avez dit que sept personnes ont été sanctionnées. Pouvez-vous nous en dire plus? Je crois que vous venez de le mentionner : que pouvez-vous nous en dire? Je pense que cela nous aidera à comprendre ce qui est considéré comme sanctionnable, que cela nous dira quelque chose de la situation.

Mme Denham : Bien sûr. En ce qui concerne les sanctions que le Canada a imposées — et il y a eu plusieurs sanctions depuis l'invasion illégale —, je n'ai pas le chiffre exact avec moi. Pour ce qui est de la désinformation, permettez-moi de commencer en disant que, dans notre régime de sanctions, que nous devons appliquer très judicieusement, quelques critères doivent être remplis pour que des sanctions puissent être imposées. Premièrement, il faut être en mesure de justifier les sanctions à l'aide de renseignements; il faut donc des renseignements de sources ouvertes pour prouver les faits; deuxièmement, il y a le critère des indications de violations graves des droits de la personne; troisièmement…

Mme Anderson : Il y a le critère de la corruption internationale.

Mme Denham : Je vous remercie : il y a le critère de la corruption internationale. J'oublie toujours le troisième.

Ce sont là les domaines pour lesquels nous pouvons imposer des sanctions et que l'équipe étudie pour déterminer si les personnes contre lesquelles des sanctions ont été suggérées ou recommandées entrent dans une de ces catégories. À l'heure actuelle, les cyberactivités ne font pas partie de ces trois domaines. Ce que nous avons pu faire, c'est imposer des sanctions pour désinformation. Il y a eu d'autres sanctions dont

corruption and other human rights violations taking place within Ukraine — and those packages undergo a review, are approved and when and if possible we share that information with like-minded people in other countries, because the power and potential impact of sanctions are increased when there are multiple sanctions imposed by multiple countries on the same individuals.

Senator Dasko: Was Ukraine ever sanctioned, and by whom?

Ms. Denham: I was referencing sanctions packages put in place by Canada against the Russians who had been identified as participating in, advocating for or being a member of disinformation campaigns that had been launched.

Senator Dasko: In Canada?

Ms. Denham: No, in Ukraine.

Senator Dasko: Our laws are sanctioning actors in Ukraine who are disseminating disinformation. That's my understanding.

Ms. Denham: Yes, the individuals that were sanctioned were Russian actors — not Ukrainians — involved in disinformation campaigns, who were targeting Ukraine or undermining support for Ukraine internationally.

Senator Dasko: What kinds of sanctions did we impose on them?

Ms. Denham: I can speak generally. Again, these would be economic sanctions.

Senator Dasko: Is this public information?

Ms. Denham: The sanctions packages are all released publicly, so you can actually get the names of the individuals. I don't have them all here with me. But if you think about the economic sanctions, examples that have been made public include blocking assets, freezing assets and so forth.

[*Translation*]

Senator Carignan: My question concerns the cybersecurity ecosystem. There are more and more companies specializing in cybersecurity that are selling their services, companies that become future NVIDIAs and explode on the stock market.

vous avez entendu parler — des communiqués publics au sujet de la corruption et d'autres violations des droits de la personne en Ukraine — et ces dossiers subissent un examen, sont approuvés et, dans la mesure du possible, quand c'est possible, nous transmettons l'information à des personnes aux vues similaires dans d'autres pays, parce que la portée et l'effet potentiel des sanctions sont plus grands quand plusieurs sanctions sont imposées aux mêmes personnes par plusieurs pays.

La sénatrice Dasko : L'Ukraine a-t-elle jamais été sanctionnée, et par qui?

Mme Denham : Je parlais de séries de sanctions prises par le Canada contre les Russes qui avaient été identifiés comme des participants à des campagnes de désinformation qui avaient été lancées, ou comme des personnes qui appuyaient ces campagnes ou qui y étaient impliquées.

La sénatrice Dasko : Au Canada?

Mme Denham : Non, en Ukraine.

La sénatrice Dasko : Nos lois sanctionnent des acteurs en Ukraine qui diffusent de la désinformation. C'est ce que je comprends.

Mme Denham : Oui, les personnes qui ont été sanctionnées étaient des acteurs russes — et non des Ukrainiens — impliqués dans des campagnes de désinformation, qui prenaient l'Ukraine pour cible ou qui minaient l'appui à l'Ukraine sur la scène internationale.

La sénatrice Dasko : Quel genre de sanctions leur avons-nous imposées?

Mme Denham : Je peux en parler de manière générale. Encore une fois, il s'agit de sanctions économiques.

La sénatrice Dasko : Ces renseignements sont-ils publics?

Mme Denham : Les séries de sanctions sont toutes rendues publiques; vous pouvez trouver le nom des personnes concernées. Je ne les ai pas tous ici avec moi. Cependant, si l'on pense aux sanctions économiques, les exemples qui ont été rendus publics sont entre autres le blocage des avoirs, le gel des avoirs, parmi d'autres.

[*Français*]

Le sénateur Carignan : Ma question porte sur l'écosystème de la cybersécurité. Il y a de plus en plus d'entreprises spécialisées en cybersécurité qui vendent leurs services, des entreprises qui deviennent de futurs NVIDIA et qui explosent au marché boursier.

I'm trying to see how — or even if — these companies protect our infrastructure well. Are these companies helping to protect our critical infrastructure? I'm thinking of the electricity system, the Canadian banking system, banking transactions and all the strategic civilian infrastructure that could be targeted. Do you support them? Are you giving information to these companies or organizations, whether it is Hydro-Québec or another, that manage essential or strategic infrastructure? Or are we letting the big private companies — Israeli and American companies, for instance — that specialize in cybersecurity advise our strategic organizations or companies?

Mr. Khoury: Thank you for the question. Partnerships are very important to us, whether at the federal or provincial level or with organizations. We work with everyone to forge partnerships in order to exchange information in a timely manner, not just in times of crisis. Whether it's with the big banks or with organizations like Hydro-Québec or others, we have partnerships that enable us to share information when needed and to encourage the exchange of technical knowledge, for instance about things we see and ways we can help them defend themselves better.

As you've seen, there are a lot of commercial companies specializing in cybersecurity. At the Canadian Centre for Cyber Security, we are not in a position to recommend company A over company B. We suggest that people take certain factors into consideration before choosing who they do business with. Basically, large companies have their own cybersecurity teams and they rely on organizations like us or other specialist companies to provide them with what is known as threat intel in order to better protect themselves. That's how we operate: Ultimately, everyone has to play their part, but from the outset, partnerships are present in everything we do.

Senator Carignan: You don't have a set modus operandi for a sector, with standards for communication or timely information? Maybe so, but I wonder, because we see what is happening with the Foreign Interference Commission. We see that there are wait times; we see that a decision is made to transmit information, not to transmit it or to transmit it within a certain timeframe. How does this work, and how can relevant information be passed on quickly without sitting on a desk because someone thinks it's not necessarily important now, but it might be in the future?

J'essaie de voir comment — ou même si — ces entreprises protègent bien nos infrastructures. Est-ce que ce sont ces entreprises qui aident à protéger nos infrastructures essentielles? Je pense au système d'électricité, au système bancaire canadien, aux transactions bancaires et à toutes les cibles stratégiques des infrastructures civiles qui pourraient être visées. Est-ce que vous les soutenez? Est-ce que vous donnez de l'information à ces entreprises ou à ces organismes, que ce soit Hydro-Québec ou un autre, qui gèrent des infrastructures essentielles ou stratégiques? Est-ce qu'on laisse plutôt les grandes entreprises privées — il y a des entreprises israéliennes et américaines — qui sont spécialisées dans la cybersécurité conseiller nos organismes ou entreprises stratégiques?

M. Khoury : Merci pour la question. Le partenariat est très important pour nous, que ce soit à l'échelle fédérale ou provinciale ou avec les organisations. Nous travaillons avec tout le monde pour tisser des partenariats afin d'échanger de l'information, pas seulement en temps de crise, mais pour maintenir un bon rythme dans l'échange d'information. Que ce soit avec les grandes banques ou avec des organismes comme Hydro-Québec ou d'autres, nous avons des partenariats qui nous permettent justement, quand nous avons quelque chose à partager, de le faire et de promouvoir un échange de connaissances techniques, comme ce que nous constatons et comment nous pouvons les aider à mieux se défendre.

Comme vous l'avez constaté, il y a beaucoup de compagnies commerciales qui se spécialisent dans le domaine de la cybersécurité. Au Centre canadien pour la cybersécurité, nous ne sommes pas en mesure de recommander la compagnie A plutôt que la compagnie B. Nous suggérons aux gens de prendre en considération certains facteurs avant de choisir avec qui ils vont faire affaire. Principalement, les grosses entreprises ont leurs propres équipes de cybersécurité et elles se fient sur des organismes comme nous ou d'autres compagnies spécialisées pour recevoir ce qu'on appelle en anglais du *threat intel*, pour être en mesure de mieux se protéger ensuite. C'est comme cela que nous fonctionnons : ultimement, chacun doit jouer son rôle, mais de prime à bord, le partenariat est présent dans tout ce qu'on fait.

Le sénateur Carignan : Vous n'avez pas de *modus operandi* fixé d'avance pour un secteur, avec des normes de communication ou de rapidité d'information? Peut-être que oui, mais je me pose la question, parce qu'on voit ce qui se passe avec la Commission sur l'ingérence étrangère. On voit qu'il y a des délais; on voit qu'il y a une décision qui est prise de transmettre de l'information, de ne pas la transmettre ou de la transmettre dans un certain délai. Comment est-ce que cela fonctionne, et comment peut-on transmettre rapidement l'information pertinente sans qu'elle reste sur un bureau en pensant que ce n'est pas nécessairement important maintenant, mais que cela pourrait l'être, effectivement?

Mr. Khoury: Our teams monitor everything that happens in the cyberworld 24 hours a day, 7 days a week. We try to react as quickly as possible. If the information is classified, we can declassify it within a few hours and share it with the private sector. On your first point about standards, there are no standards for the private sector at the moment, but Bill C-26, which is currently before Parliament, will establish standards in four main sectors. Working with our counterparts in the provinces and territories, we hope to develop a similar or equivalent system for sectors not covered by Bill C-26.

[*English*]

Senator Yussuff: Thank you, witnesses, for being here. I have two questions. One is following up on what my colleague, Senator Deacon, asked earlier. With regard to the war in Ukraine, what lessons did we learn in the context of the cyber dimensions of war? This is a whole new area that — it seems to me — will dominate this new century: how wars are fought and — more importantly — how information is used. Equally, how does our country respond to this? We're playing an important role on the ground in supporting Ukraine in a multitude of ways to help them with the challenges they face. What have we learned and how does this inform us in going forward with our own challenges and dealing with these sorts of issues?

Mr. Khoury: Thank you for the question. What we've learned is what Russia demonstrated, which is that cyber is yet another tool in the range of capability that a military or nation has at its disposal, and the synchronicity between them can be fairly damaging. It's not just about kinetic power, but if you combine kinetic and cyber, you can achieve extra impact. We're learning a lot from what Russia is doing both when it's working and when it's not working, because there are a lot of things in the context of the conflict that did not go according to plan for the Russian side. This is partly because of the resilience of Ukrainian society, and they've been the subject of cyberattack for many years, so they have built an element of resilience. That's what we're advocating for in Canada: We need to build resilience in society to be able to withstand potential conflict or potential cyberconflict.

The other thing is this concept that we have also talked about: pre-positioning on critical infrastructure. It's not in time of war that the enemy will come after us. Sometimes they can be hiding within our own networks, and, in time of conflict, spring into action. That's why we're also working diligently with critical infrastructure operators to make sure they go hunting on their network for any sign of suspicious activity, because we want to avoid the scenario we picked up last summer on Volt Typhoon,

M. Khoury : Nos équipes veillent 24 heures par jour, 7 jours sur 7, sur tout ce qui se passe dans le monde cyber. Nous tentons de réagir le plus vite possible. S'il s'agit d'information de nature classifiée, en l'espace de quelques heures, nous pouvons la déclassifier pour la partager avec le secteur privé. Pour votre premier point sur les normes, il n'y a pas de normes pour le secteur privé à l'heure actuelle, mais le projet de loi C-26, qui est présentement à l'étude au Parlement, permettra d'établir des normes dans quatre principaux secteurs. En travaillant avec nos homologues des provinces et territoires, nous espérons développer un système semblable ou équivalent pour les secteurs qui ne sont pas couverts par le projet de loi C-26.

[*Traduction*]

Le sénateur Yussuff : Je remercie les témoins d'être ici. J'ai deux questions. Premièrement, j'aimerais revenir à ce qu'a demandé ma collègue la sénatrice Deacon. En ce qui concerne la guerre en Ukraine, qu'avons-nous appris dans le contexte des dimensions cybernétiques de la guerre? Il s'agit d'un tout nouveau domaine qui — me semble-t-il — dominera ce nouveau siècle : la manière de faire la guerre et, de façon plus importante encore, la manière d'utiliser l'information. De façon analogue, quelle est la réaction de notre pays? Nous jouons un rôle important sur le terrain en appuyant l'Ukraine d'une multitude de façons pour l'aider à relever les défis auxquels elle est confrontée. Qu'avons-nous appris et comment ces leçons nous éclairent-elles face à nos propres défis et quand nous sommes aux prises avec ce genre de problèmes?

M. Khoury : Je vous remercie pour votre question. Nous avons appris ce dont la Russie a fait la démonstration, à savoir que les cyberopérations sont un outil de plus dans la gamme de capacités dont dispose une armée ou un pays, et que la synchronisation entre les opérations peut être assez dommageable. Il ne s'agit pas seulement de puissance cinétique; si l'on combine la puissance cinétique et la puissance cybernétique, on peut avoir plus d'impact. Nous tirons de nombreux enseignements de ce que fait la Russie, quand cela fonctionne et quand cela ne fonctionne pas, parce que, dans le contexte du conflit, beaucoup de choses ne se sont pas déroulées comme planifiés du côté russe. C'est en partie à cause de la résilience de la société ukrainienne, qui est la cible de cyberattaques depuis de nombreuses années et qui a gagné en résilience. C'est ce que nous préconisons au Canada : il faut renforcer la résilience au sein de la société pour être en mesure de résister à des conflits ou à des cyberconflits potentiels.

L'autre chose, c'est le concept dont nous avons également parlé : le prépositionnement par rapport aux infrastructures essentielles. Ce n'est pas en temps de guerre que l'ennemi s'en prendra à nous. Parfois, il peut se dissimuler à l'intérieur de nos propres réseaux, et, en temps de conflit, passer à l'action. C'est pourquoi nous travaillons également assidûment avec les exploitants des infrastructures essentielles pour nous assurer qu'ils sont à l'affût de tout signe d'activité suspecte dans leur

which was a People's Republic of China, or PRC, actor hiding on a critical infrastructure network.

Senator Yussuff: Do we have a similar capacity in our response? We're not at war with anybody, but do we have the capacity to target their society and infrastructure in a way similar to what they are doing to us?

Mr. Khoury: Within the CSE authorities, we have the authority to conduct active and defensive cyber operations. There's a whole approval regime on when those authorities are used. Beyond that, we don't comment publicly on what operations have been carried out under those authorities.

Senator Yussuff: In the context of disinformation, this is broadly affecting Canadian society, almost on a regular basis. The government does not tend to move fast in how we respond to disinformation.

How can we work better in our civil society organization, given the scope of this issue and how much is permeating through Canadian society, whether it is from young people, also adults? Every day there is something that is spread that is not true. We're struggling with this in the context of Russia and China, other actors. This is a huge challenge for our country. How do we improve our ability to respond to this and build a better capacity in civil society?

Ms. Denham: Mr. Khoury also mentioned it: We're focused a lot on the discussions of the resilience of the society as a whole. I have spoken about the Rapid Response Mechanism.

There are certain elements that governments are best placed for, i.e. we can learn from our allies, watch internationally what is happening and hear about those tactics and share it with our domestic agencies. We can hear what some of those narratives are for the purposes of making sure that people understand, when there are certain narratives, which ones are based on disinformation and better fill the information landscape, is how I would describe it.

Some people ask for governments to say what is truthful or not. That is not where governments should be. We should be saying these are the tactics that we are seeing. These are the type of narratives we're seeing. Here is the fact-based information about what we're doing or how we're responding. The whole-of-society resilience then comes in when you have different civil

réseau, parce que nous voulons éviter le scénario qui a été mis au jour l'été dernier avec Volt Typhoon, un acteur de la République populaire de Chine qui se dissimulait dans un réseau d'infrastructures essentielles.

Le sénateur Yussuff : Avons-nous des capacités semblables dans notre réaction? Nous ne sommes pas en guerre avec qui que ce soit, mais avons-nous la capacité de prendre pour cible une société et des infrastructures comme notre société et nos infrastructures sont prises pour cible?

M. Khoury : Dans le cadre des pouvoirs du Centre de la sécurité des télécommunications, nous pouvons mener des cyberopérations actives et défensives. Il y a tout un régime d'approbation pour déterminer le moment où ces pouvoirs sont utilisés. Au-delà de cela, nous ne faisons pas de commentaires en public à propos des opérations qui ont été menées en vertu de ces pouvoirs.

Le sénateur Yussuff : Dans le contexte de la désinformation, de larges répercussions se font sentir sur la société canadienne, presque de manière régulière. Le gouvernement n'a pas tendance à réagir rapidement à la désinformation.

Comment pouvons-nous mieux travailler dans l'organisation de la société civile, compte tenu de l'ampleur du problème et du degré auquel il est présent dans la société canadienne, qu'il s'agisse des jeunes ou des adultes? Tous les jours, des informations qui ne sont pas vraies sont répandues. Nous sommes confrontés à ce problème avec la Russie et la Chine, et avec d'autres acteurs. Il s'agit d'un énorme défi pour notre pays. Comment améliorer notre capacité de réaction et renforcer les capacités dans la société civile?

Mme Denham : M. Khoury l'a également mentionné, nous prêtons une grande attention aux discussions sur la résilience de la société dans son ensemble. J'ai parlé du Mécanisme de réponse rapide.

Dans certains cas, ce sont les gouvernements qui sont les mieux placés; par exemple, nous pouvons apprendre au contact de nos alliés, constater ce qui se fait à l'international ainsi qu'entendre parler de certaines tactiques et en faire part aux organismes nationaux du Canada. Nous pouvons nous familiariser avec certains discours pour nous assurer que la population comprend, quand il y a certains discours, lesquels sont de la désinformation, et mieux occuper la scène de l'information, c'est ce que je dirais.

Certains demandent aux gouvernements de dire ce qui est vrai et ce qui ne l'est pas. Ce n'est pas le rôle des gouvernements. Nous devons dire : voici les tactiques que nous observons. Voici le type de discours que nous voyons. Voici les renseignements factuels sur ce que nous faisons ou sur notre réaction. La résilience à l'échelle de la société devient alors réalité quand

society and academic experts investing in their capabilities to understand what this environment looks like.

There are a few Canadian entities that are knowledgeable in this area. You will be hearing from some of them. Continue to invest in those capabilities and capacities. Again, when you talk about calling out certain tactics, it isn't always the government that is best placed; it is media outlets, academics, individuals being more understanding of what they're consuming.

Traditionally, Canada hasn't been a country that has grown up with massive disinformation campaigns. We're not used to it. I speak to high school students as well about being very discerning about when you see something, how do you respond? If your emotions are either really excited or really angry, there's something happening there. We have to get more discerning.

It's making sure we have the capabilities and learning with our international allies, and within our system domestically supporting the academic community and experts who are working in this space so that they can help with the education piece.

Then there's another whole piece of work that the Department of Canadian Heritage does working with media entities and building up that ecosystem. It really is a whole-of-society endeavour.

Senator Yussuff: Thank you.

Senator McNair: This is a question for Mr. Khoury: How does the CSE counter specific disinformation programs targeting Canadians? Do you have the capacity to respond to those disinformation campaigns? From what you said to Senator Yussuff, it appears we do have some limited capacity to retaliate in some fashion through an approval process.

Mr. Khoury: Thank you for the question.

We are not a regulator when it comes to information. We look for signs that nation states use cyber means to influence or to promote disinformation.

In some cases, we do counter the narrative — in the case of the doctored images of the Canadian soldiers, because we had intelligence to prove otherwise — as that was a particular case that went through proper government engagement to say we wanted to release that.

différents experts de la société civile et du monde universitaire investissent dans leurs capacités à comprendre ce qui caractérise cet environnement.

Quelques entités canadiennes ont des compétences dans ce domaine. Vous en entendrez certaines. Continuons à investir dans ces capacités. Encore une fois, quand il est question de dénoncer certaines tactiques, le gouvernement n'est pas toujours le mieux placé; ce sont plutôt les médias, les universitaires, les personnes qui ont une compréhension plus fine de l'information qu'elles consomment.

Traditionnellement, le Canada n'est pas un pays qui a connu des campagnes de désinformation massives. Nous n'y sommes pas habitués. Je parle à des élèves du secondaire et je les encourage à faire preuve de discernement : quand on voit quelque chose, comment y réagit-on? Si l'on a des émotions qui traduisent un grand enthousiasme ou une grande colère, il y a quelque chose de louche. Il faut apprendre à faire preuve d'un plus grand discernement.

Il faut veiller à avoir les capacités et il faut apprendre au contact de nos alliés à l'international, et dans notre système au Canada, il faut appuyer le monde universitaire et les experts qui travaillent sur ces questions pour qu'ils puissent apporter leur pierre à l'édifice dans le domaine de l'éducation.

Par ailleurs, il y a tout un travail mené par le ministère du Patrimoine canadien en collaborant avec les médias et en bâtissant l'écosystème en question. C'est vraiment un effort de l'ensemble de la société.

Le sénateur Yussuff : Je vous remercie.

Le sénateur McNair : Ma question s'adresse à M. Khoury. Comment le Centre de la sécurité des télécommunications contre-t-il les programmes particuliers de désinformation qui ciblent les Canadiens? Avez-vous la capacité de réagir à ces campagnes de désinformation? À en juger par votre réponse au sénateur Yussuff, il semble que nous ayons une capacité limitée de riposter d'une manière ou d'une autre en suivant un processus d'approbation.

M. Khoury : Je vous remercie pour votre question.

Nous ne sommes pas un organisme de réglementation s'agissant de l'information. Nous cherchons des signes que les États-nations utilisent des moyens cybernétiques pour exercer une influence ou promouvoir la désinformation.

Dans certains cas, nous réfutons ce qui est dit — dans le cas des images trafiquées de soldats canadiens, parce que nous avions des renseignements prouvant le contraire. Il s'agissait d'un cas particulier dans lequel le gouvernement a approuvé la publication d'une réaction en suivant la procédure appropriée.

As far as our authorities, these are authorities to carry out cyber operations, not to do disinformation campaigns per se. It's to impose a cost on our adversaries using cyber means. It could be disabling infrastructure, for example, or it could be along those lines, so a pure cyber means.

As far as countering the narrative, I'll look to my colleague, Ms. Denham, to talk about the role of the RRM in calling out misinformation.

Ms. Denham: Sure. To add a few more examples, the RRM also publishes an annual report where we do agree with our G7 colleagues on the tactics we're seeing and which countries are conducting them. We now have two annual reports that are available online for 2021 and 2022.

We have a website that was put up. This is specific to the disinformation that was targeting Ukraine, Russian disinformation, to be clear. It is trying to counter disinformation with facts. An example of that is having experts come and do interviews, sharing what tactics they are seeing; what does that look like, then posting that on the website.

We've done social media campaigns. Before Russia does regional votes or moving toward annexing different territories, we published a playbook. Here are the traditional steps that Russia does every time. They change the curriculum in schools. We've noted the ten steps, with the last one being annexation of territory. It's pushing out the information. It's countering the narratives that we see and filling that narrative space with a counter dialogue. Those are some of the actions that we've taken, in addition to information sharing through the RRM.

[*Translation*]

Senator Dagenais: You said, Mr. Khoury, that the Russians react quickly to your reports and make some adjustments.

The questions this raises in my mind are the following: Are your communications too public, could they be infiltrated, and where do the Russians get their information to make some adjustments?

[*English*]

Senator M. Deacon: Carrying on from my colleague Senator Yussuff on learning, I read that Ukrainian power plants were taken off-line some time ago following Russian cyberattacks before the war and that they are quarantined from the rest of their company's cyber infrastructure. Is that something we practise or

En ce qui concerne nos pouvoirs, il s'agit de pouvoirs permettant de mener des cyberopérations et non des campagnes de désinformation à proprement parler. Il s'agit d'imposer un coût à nos adversaires en utilisant des moyens cybernétiques. Il peut s'agir de paralyser des infrastructures, par exemple, ou d'une intervention du même ordre, purement cybernétique.

En ce qui concerne la lutte contre les discours, je laisserai ma collègue, Mme Denham parler du rôle du Mécanisme de réponse rapide pour dénoncer la mésinformation.

Mme Denham : Pour ajouter quelques exemples, le Mécanisme de réponse rapide publie également un rapport annuel, dans lequel nous présentons la position commune à laquelle nous parvenons avec nos collègues du G7 concernant les tactiques observées et les pays qui les mettent en œuvre. Deux rapports annuels sont actuellement disponibles en ligne, ceux de 2021 et de 2022.

Nous avons un site Web qui a été mis en place. Il concerne en particulier la désinformation qui visait l'Ukraine, la désinformation russe, s'entend. Il cherche à réfuter la désinformation à l'aide de faits. Par exemple, des experts donnent des entrevues, expliquent les tactiques qu'ils observent, la forme qu'elles prennent; c'est ensuite publié sur le site Web.

Nous avons mené des campagnes dans les médias sociaux. Avant la tenue de scrutins régionaux ou avant que la Russie n'intervienne pour annexer différents territoires… Nous avons publié un scénario qui contient les étapes habituelles que la Russie suit chaque fois. Elle modifie les programmes scolaires dans les écoles. Nous avons noté les dix étapes, la dernière étant l'annexion du territoire. Il s'agit de présenter l'information. Il s'agit de réfuter les discours que nous observons et d'occuper l'espace à l'aide d'un contre-discours. Ce sont quelques-unes des mesures que nous avons prises, en plus de la diffusion de renseignements par l'intermédiaire du Mécanisme de réponse rapide.

[*Français*]

Le sénateur Dagenais : Vous avez dit, monsieur Khoury, que les Russes réagissent rapidement à vos signalements et corrigent le tir.

Les questions que cela soulève dans mon esprit sont les suivantes : est-ce que vos communications sont trop publiques, est-ce qu'elles pourraient être infiltrées et où prennent-ils leurs informations pour corriger le tir?

[*Traduction*]

La sénatrice M. Deacon : En complément à la question de mon collègue le sénateur Yussuff à propos de l'apprentissage, j'ai lu que des centrales électriques ukrainiennes ont été mises hors ligne il y a quelque temps à la suite de cyberattaques russes menées avant la guerre et qu'elles sont isolées du reste des

think about here in Canada, or what else are we seeing that Ukraine does to protect its infrastructure that we might consider?

Senator Dasko: Some of the messages you have mentioned, and I've seen in the documents, seem simplistic — for example, there are Nazis in Ukraine, or when Russia says they believe in freedom when, in fact, there's no independent journalism; journalists have left the country, or they're in jail — there are those kinds of messages that are highly unbelievable; they have no credibility.

There must be some messages that are more credible, salient and do have some kind of impact. I wonder if you can tell me what some of those more salient messages might be. I'm assuming the ones I mentioned are utterly ridiculous; at least they are to me.

Ms. Denham: I'll go quickly. Mr. Khoury has the other answers.

It seems like they're highly unbelievable perhaps to yourself, but these are narratives that had a lot of resonance, particularly if you are thinking internationally and international audiences.

Senator Dasko: That Russia believes in freedom of speech?

Ms. Denham: There are still audiences. On Russia's ability to adapt, they watch which messages seem to resonate and get picked up, then they double down.

When they're trying a narrative that says they believe in freedom, if that one doesn't quite hit home, they will come around with other messages. They watch which ones have the biggest resonance.

Some of the ones that have been most persistent, Nazism was out early on; another one has been that nuclear and biological weapons were in Ukraine and that western powers were in control of those; they have denied attacks on civilians. We have seen that over and over. Another one more recently is the questioning of arms shipments that have gone to Ukraine in that that those have been sold on the black market, particularly to Hamas and others.

You've heard pieces of those, probably, but they resonate quite strongly with different audiences internationally, and those would be the messages they amplify.

The Chair: I want to give a very quick answer to the other two questions, please.

cyberinfrastructures de leur entreprise. Est-ce quelque chose que nous pratiquons ici, au Canada, ou que nous considérons? Quelles autres mesures prises par l'Ukraine pour protéger ses infrastructures pourrions-nous envisager?

La sénatrice Dasko : Certains des messages que vous avez mentionnés et que j'ai vus dans les documents semblent simplistes — par exemple, il y a des nazis en Ukraine, ou quand la Russie affirme croire en la liberté, alors que, en réalité, il n'y a pas de journalisme indépendant en Russie; les journalistes ont quitté le pays, ou sont en prison —; il y a ce genre de messages hautement invraisemblables, qui n'ont aucune crédibilité.

Il y a certainement des messages plus crédibles, qui ressortent et qui portent. Je me demande si vous pouvez m'en dire plus sur certains de ces messages qui ressortent plus nettement. Je suppose que ceux que j'ai mentionnés sont complètement ridicules; à tout le moins, ils le sont à mes yeux.

Mme Denham : Je vais dire un mot rapidement. Les autres réponses sont pour M. Khoury.

Ces discours vous semblent peut-être totalement invraisemblables, mais ils ont trouvé un puissant écho, en particulier à l'international et auprès d'auditoires étrangers.

La sénatrice Dasko : Que la Russie croit en la liberté d'expression?

Mme Denham : Certains auditoires le pensent. En ce qui concerne la capacité d'adaptation de la Russie, elle regarde quels messages semblent trouver un écho et circulent, et elle les amplifie.

Quand la Russie met à l'essai un discours qui dit qu'elle croit en la liberté, si ce discours ne trouve pas vraiment d'écho, elle crée d'autres messages. Elle regarde quels messages trouvent le plus d'écho.

Certains des messages les plus persistants, depuis le début, concernent le nazisme; un autre concerne la présence en Ukraine d'armes nucléaires et biologiques sous le contrôle des puissances occidentales; la Russie a nié des attaques menées contre des civils. Nous l'avons constaté à maintes reprises. Un autre message qui a circulé plus récemment sème le doute concernant les armes envoyées à l'Ukraine et suggère qu'elles auraient été vendues sur le marché noir, en particulier au Hamas et à d'autres.

Vous avez probablement entendu certains éléments de ces discours; ils trouvent un puissant écho auprès de différents auditoires à l'international, et ces messages sont ceux que la Russie amplifie.

Le président : Je donnerai une réponse très brève aux deux autres questions.

[*Translation*]

Mr. Khoury: In some cases, these are public messages, but the Russians realize that their technique isn't working. That's how they adapt to understand why it didn't work. So they change the code, and if we catch it, it doesn't work either. It's a game between us and them.

[*English*]

To the question of whether we are practising hygiene, yes. For example, when it comes to a hydroelectric station, we always say to separate your IT from your operational technology, or OT, networks — the OT network being the operational network of the electricity. Make sure that is not accessible from the internet, so we don't run into the same issue that Ukraine ran into in 2015 and 2016.

The Chair: Thank you so much. Thank you, Mr. Khoury, Ms. Denham and Ms. Anderson, for very fulsome answers to lots of tough questions. We thank you for the work that you do. We have been talking about one aspect of that work today. We know it's much broader than this.

On behalf of my colleagues around the table, our colleagues in the Senate and Canadians, we thank you very much for the very important work that you do every day. Thanks again.

For our second panel, we now welcome Anthony Seaboyer, Director, Centre for Security Armed Forces and Society at the Royal Military College of Canada; Svitlana Matviyenko, Associate Professor, Critical Media Analysis at the School of Communication at Simon Fraser University; and Aaron Erlich, Associate Professor, Department of Political Science at McGill University. Thank you for joining us today.

I invite you to provide your opening remarks, which will be followed by questions from our members. We're starting this evening with Ms. Svitlana Matviyenko. Please proceed when you're ready.

Svitlana Matviyenko, Associate Professor, Critical Media Analysis, School of Communication, Simon Fraser University, as an individual: I wanted to be here and thank you for the opportunity to share my testimony with you today.

As confirmed by substantial research and investigations, for several decades, the Russian government has been waging multi-vector disinformation and cyberwarfare, targeting Ukraine and many international communities. The means and dynamics of this war changed significantly after the full-scale invasion of Ukraine. Today, the Russian disinformation techniques have

[*Français*]

M. Khoury : Dans certains cas, ce sont des messages publics, mais les Russes constatent que leur technique ne fonctionne pas. C'est de cette manière qu'ils s'adaptent pour comprendre pourquoi cela n'a pas fonctionné. Donc, ils changent le code et si on l'attrape, cela ne fonctionne pas non plus. C'est un jeu entre eux et nous.

[*Traduction*]

À la question de savoir si nous prenons des mesures d'hygiène, je réponds oui. Par exemple, dans le cas d'une centrale hydroélectrique, nous recommandons toujours de séparer le réseau des technologies de l'information de celui des technologies opérationnelles, le réseau des technologies opérationnelles étant le réseau opérationnel de l'électricité. Il faut s'assurer qu'il n'est pas accessible à partir d'Internet pour éviter d'avoir le problème que l'Ukraine a rencontré en 2015 et en 2016.

Le président : Je vous remercie, monsieur Khoury, madame Denham et madame Anderson, pour vos réponses très complètes à beaucoup de questions difficiles. Nous vous remercions pour le travail que vous accomplissez. Nous parlons d'un aspect de ce travail aujourd'hui. Nous savons qu'il y en a beaucoup d'autres.

Au nom de mes collègues autour de la table, de nos collègues au Sénat et des Canadiens, je vous remercie pour le travail très important que vous effectuez chaque jour.

Pour notre deuxième groupe de témoins, nous accueillons Anthony Seaboyer, directeur du Centre pour la sécurité des forces armées et de la société au Collège militaire royal du Canada; Svitlana Matviyenko, professeure agrégée d'analyse critique des médias à l'École de communication de l'Université Simon Fraser; et Aaron Erlich, professeur agrégé au Département de science politique de l'Université McGill. Je vous remercie de vous joindre à nous aujourd'hui.

Je vous invite à présenter vos déclarations préliminaires, qui seront suivies des questions de nos membres. Madame Svitlana Matviyenko, ce soir, nous commençons par vous. Si vous êtes prête, vous avez la parole.

Svitlana Matviyenko, professeure agrégée, Analyse critique des médias, École de communication, Université Simon Fraser, à titre personnel : Je tenais à être ici et je vous remercie de me donner l'occasion de vous faire part de mon témoignage aujourd'hui.

Comme le confirment d'abondantes recherches et enquêtes, depuis plusieurs décennies, le gouvernement russe pratique la désinformation multivectorielle et mène une cyberguerre contre l'Ukraine et de nombreuses communautés à l'international. Les moyens et la dynamique de cette guerre ont considérablement changé après l'invasion à grande échelle de l'Ukraine.

evolved from opinion manipulation into a system of strategic production of terror.

Disinformation is usually understood as false information that is deliberately intended to mislead public opinion and manipulate public opinion, either in a subtle way — for example, like *Russia Today,* or RT, did in Canada between 2009 and 2022 — by gradually building a relationship of trust with audiences to become a perfect tool that amplified and propagated information in the interests of the Russian government at a chosen moment, or more aggressively by targeting Canadian users directly on social media from fake accounts.

Given the scope, intensity and the nature of information warfare since 2022, the term "disinformation" can no longer appropriately describe its impact on users and the aggressor's intentions in Ukraine. Don't get me wrong: Disinformation remains one of the core techniques of destabilization, but in the context of the all-out war, it is an integral part of more complex warfare events, consisting of both kinetic and cyber operations.

Today, the intention of the Russian aggressor in Ukraine is not to misinform but to terrorize. For example, when the Russian government and media deny the attacks on Ukrainian civilian infrastructure, the genocide in Bucha or the destruction of the Kakhovka Dam, for a Canadian user, those instances might indeed qualify as disinformation, with potential to produce uncertainty or noise when nothing is believable. The impact of such disinformation on Ukrainians is different, as they are subjected to violence several times. In addition to witnessing these horrors of war, they receive and must combat such disinformation in the media or on social media while being targeted by drones and missiles, deprived of sleep and traumatized by their personal and communal losses.

This is terrorism with the clear goals of attrition, intimidation, provocation and outbidding that is employed by the Russian Federation for the purposes of suppressing and subjugating the Ukrainian population to undermine their human dignity and, therefore, their ability to resist the aggressor.

The Russian strategy to terrorize does not stay within the borders of Ukraine. My research also follows the Russian weaponization of nuclear infrastructure, from the occupation of the Chernobyl nuclear power plant, to the occupation of the Zaporizhzhya nuclear power plant, and the use of nuclear threat for inducing terror among international audiences.

A nuclear catastrophe or a nuclear strike does not leave anyone indifferent. Radiation, as we say in media studies, was a mass medium that made the world global and erased the sense of

Aujourd'hui, les techniques de désinformation russes sont passées de la manipulation de l'opinion à un système de production stratégique de terreur.

En général, on entend par désinformation une information fausse qui vise délibérément à induire l'opinion publique en erreur et à manipuler l'opinion publique, soit avec finesse, comme l'a fait par exemple *Russia Today* au Canada entre 2009 et 2022, en bâtissant progressivement une relation de confiance avec le public pour devenir un outil parfait qui a amplifié et propagé de l'information dans l'intérêt du gouvernement russe à un moment choisi, soit plus énergiquement en ciblant les utilisateurs canadiens directement dans les médias sociaux à partir de faux comptes.

Compte tenu de la portée, de l'intensité et de la nature de la guerre de l'information menée depuis 2022, le terme « désinformation » ne peut plus décrire de façon appropriée l'effet produit sur les utilisateurs et les intentions de l'agresseur en Ukraine. Comprenez-moi bien : la désinformation reste l'une des techniques fondamentales de déstabilisation, mais, dans le contexte de la guerre totale, elle fait partie intégrante de faits de guerre plus complexes qui prennent la forme d'opérations tant cinétiques que cybernétiques.

Aujourd'hui, en Ukraine, l'agresseur russe ne cherche pas à mésinformer, mais à terroriser. Ainsi, pour l'usager canadien, le fait que l'État et les médias russes nient les attaques contre des infrastructures civiles ukrainiennes, le génocide à Boutcha ou la destruction du barrage de Kakhovka peut bel et bien constituer de la désinformation qui, en l'absence d'information crédible, est susceptible d'engendrer de l'incertitude ou du bruit. Cette désinformation n'a toutefois pas le même effet sur les Ukrainiens, puisqu'ils sont soumis à de la violence à répétition. En plus d'être témoins des horreurs de la guerre, ils reçoivent en effet de la désinformation dans les médias traditionnels et sur les réseaux sociaux. Ils doivent la combattre tout en étant ciblés par des drones ou des missiles, privés de sommeil et traumatisés par leurs pertes individuelles et communes.

Il s'agit d'un terrorisme ouvertement axé sur l'attrition, l'intimidation, la provocation et l'escalade. La Russie vise ainsi un objectif de suppression et de subjugation des Ukrainiens, de façon à éroder leur dignité humaine et, ce faisant, leur capacité de résistance à son agression.

La stratégie de terreur de la Russie n'est d'ailleurs pas confinée aux frontières de l'Ukraine. Mes recherches suivent aussi le fil de sa militarisation de l'infrastructure nucléaire, depuis l'occupation de la centrale nucléaire de Tchernobyl jusqu'à celle de la centrale nucléaire de Zaporijjia, dans le but de brandir la menace nucléaire pour terroriser la population planétaire.

Une catastrophe nucléaire ou une frappe nucléaire ne laissent personne indifférent. Comme on le dit en études des médias, la radiation est un média de masse qui, avant Internet, a mondialisé

distance before the internet. Its deadly invisible matter is believed to reach anyone, anywhere. Disinformation, accompanied by a nuclear threat, achieves its purposes more effectively.

I was reminded of that just last night by a taxi driver here in Ottawa, who, at first, seemed very upset about what he called "governmental spendings." Then, he immediately jumped to the subject of war in Ukraine: "Why send weapons if Ukraine cannot win the war?" he passionately proclaimed by explaining his argument: "The Russians have the nukes."

I know, and you probably know, that the logic combining these subjects in one sentence is popular, and it is not coincidental. It is induced by terror, specifically, by nuclear terror, as Russia's war against Ukraine unfolds on the nexus of cyber and nuclear.

Thank you. I look forward to your questions.

The Chair: Thank you, Ms. Matviyenko. We will now hear from Anthony Seaboyer. Please proceed when you're ready.

Anthony Seaboyer, Director, Centre for Security Armed Forces and Society, Royal Military College of Canada, as an individual: Thank you for inviting me to speak. My research focuses on the weaponization of information by authoritarian regimes, such as China, Russia, Iran and North Korea. I look at how they target democracies with hybrid, grey-zone warfares and disinformation to undermine rules-based democratic countries like Canada, particularly with AI-enabled applications, which is my focus.

AI-enabled applications are significantly enhancing the effectiveness of information attacks on democracies. Democratic societies urgently need to take substantive measures beyond what we're already doing to defend against attempts to influence and undermine democracies through the weaponization of information.

I would like to bring to your attention how Russia's exploitation of AI-enabled applications is considerably increasing the corrosive impact of Russian disinformation campaigns related to Ukraine and democracies far beyond what Russia was capable of doing before. The key takeaway I'd like to share with you is that Russian disinformation campaigns, now based on these new AI-enabled capabilities, are much more effective, larger in scale, harder to detect by target audiences and those defending against them, they are more sophisticated and much harder to defend against. They are a much greater threat to democracies than Russian disinformation has been before.

la planète et aboli les distances. Sa matière aussi mortelle qu'invisible serait en mesure d'atteindre n'importe qui, n'importe où. Conjuguée à la menace nucléaire, la désinformation atteint ses objectifs d'autant plus efficacement.

C'est ce qui m'est revenu à l'esprit, hier soir, lorsqu'un chauffeur de taxi d'Ottawa qui semblait initialement très contrarié par les « dépenses du gouvernement », comme il disait, a sauté du coq à l'âne pour parler de la guerre en Ukraine. Il a expliqué son raisonnement en demandant avec véhémence: « Si l'Ukraine ne peut pas remporter la guerre, pourquoi envoyer des armes là-bas? Les Russes ont des bombes nucléaires. »

Je sais, et vous aussi sans doute, qu'il est courant de faire la combinaison logique de ces sujets dans la même phrase. Ce n'est pas une coïncidence : c'est l'effet de la terreur, plus précisément de la terreur nucléaire, puisque la guerre que la Russie mène contre l'Ukraine conjugue cybernétique et nucléaire.

Je vous remercie et je répondrai à vos questions avec plaisir.

Le président : Merci, madame Matviyenko. Passons maintenant à Anthony Seaboyer. Quand vous serez prêt, allez-y.

Anthony Seaboyer, directeur, Centre pour la sécurité des forces armées et de la société, Collège militaire royal du Canada, à titre individuel : Je vous remercie de m'avoir invité à intervenir. Mes travaux portent sur l'instrumentalisation de l'information à des fins militaires par les régimes autoritaires comme ceux de la Chine, de la Russie, de l'Iran et de la Corée du Nord. Je m'intéresse aux méthodes qu'ils emploient pour s'en prendre aux démocraties au moyen de la désinformation ainsi que de tactiques hybrides et en zone grise dans le but de déstabiliser des pays de droit démocratiques comme le Canada, en particulier au moyen d'applications fondées sur l'intelligence artificielle. C'est là-dessus que je me concentre.

Ces applications rendent les infoattaques contre les démocraties considérablement plus efficaces. Les sociétés démocratiques doivent de toute urgence redoubler d'efforts pour se prémunir contre les tentatives d'instrumentaliser l'information dans le but de les influencer ou d'éroder la démocratie.

J'attire votre attention sur le fait qu'en employant des applications fondées sur l'intelligence artificielle, la Russie accroît l'effet corrosif de ses campagnes de désinformation en Ukraine et dans les États démocratiques, bien au-delà de ce qui était le cas jusqu'ici. Ce que je veux que vous reteniez, c'est que, vu les dernières percées en matière d'intelligence artificielle, les campagnes de désinformation de la Russie sont nettement plus efficaces qu'auparavant, de plus grande envergure, et plus difficiles à détecter par les auditoires cibles et pour quiconque qui cherche à y résister. Elles sont plus perfectionnées, et il est extrêmement plus difficile de s'en prémunir. La désinformation russe représente une menace plus grave que jamais auparavant pour les démocraties, et de loin.

The difference comes from AI-enabled applications enabling Russian disinformation attacks to be more subtle, plausible and micro-targeted based on information that's analyzed and used to design the attacks. What Russia is doing has not changed. It goes back at least as far as the 1960s in terms of what we call "Russian reflexive control." What is new, though, is the precision and scale at which this can be done when using generative AI applications.

I could share many forms of how that is done, but I'm going to share just a few here, targeting the military in Ukraine, specifically. Russia uses generative AI to falsify political and military orders, undermine morale of citizens and members of the security community, divide allies, discredit military leaders, Russia, indirectly targets military members while directly targeting citizens by legitimizing violent protest, sowing confusion in target audiences, polarizing societies, discrediting political leaders, delegitimizing decision-making processes and political systems, and radicalizing target audiences.

We're all aware of the examples in the U.S. I'd like to focus your attention on the second-largest contributor of military aid to Ukraine, which is Germany. Germany has been targeted by Russia with a campaign containing over 50,000 dedicated accounts that produced over 200,000 disinfirmation-spreading posts a day, trying to sow doubt about supporting Ukraine. The message spread was "support for Ukraine undermines Germany's economic prosperity and could lead to a nuclear war."

Russian messaging was designed to look exactly like actual posts from legitimate news websites, going down to the level of the tone and writing style — this is what generative AI can do which was very difficult to do before and impossible at scale. They were basically indistinguishable except for the content of actual *Der Spiegel* and *Süddeutsche Zeitung* articles, making messaging basically indistinguishable for the reader from actual original news posts.

In this way, Russia is employing AI in a way to create entire alternative information ecosystems. It does this by actively seeking voices of doubt and unease with Germany's support of Ukraine and tries to amplify and enlarges those voices, not just in Germany but also in Canada, the United States and other Western countries.

For the Kremlin, like other authoritarian undemocratic regimes such as China, the sheer existence of democracies — and this is why they're doing this — is perceived as a threat to regime survival. Authoritarian autocratic regimes whose political power is based in repression, violence, censorship and corruption cannot compete with the living conditions of civilian citizens in

La différence vient du fait que les applications fondées sur l'intelligence artificielle permettent à la Russie d'opérer des frappes de désinformation plus subtiles, plus plausibles et microciblées qui sont mises au point à l'issue d'une analyse des faits. La Russie procède ainsi depuis longtemps. Il s'agit de « contrôle réflexif à la russe », une méthode qu'elle applique depuis au moins les années 1960. La nouveauté, c'est la précision et l'ampleur des opérations que les applications fondées sur l'intelligence artificielle rendent possibles.

Je pourrais donner de nombreux exemples de cette technique, mais je m'en tiendrai à quelques-uns qui ciblent en particulier l'armée ukrainienne. La Russie utilise l'intelligence artificielle générative pour falsifier des ordres politiques et militaires, éroder le moral des Ukrainiens et du milieu de la sécurité, semer la discorde entre alliés et discréditer de hauts gradés. Elle cible à la fois des soldats, indirectement, et des citoyens, directement, en légitimant les manifestations violentes de manière à semer la confusion parmi les auditoires cibles, à polariser les sociétés, à discréditer les autorités politiques, à remettre en cause la légitimité des processus décisionnels et des régimes politiques ainsi qu'à radicaliser les auditoires cibles.

Nous sommes tous bien au fait de ce qui s'est passé aux États-Unis, alors j'aimerais attirer votre attention en particulier sur le deuxième pays en importance en matière d'aide militaire à l'Ukraine, c'est-à-dire l'Allemagne. La Russie s'en est prise à l'Allemagne au moyen d'une campagne qui a mobilisé au-delà de 50 000 comptes dédiés. Ces comptes publiaient quotidiennement plus de 200 000 billets de désinformation pour remettre en question l'aide à l'Ukraine en affirmant qu'elle nuisait à la prospérité économique de l'Allemagne et que cela risquait de se solder par une guerre nucléaire.

Les messages russes étaient rédigés de façon à ressembler à de vrais billets de sites d'information légitimes, jusque dans le ton et le style, quelque chose qui était jusqu'ici extrêmement difficile à accomplir et irréalisable à grande échelle, mais que l'intelligence artificielle fait très bien. Au-delà de leur contenu, pour le lecteur, les billets étaient pratiquement impossibles à distinguer de ceux que publient réellement *Der Spiegel* ou le *Süddeutsche Zeitung*.

La Russie se sert ainsi de l'intelligence artificielle de manière à créer des écosystèmes d'information parallèles en amplifiant et en relayant activement l'expression de doutes et de malaises sur le soutien de l'Ukraine par l'Allemagne, non seulement en Allemagne même, mais aussi au Canada, aux États-Unis et ailleurs en Occident.

Pour le Kremlin comme pour tout autre État autoritaire et non démocratique — la Chine, par exemple —, l'existence même de démocraties fait figure de menace à la survie du régime. C'est d'ailleurs pourquoi ils agissent ainsi. Les régimes autocratiques autoritaires dont le pouvoir politique repose sur la répression, la violence, la censure et la corruption ne peuvent pas soutenir la

rules-based democracies. Liberal democracies are clearly superior to strong man dictatorships in terms of living conditions, economic development, political stability and general happiness of the people. This creates a very severe pressure for those systems, and they try to counter this pressure with disinformation.

Russian AI-enabled disinformation campaigns go beyond individual targeted operations focusing on elections, for example. They are in a much wider sense reflexive control operations affecting behavioural change by targeting the world view of citizens. Beyond that, though, they aim foremost at eradicating organic political will formation.

They do this in the following method, which is complex. They achieve cognitive overload by flooding the information space with targeted disinformation campaigns and with misinformation that additionally creates noise and confusion leading to an information overload perceived by members of the target audiences.

At the massive scale which can be generated with AI applications, they create information suffocation. Citizens are then so overwhelmed with information and find it so difficult to find out what is actually happening that they turn away from news sources which lead to information apathy.

Over time, information apathy leads to the "deer in the headlights" effect of information paralysis where target audiences are so overwhelmed that they stop participating in the political process.

This then leads to the final goal of exploitation of information by authoritarian regimes: The feeling of loss of agency of citizens that effectively eradicates civil societies and prevents organic political will formation. AI-enabled applications make achieving the loss of agency of citizens much easier and faster to achieve. Therefore, Russian AI-enabled disinformation campaigns comprise an existential threat to our Canadian democratic society and our way of life. Thank you for your attention.

The Chair: The final witness is Mr. Erlich. Please proceed when you're ready.

[*Translation*]

Aaron Erlich, Associate Professor, Department of Political Science, McGill University, as an individual: Good afternoon to you all.

concurrence face aux conditions de vie des civils dans les démocraties de droit. Les démocraties libérales sont de toute évidence supérieures aux dictatures totalitaires, que ce soit sur le plan des conditions de vie, du développement économique, de la stabilité politique ou du bonheur général de la population. Ces régimes ressentent donc une pression très intense et ils s'efforcent de la contrer au moyen de la désinformation.

Les campagnes russes de désinformation fondées sur l'intelligence artificielle ne se limitent pas au ciblage individuel en contexte électoral, par exemple. Il s'agit d'exercer un contrôle réflexif dans un sens beaucoup plus large, de manière à induire des changements de comportement en recadrant la perception individuelle du monde. Au-delà de cela, néanmoins, elles visent avant tout à éradiquer la formation spontanée d'une volonté politique.

Pour ce faire, les Russes appliquent une méthode complexe dans le but de provoquer une surcharge cognitive au sein des auditoires cibles: ils inondent les espaces d'information dans le cadre de campagnes de désinformation ciblées tout en répandant de la mésinformation de manière à créer du bruit et à générer de la confusion.

Le volume titanesque d'information que les applications fondées sur l'intelligence artificielle arrivent à générer finit par suffoquer les auditoires. Ils en reçoivent tellement et ils ont tellement de mal à distinguer le vrai du faux qu'ils finissent par délaisser les sources journalistiques, avec pour conséquence une apathie informationnelle.

Au fil du temps, l'apathie informationnelle engendre une espèce de blocage mental: les auditoires cibles sont tellement dépassés qu'ils cessent de s'investir dans le processus politique.

C'est ainsi que les régimes autoritaires atteignent leur objectif final: parce que l'information a été exploitée, les gens ont l'impression de ne plus avoir de libre arbitre, ce qui enraie pour ainsi dire les sociétés civiles tout en empêchant la formation spontanée d'une volonté politique. Les applications fondées sur l'intelligence artificielle accélèrent et facilitent grandement la perte du libre arbitre. En conséquence, les campagnes de désinformation russes fondées sur l'intelligence artificielle constituent une menace existentielle pour la société démocratique canadienne et notre mode de vie. Je vous remercie de votre attention.

Le président : M. Erlich est notre dernier témoin. Lorsque vous serez prêt, allez-y.

[*Français*]

Aaron Erlich, professeur agrégé, Département de science politique, Université McGill, à titre personnel : Bon après-midi à tous.

[*English*]

It's a pleasure to be with you today.

I am a quantitative and predominantly behavioural social scientist; that is, I study the human side of the equation. I'm interested in the demographic, political and social factors that are correlated with disinformation. I'm also interested in what can help inoculate citizens in terms of believing disinformation, what the last panellists often referred to as information resilience or resilience.

I have worked consistently running large-scale surveys and laboratory experiments in Ukraine since 2014, and I have been working and travelling in the region since 2003.

I will make six very brief points based on my empirical studies.

First, we really do need to focus on promoting critical thinking skills at home and abroad. We've run studies in Ukraine mirroring extensive studies in the United States. There is good evidence to believe that improving critical thinking skills and reminding individuals to think critically about media reduces belief in disinformation. Importantly, it does not harm trust in stories that are verifiably true. This type of study should be continually studied at home and abroad. As the last panellists noted, the deluge of generative AI-created disinformation, a lot of which will be generated by pro-Kremlin forces, is going to severely test citizens' discernment capacities. We really are ready for what's about to come. We're at the very beginning of what is going to be an amazing ability to generate at mass scale these types of stories.

We can actually learn a lot from Ukraine. Ukraine in studies that we have done does very well at discerning disinformation despite the other things it might be causing, and with the exception of economic stories which Ukrainians on average are able to distinguish true from false stories in our studies. They've also done interesting things some other panellists asked about. There is, for example, dedicated university curriculum on disinformation and information resilience currently in Ukraine.

Two, we need to teach skills to people with connections to Russia and other authoritarian contexts to reach out better to counter Russian and other authoritarian citizens' belief in propaganda. I think we often discount the importance of what citizens in the sending countries actually believe. It's hard for random strangers to do this. Recently a team and I sent a quarter of a million messages to Russians, messages designed by top academic teams, and only one increased engagement with information about Ukraine. On the other hand, in a different project, we ran a pilot study asking Ukrainians about their

[*Traduction*]

Je suis ravi d'être parmi vous aujourd'hui.

Je suis un chercheur en sciences humaines quantitatives et surtout comportementales. J'étudie donc le côté humain de l'équation. Je m'intéresse aux facteurs démographiques, politiques et sociaux de la désinformation ainsi qu'aux moyens d'immuniser les gens contre la désinformation, d'accroître leur résilience, comme l'a dit quelqu'un dans le panel précédent, leur résilience informationnelle.

Depuis 2014, je mène régulièrement des expériences en laboratoire et des enquêtes à grande échelle en Ukraine, un pays que j'étudie et où je me rends depuis 2003.

Voici brièvement les six points à retenir, en fonction de mes recherches empiriques.

Primo, il faut vraiment miser sur le développement de l'esprit critique, au Canada et ailleurs dans le monde. Nous avons reproduit en Ukraine de vastes études qui avaient été réalisées aux États-Unis. Tout semble indiquer que l'amélioration de l'aptitude au raisonnement critique et le fait de rappeler aux gens d'user de sens critique face au contenu médiatique les rendent moins susceptibles de croire la désinformation sans pour autant nuire à la confiance qu'inspire le contenu factuellement vrai. Il faut procéder à ce genre d'études en permanence, ici et à l'étranger. Comme l'ont signalé les intervenants précédents, le déluge de désinformation créée par intelligence artificielle, en grande partie par des forces pro-Kremlin, met durement à l'épreuve la faculté de discernement individuelle. À n'en pas douter, nous sommes prêts pour ce qui s'en vient. La capacité de générer un volume considérable de faux contenu commence tout juste à être exceptionnelle.

Nous avons beaucoup à apprendre de l'Ukraine. Dans les études que nous avons menées, l'Ukraine obtient de très bons résultats relativement à la détection de désinformation, malgré tout ce que celle-ci entraîne. À l'exception des nouvelles économiques, l'Ukrainien moyen arrive à distinguer le vrai du faux. C'est ce que montrent nos études. Il se fait aussi là-bas des choses intéressantes qui se rapportent aux questions d'autres intervenants. Par exemple, il existe en Ukraine un programme universitaire axé strictement sur la désinformation et la résilience informationnelle.

Secundo, il faut inculquer des compétences aux personnes qui ont des liens avec la Russie et d'autres contextes autoritaires de façon à mieux contrer la propagande des États autoritaires comme la Russie sur leur territoire. Je pense qu'on fait souvent abstraction de l'importance que revêt ce que croient les gens qui fournissent de l'information à ceux qui sont sur place. C'est difficile de rétablir les faits quand on n'est qu'un inconnu parmi d'autres. Dernièrement, une équipe et moi avons envoyé un quart de millions de messages à des Russes, des messages rédigés par des équipes d'universitaires chevronnés, mais un seul d'entre eux

communications with friends and family in Russia. There are approximately 11 million Russian citizens with family members in Ukraine. While many believed they couldn't convince their family of anything, some did report success.

Three, we should harness linguistic reorientation. The messaging of language matters. Canada is familiar with these issues. Many in Ukraine are now opting to read in Ukrainian rather than Russia. In studies run before the full-scale invasion, approximately 50% of Ukrainians would answer survey questions in Russian, now it's 10% in many studies. Currently we are running studies about whether reading disinformation in Ukrainian versus Russian reduces belief in disinformation, and some very preliminary results suggest this reduces belief in disinformation.

We also need to help NGOs target hard-to-reach populations and trust the creativity of local actors. Citizens who are most often influenced by disinformation are not on traditional media or social media. Advertising on sports betting websites, for example, is a creative, locally based solution to trying to reach some of these populations. This is an idea from a Ukrainian NGO that understands how to target populations in Ukraine.

Another thing that the senators may be interested in is understanding what media bans do. Impressive research on Ukraine, not my own, shows how banning Russian TV has reduced support for Putin and pro-Russian positions. Ukraine has banned Russian state media. They also banned Vkontakte, which is a Russian competitor to LinkedIn, and this has also limited exposure to harmful and malicious contact, though not without freedom of speech concerns.

Again, as the first panellists note, I think it's important to continue to support research in this area at scale not just on media but also on the social and behavioural sides. Thank you and I look forward to your questions.

The Chair: Thank you very much. We'll now proceed to questions. Briefly, colleagues, we have four minutes for questions and answers. So you know what to do. We're starting with our deputy chair, Senator Dagenais.

a engendré de l'interaction avec l'information sur l'Ukraine. En revanche, pour un autre projet, dans le cadre d'une étude pilote, nous avons interrogé des Ukrainiens à propos de leurs communications avec leurs proches en Russie. Environ 11 millions de citoyens russes ont de la famille en Ukraine. Même si beaucoup de participants n'avaient pas l'impression de pouvoir convaincre leur parenté de quoi que ce soit, certains ont rapporté avoir réussi.

Tertio, il faut miser sur la réorientation linguistique. La langue employée pour communiquer un message fait la différence. Nous en sommes très conscients au Canada. Beaucoup d'Ukrainiens choisissent désormais de lire en ukrainien plutôt qu'en russe. Dans les études menées avant l'invasion proprement dite, environ 50 % des Ukrainiens répondaient aux questions en russe, mais maintenant, c'est souvent 10 %. Nous sommes en train de réaliser des études pour déterminer si les gens croient moins la désinformation lorsqu'ils la lisent en ukrainien plutôt qu'en russe, et les résultats préliminaires laissent présager que c'est le cas.

Il faut par ailleurs aider les ONG à cibler les populations difficiles à joindre et compter sur la créativité des acteurs locaux. Les gens les plus susceptibles à la désinformation ne consultent pas les médias traditionnels et ils n'utilisent pas les réseaux sociaux. Les publicités sur les sites de jeu en ligne, par exemple, représentent un moyen créatif de tenter de les joindre dans leur propre contexte. L'idée est venue d'une ONG ukrainienne dont l'équipe sait comment cibler des segments de population en Ukraine.

Les sénateurs devraient aussi s'intéresser aux effets des interdictions de diffusion ou de publication. Des travaux de recherche impressionnants sur l'Ukraine auxquels je n'ai pas participé ont montré qu'interdire les chaînes de télévision russes a fait perdre du terrain à Poutine et aux discours prorusses. L'Ukraine a interdit les médias d'État russes, mais aussi Vkontakte, un concurrent russe de LinkedIn, ce qui a contribué à limiter l'exposition au contenu préjudiciable et malveillant, quoique non sans porter atteinte à la liberté d'expression.

Comme les intervenants du premier panel, je pense qu'il est nécessaire de continuer à soutenir la recherche à grande échelle dans ce domaine, non seulement en ce qui concerne les médias, mais aussi sous l'angle social et comportemental. Je vous remercie et je serai heureux de répondre à vos questions.

Le président : Merci beaucoup. Nous passons maintenant aux questions. Pour résumer, nous disposons de quatre minutes pour les questions et les réponses, alors vous savez à quoi vous en tenir. Nous commençons avec notre vice-président, le sénateur Dagenais.

[*Translation*]

Senator Dagenais: My question is for Mr. Erlich. When we look at the cyberoperations and disinformation launched by the Russians since the beginning of the war in Ukraine, do we have any examples that would lead us to conclude that the Russians' tactics have really been successful? Or, with a certain amount of hindsight, can we conclude that none of their attacks has had a devastating effect?

[*English*]

Mr. Erlich: Thank you very much for the question. What I can say is that we ran studies before the full-scale invasion where we have a lot of information, for example, you heard about these Nazi stories. Most Ukrainian don't believe these to be true. Where Russia seems to have had more success — and I believe is still probably the area where they can have success is on the question of the economy. Because Ukraine's economy has had so many problems for so long, including we must understand endemic corruption that has plagues Ukraine, the Ukrainian population is actually much more susceptible to stories on economic disinformation. Whether it's devastating or not is hard for me to say specifically, but certainly the area of most concern are questions related to the economy. They are the ones where the disinformation has the most ability to sway Ukrainian public opinion.

[*Translation*]

Senator Dagenais: Ms. Matviyenko, we've taken in a number of Ukrainian refugees since the war began.

Based on your experience in the field, could you tell us whether disinformation may have had a significant effect on the decision-making of part of the civilian population trying to escape the war?

[*English*]

Ms. Matviyenko: Thank you for the question. I don't think so. I think Ukrainians were able to find this information, and there is a general understanding that Canada is a welcoming country. I myself received a number of requests, for example, because I was in Ukraine during the time of the invasion. I spent all of 2021 and 2022 there, so I witnessed the situation before the invasion and how it unfolded during the first year.

I was in communication with many people. People knew that I live in Canada, and I had numerous requests to help. That was amazing to see. So there is a relation of trust, and it continues.

[*Translation*]

Senator Dagenais: I have another question for you, Ms. Matviyenko.

[*Français*]

Le sénateur Dagenais : Ma question s'adresse à M. Erlich. Lorsqu'on regarde les cyberopérations et la désinformation lancées par les Russes depuis le début de la guerre en Ukraine, est-ce qu'on a des exemples permettant de conclure que les tactiques des Russes ont réellement porté leurs fruits? Ou alors, avec un certain recul, peut-on conclure qu'aucune de leurs attaques n'a eu un effet dévastateur?

[*Traduction*]

M. Erlich : Merci beaucoup de la question. Ce que je peux dire, c'est que dans les études menées avant l'invasion à proprement parler, il y a beaucoup d'information. Par exemple, il était question à l'occasion de nazis. La plupart des Ukrainiens ne croient pas à ces histoires-là. Là où la Russie semble avoir eu plus de succès, et c'est peut-être encore le cas aujourd'hui, je pense, c'est en matière d'économie. L'économie de l'Ukraine va tellement mal depuis tellement longtemps — rappelons-nous entre autres que la corruption y est endémique — que les Ukrainiens sont très susceptibles à la désinformation de nature économique. Je suis incapable de dire exactement si son effet peut être qualifié de dévastateur, mais il n'en reste pas moins que le domaine le plus sensible, c'est tout ce qui touche l'économie. C'est là où la désinformation risque le plus d'influencer l'opinion publique en Ukraine.

[*Français*]

Le sénateur Dagenais : Madame Matviyenko, on a accueilli plusieurs réfugiés ukrainiens depuis le début de la guerre.

Avec vos expériences sur le terrain, pourriez-vous nous dire si la désinformation peut avoir eu un effet important sur la prise de décisions d'une partie de la population civile qui tente d'échapper à la guerre?

[*Traduction*]

Mme Matviyenko : Je vous remercie de votre question. Je ne le crois pas. Je pense que les Ukrainiens sont en mesure de trouver l'information nécessaire. Le Canada est généralement perçu comme un pays accueillant. J'étais en Ukraine au moment de l'invasion, alors j'ai moi-même répondu à beaucoup de questions. J'ai passé 2021 et 2002 là-bas, alors j'ai pu constater de moi-même quelle était la situation avant l'invasion et comment les choses ont évolué la première année.

Je communiquais avec beaucoup de gens. Ils savaient que je vis au Canada, alors j'ai reçu de nombreux appels à l'aide. J'ai été renversée. Le lien de confiance reste donc solide.

[*Français*]

Le sénateur Dagenais : J'ai une autre question pour vous, madame Matviyenko.

Could you compare the disinformation operations carried out here in Canada to those in the United States, or to those in Europe or in certain countries that are closer to Russia than we are?

If it's possible, I'd like to know if you see any difference between the messages and objectives of the Russians depending on who they're targeting.

[*English*]

Ms. Matviyenko: I would say so, yes. I probably can't provide you with a more specific example, but as was said in the previous panel, practices of disinformation are themselves a learning practice. This is absolutely true, and we can see how through time, certain disinformation, memes or items appear and disappear, and some of them stay over time entirely.

It's interesting how this Nazi theme has been evolving. In fact, it is much older than several years ago. It began in 2004 during the Yushchenko-Yanukovych presidential campaign. This was the first time Yanukovych hired a Russian political consultant, and the idea to divide the country appeared there. Somehow, they decided to attach this Nazi talk to Yushchenko. After a few years, it disappeared, but then we see how it reappeared suddenly several years ago. These things sometimes have history. It's interesting to trace them. Some of them indeed live a very long time.

[*Translation*]

Senator Dagenais: Thank you very much, Ms. Matviyenko.

[*English*]

Senator Boehm: Thank you to our academic panellists. You all gave very good and interesting presentations.

My question is for Professor Erlich. In the article that you co-authored with Professor Calvin Garner, you addressed the capacity of residents of Ukraine to discern between pro-Kremlin disinformation and true statements. As you mentioned in your remarks, you found that Ukrainians, despite years of sustained exposure to Russian disinformation, are on average able to — I'll use parliamentary language: "distinguish" as opposed to "cull" — distinguish between true stories and pro-Kremlin disinformation claims.

Based on your research — and perhaps your colleagues on the panel might have views on this as well — what sort of practices could we take from that in Canada in terms of countering propaganda of this kind locally? I ask this bearing in mind that any time any government introduces legislation, there's always the question of freedom of expression and the infringement of

Est-ce que vous pourriez comparer les opérations de désinformation menées ici au Canada à celles qui sont faites aux États-Unis, ou encore à celles qui sont faites en Europe ou dans certains pays qui sont plus proches que nous de la Russie?

Si c'est possible, j'aimerais savoir si vous voyez une différence entre les messages et les objectifs des Russes selon ceux à qui ils s'adressent.

[*Traduction*]

Mme Matviyenko : Je dirais que oui. Je ne peux probablement pas vous fournir d'exemple précis, mais comme quelqu'un l'a dit dans le panel précédent, la désinformation, en tant que pratique, évolue constamment. C'est on ne peut plus vrai. On constate au fil du temps qu'il y a des formes de désinformation, des mèmes ou des sujets qui apparaissent et qui disparaissent, alors qu'il y en a d'autres qui s'incrustent.

C'est curieux de constater l'évolution de cette histoire de nazis. Elle ne remonte d'ailleurs pas du tout qu'à plusieurs années. Tout a commencé en 2004, durant la campagne présidentielle Iouchtchenko-Ianoukovitch. C'était la première fois que Ianoukovitch retenait les services d'un conseiller politique russe. C'est à ce moment-là que l'idée de semer la zizanie au pays a vu le jour. Ils ont décidé, on ne sait pas trop pourquoi, d'associer Iouchtchenko et nazisme. Après quelques années, le discours s'est estompé, mais il a refait soudainement surface il y a plusieurs années. Il arrive qu'il y ait une histoire derrière ce genre de discours, et elle est parfois très ancienne, alors c'est intéressant de remonter à la source.

[*Français*]

Le sénateur Dagenais : Merci beaucoup, madame.

[*Traduction*]

Le sénateur Boehm : Je remercie notre panel d'universitaires. Vous avez tous fait d'excellentes présentations, très informatives.

Ma question s'adresse au professeur Erlich. Dans l'article que vous avez coécrit avec le professeur Calvin Garner, vous parlez de la capacité des Ukrainiens à distinguer la désinformation pro-Kremlin des renseignements factuels. Selon votre présentation, vous avez constaté que, malgré des années d'exposition constante à la désinformation russe, l'Ukrainien moyen est en mesure de distinguer les histoires vraies des affirmations qui relèvent de la désinformation pro-Kremlin.

Selon vos travaux — et peut-être que les autres participants du panel auront eux aussi une opinion sur la question —, quelles pratiques le Canada devrait-il adopter pour contrer la propagande sur son territoire? Je ne perds pas de vue le fait que, chaque fois qu'un gouvernement présente une mesure législative, la question de la liberté d'expression et de l'atteinte à nos libertés sur la toile

the actual freedom we would have on the World Wide Web. I'm wondering if you have any thoughts based on that research you've undertaken.

Mr. Erlich: Thank you, senator. It's a great question and one I've struggled with, because the number one thing that has probably made Ukraine so good at it is that they were invaded in 2014. In some ways, that was maybe Putin's biggest mistake. He really gave the Ukrainians an opportunity to learn how to cope with these things.

One important thing that can be done is to instill some kind of urgency in people. I hesitate to use the word, "fear." I don't want to use the word "fear," but we need to instill the idea in people that this is something urgent, and they can't sit back. That's what the Ukrainians did. They could no longer sit back. They felt it was urgent to learn how to deal with this. I'm sure my colleague will have many things to say, but if you talk to colleagues on the ground, they say that nobody believes anything until they've triangulated it. They sound like they've taken something from a textbook: "I've triangulated with three sources and checked with my friend in Kherson and my other friend, and now I believe it." They've gotten that urgency.

Therefore, anything we can do to help people believe that it's actually urgent is the key. Now, if I had the answer to that question, I would probably have a lot more money than I do now.

Mr. Seaboyer: I think there's a lot to learn, not just from Ukraine but particularly from other countries that have been targeted for a long time. Finland is a particular example in terms of their whole-of-government and governance approach, educating children in kindergarten focusing on critical thinking. There is a lot that can be done ethically. My research focuses on how we can ethically counter disinformation and how we can ethically counter message. There's a lot that can be done there.

Learning from Finland, they have, for example, prime time TV shows where they talk about how Russia is targeting them and why and what the exact Russian messaging is. They alert the public to these false messages. There's a lot we can learn in that regard.

I agree with Dr. Erlich's point. In my view, what we're missing in Canada is an understanding of the threat that's there. This is partially because we're not targeted as much, for example, as the United States. However, the infrastructure to be able to target Canada as much as the United States has been set up with the echo chambers. So we need to inform the public and make this more of a topic that people are aware of, and then fund research. We heard a lot about the Rapid Response Mechanism, which is an amazing part of Global Affairs Canada. It's doing a

se pose. Je me demande ce que vous en pensez, à la lumière de vos travaux.

M. Erlich : Merci, monsieur le sénateur. C'est une excellente question, et je me la pose moi-même, car si l'Ukraine obtient d'aussi bons résultats, c'est sans doute principalement à cause de l'invasion de 2014. D'une certaine façon, c'est peut-être la pire erreur de Poutine: il a vraiment donné aux Ukrainiens l'occasion d'apprendre à gérer tout cela.

Une des choses qu'il faut absolument, c'est faire comprendre aux gens qu'il y a urgence. J'hésite à dire qu'il faut leur faire peur. Je ne veux pas employer le mot « peur », mais il n'en reste pas moins que les gens doivent prendre conscience que le temps presse et qu'ils ne doivent pas rester sans rien faire. Les Ukrainiens ont réagi, eux. Ils ne pouvaient plus rester sans rien faire. Ils ont ressenti l'urgence d'apprendre comment gérer tout cela. Je suis certain que mes collègues ici présents en auront beaucoup à dire, mais si vous parliez avec ceux qui se trouvent sur le terrain, ils vous diraient que personne ne croit quoi que ce soit avant d'avoir tout confirmé et reconfirmé. À entendre les Ukrainiens, on croirait qu'ils ont consulté un manuel: « J'ai confirmé l'information auprès de trois sources et j'ai consulté deux copines, dont une à Kherson, alors je sais que c'est vrai. » Ils ont compris l'urgence d'agir.

L'essentiel, c'est par conséquent de faire tout ce qui peut convaincre les gens qu'il y a urgence. Si je savais de quoi il s'agit, cependant, je serais sans doute beaucoup plus riche.

M. Seaboyer : Je pense que nous avons beaucoup à apprendre de l'Ukraine, oui, mais surtout d'autres pays qui sont ciblés depuis longtemps. La Finlande, par exemple, adopte une approche pangouvernementale axée sur la gouvernance en sensibilisant les enfants dès la maternelle à la pensée critique. Il y a beaucoup de choses éthiquement possibles. Mes travaux portent sur la lutte éthique contre la désinformation et sur la contre-communication éthique. Il y a vraiment de quoi faire.

Pour nous inspirer de la Finlande, prenons par exemple les émissions de télévision à heure de grande écoute où l'on parle du fait que la Russie cible les Finlandais. On y explique pourquoi elle le fait et les messages exacts qu'elle transmet. On prévient la population des faussetés qui sont véhiculées. Nous avons beaucoup à apprendre sur ce plan.

Je suis du même avis que M. Erlich. Selon moi, ce qui nous manque, au Canada, c'est une prise de conscience de la menace. C'est en partie dû au fait que nous ne sommes pas aussi ciblés que, par exemple, les États-Unis. Néanmoins, l'infrastructure nécessaire pour cibler le Canada autant que les États-Unis est déjà là, avec les chambres d'écho. Il faut donc informer la population et la conscientiser au problème, puis financer la recherche. Il a beaucoup été question du Mécanisme de réponse rapide, un volet exceptionnel d'Affaires mondiales Canada.

lot of work but is seriously underfunded. If you look at how much staff they have, it's unbelievable what they're putting out. Their reports are really great, but we need far more funding for RRM and for other methods used by the government to try to mitigate disinformation attacks.

Senator Boehm: It's not existential for us. I think that would be a big factor.

Ms. Matviyenko: I completely agree with my colleagues here. I would also add that, of course, fact checking is an incredibly important thing. Indeed, in Ukraine, for the last ten years, people have been learning how to do it almost immediately. This is a skill, and it takes some time, but then you learn it.

However, we are also seeing that, actually, disinformation goes far beyond facts. What we see is an engagement with emotions, fear and even terror — as I was trying to say. These are more complex things, and probably that's where we need a broader discussion, context, education and on-the-ground reporting. What is really missing in Canadian media — in order to understand how things unfold — is reporting. I've been working with media for all this time, and I see there is a huge problem in terms of how it's done.

Senator Oh: Thank you, professors, for being here.

My question for you is this: How can Canada work with its allies and international partners to develop a coordinated response to Russia's disinformation and cyber operations targeting Ukraine? How is our punch back on the cybersecurity to Russia? Are we strong enough?

Mr. Seaboyer: About the last question — whether we are strong enough — absolutely not. Absolutely not. This has to do with many factors. Funding is one factor, but also our rules-based order. We care about transparency and accountability, and we are very careful about unintended side effects. The adversaries are not. Russia and China are not concerned about unintended side effects. They will put out 180 different messages on a topic — Russia, for example, the MH17 that was shot down — and they don't care about what sticks and what doesn't stick and what effects this has on target audiences. We do not do that, cannot do that, don't need to do that and don't want to do that. We have a completely different ethical background and different regulations dealing with that. So that puts us on one level that tilts the playing field significantly to the advantage of the adversary, which they're exploiting deliberately. They know that we can't act in that way, but I argue — based on my research — that we don't need to fight fire with fire. If we fight fire with fire, we become the enemy, and we don't need to fight the enemy then.

L'équipe ne chôme pas, mais elle est gravement sous-financée. Quand on pense au nombre de personnes qui la composent, c'est incroyable qu'elle arrive à en faire autant. Ses rapports sont exceptionnels, mais il faut hausser nettement son financement, ainsi que celui d'autres mécanismes gouvernementaux de lutte contre les infoattaques destinées à désinformer.

Le sénateur Boehm : Dans notre cas, la menace n'est pas existentielle. Je pense que c'est sans doute un facteur majeur.

Mme Matviyenko : Je suis entièrement d'accord avec mes collègues. J'ajouterais que la vérification des faits est évidemment un incontournable. D'ailleurs, en Ukraine, depuis 10 ans, les gens apprennent à le faire presque spontanément. C'est une compétence, et il faut un certain temps, mais elle s'acquiert.

Cela dit, selon ce que l'on constate, la désinformation ne passe pas que par les faits. Elle fait appel aux émotions, à la peur, même à la terreur. C'est ce que j'essayais de dire. Ce sont des éléments plus complexes, et c'est probablement là-dessus qu'il faut engager le débat social, mettre les choses en contexte ainsi que miser sur la sensibilisation et le journalisme de terrain. Ce qu'il manque vraiment dans le paysage médiatique canadien, pour comprendre l'évolution des événements, ce sont des constats sur le terrain. Je travaille depuis longtemps avec les médias et je constate un problème énorme sur ce plan.

Le sénateur Oh : Je vous remercie, madame, messieurs, de votre présence.

Voici ma question: comment le Canada peut-il se concerter avec ses alliés et ses partenaires du monde entier de façon à coordonner la réaction aux campagnes de désinformation et aux cyberopérations de la Russie envers l'Ukraine? Réagissons-nous efficacement aux efforts de la Russie en matière de cybersécurité? Avons-nous les reins assez solides?

M. Seaboyer : Sur cette dernière question, à savoir si nous avons les reins assez solides : absolument pas. Ce n'est absolument pas le cas. Divers facteurs sont en cause. Il y a notamment le financement, mais aussi notre ordre fondé sur des règles. En effet, nous avons la transparence et la reddition de comptes à cœur, et nous cherchons à tout prix à éviter leurs effets indésirables, sauf que ce n'est pas le cas de nos adversaires. La Russie et la Chine ne se soucient pas des effets indésirables. Elles vont diffuser 180 messages différents sur un même sujet — pensons par exemple, dans le cas de la Russie, à l'appareil MH17 qui a été abattu —, peu importe la crédibilité qui leur sera accordée et leurs effets sur les auditoires cibles. Nous ne procédons pas ainsi, nous ne le pouvons pas, nous n'avons pas besoin de le faire et nous ne le voulons pas. Nous avons une éthique complètement différente et des règlements différents à ce sujet, ce qui confère un avantage considérable à l'adversaire, un avantage qu'il exploite délibérément. Il sait que nous ne pouvons pas agir ainsi, mais j'estime d'après mes recherches que nous n'avons pas à combattre le feu par le feu.

I'm working on developing ethical methods of influence operations — ethical AI-enabled methods of influence operations — and this is early stages, but we can, in a transparent and open way with white operations, or white ops, influence target audiences by informing them about the challenges they face in those countries. The difference is the fundamental corruption in Russia, the fundamental corruption in China and the living conditions of the people. If we talk about and make people aware of that, it can be a very effective way of creating a counterbalance and a counter defence against the attacks.

Senator Oh: Any other comments? No?

Senator M. Deacon: I'm going off script a little bit. As I listen, I must say that we learned this first-hand at the 2014 closing ceremony of the Sochi Olympics, and trying to have our young people understand what battles they can and can't have. All the things you're saying today are sober reminders of the continued work in this area. Also, working with young people, one of the most important things you're talking about today, specifically, Mr. Erlich, is that of critical thinking skills. We met with hundreds of teachers last week, and they're just looking for the answers: How do we help our students with disinformation? What do we do? There are plenty of examples of activities they can do, but I couldn't agree with you more as I'm mulling over and listening today about teaching citizens critical thinking skills. I worry, however, that the people who need to hear this most are the people least inclined to listen to any kind of public trust or public message on this. How does the government speak to people who are the least inclined to listen to or to trust the government?

If you can perhaps think about that first, and if anyone else could respond that would be great.

Mr. Erlich: Thank you for the question. It's a great question. I mentioned one thing about meeting people where they are, and I think that is very important, and targeting communities is very important. I can think of an example from Nigeria where I did a little bit of work. They hired a famous rap star to speak out about the issue. I mentioned that some Ukrainian NGOs were placing ads on sports betting and pornography websites, because those are the types of people who aren't going to be in your critical thinking high school classes. When we talk about primary education — yes — we can reach people, but when we're talking about people who are already adults, we have to think about where adults are spending their free time, and there's a lot of good research on that. Then we need to think about what kind of people are actually going to be able to convince those types of

Combattre le feu par le feu, c'est devenir l'ennemi, auquel cas cela ne sert à rien de combattre l'ennemi.

Je cherche à mettre au point des méthodes d'influence éthiques et fondées sur l'intelligence artificielle. Je n'en suis qu'aux débuts, mais c'est possible d'influencer des auditoires cibles ouvertement et en toute transparence, au moyen d'opérations blanches, en les informant des risques en cause dans les pays concernés. La différence, c'est la corruption fondamentale qui règne en Russie, la corruption fondamentale qui règne en Chine et les conditions de vie des gens. En parler et y conscientiser la population peuvent être des moyens très efficaces de rééquilibrer le jeu et de contrer les attaques.

Le sénateur Oh : Y a-t-il d'autres commentaires? Personne?

La sénatrice M. Deacon : Je vais ouvrir une petite parenthèse. J'écoute et j'avoue que nous avons directement pris conscience de cette réalité au cours de la cérémonie de clôture des Jeux olympiques de Sotchi, en 2014, lorsqu'il a fallu faire comprendre aux jeunes quelles batailles peuvent ou non être livrées. Tout ce que vous dites aujourd'hui nous donne à réfléchir en nous rappelant les efforts qui se poursuivent dans ce domaine. De plus, l'un des points les plus importants dont il a été question aujourd'hui, en particulier dans les interventions de M. Erlich, c'est la nécessité de cultiver la pensée critique chez les jeunes. Nous avons rencontré des centaines d'enseignants la semaine dernière, et ils cherchent simplement des réponses. Ils veulent savoir comment aider les élèves à composer avec la désinformation, comment s'y prendre. Il y a des tonnes d'exemples d'activités qu'ils peuvent leur faire faire, mais en vous écoutant parler d'inculquer des compétences en réflexion critique, je me dis que je suis d'accord avec vous sur toute la ligne. Je redoute par contre que les gens qui ont le plus besoin d'être sensibilisés soient les moins disposés à faire confiance de près ou de loin aux messages d'intérêt public sur la question. Comment l'État peut-il arriver à convaincre les gens les moins disposés à l'écouter ou à lui faire confiance?

Je vous invite à y réfléchir le premier, puis si quelqu'un d'autre veut intervenir, ce serait fantastique.

M. Erlich : Merci de la question. C'est une excellente question. J'ai dit qu'il faut approcher les gens sur leur propre terrain. Je pense que c'est nécessaire. Il faut aussi absolument cibler des communautés données. J'ai un exemple en tête. J'ai travaillé un petit peu au Nigeria. Le gouvernement a fait appel à un rappeur célèbre pour parler du sujet. J'ai signalé que des ONG ukrainiennes affichent de la publicité sur des sites de pari sportif ou de pornographie, car les gens qui y vont ne sont pas du genre à assister à des cours d'esprit critique de niveau secondaire. Quand on parle de sensibilisation de base, oui, on peut rejoindre les gens, mais il faut se demander où ils passent leurs temps libres lorsqu'ils ont atteint l'âge adulte. Il y a beaucoup d'excellents travaux de recherche là-dessus. Il faut ensuite se demander quel genre de personnes arriveront à

people. They could be religious leaders for a certain segment of the population. A lot of good work in sub-Saharan Africa using various religious leaders to counter disinformation in church services. Sports figures are often used. It involves a bit of trial and error, but also targeting and thinking about whom the appropriate people are for different Canadian communities. Is it going to be a hockey star? In the Greater Toronto Area, or GTA, is it going to be somebody else such as a popular singer or someone like that? It's not going to be a one-stop-fits-all; it will require community engagement to figure out what kinds of people in the communities are going to work along with some internet-based smart targeting.

Mr. Seaboyer: Research shows — and I can share resources with you — that about 15 to 25% of the population, depending on the country, who want to believe disinformation. So that's their inclination, and it's really hard to reach those people. That's a maximum of 25%. I would not recommend focusing primarily on those. There's at least another 25% who are very susceptible to critical thinking and information education, and it's those — together with another 50% — who can be persuaded.

I mentioned Russian reflexive control. Russian reflexive control is very vulnerable to informing people about what is happening, why it's happening, how it is happening and what it looks like. If you know all those things, you're far less likely when you don't want to believe the disinformation — that's the exception — to fall for that. A lot can be done with education. But the fact that I wanted to bring to your attention is that a lot of this happens with information overload, overstimulating the cognitive capability of people so that they turn away because it's too exhausting and too unpleasant, so they disengage from the political process. That has to be addressed in a different way. In my view that is also about media literacy: How much time do we spend and what sources do we choose? That's a different aspect to focus on.

Senator Cardozo: My first question is for Professor Seaboyer. You mentioned falsifying military orders. I'm wondering to what extent that can happen now or is likely to happen in the next short period. I'm thinking about everything from causing tanks to fire on their own people rather than the other side, or causing fighter jets to go the wrong way or not do what they're required to do at times like this. Are we going to be at that point in the near future?

Mr. Seaboyer: With regard to falsifying orders, the most prominent case was the deep fake that the Russians created, making it look like President Zelenskyy was calling his troops to surrender to Russia. They're falsifying documents, which is something we've seen for a long time. With AI-enabled

convaincre ces adultes. Pour certaines tranches de la population, ce pourrait être des chefs religieux. En Afrique subsaharienne, lorsqu'on fait appel à eux pour contrer la désinformation au cours des services religieux, les résultats sont très positifs. Il n'est pas rare qu'on fasse appel à des personnalités sportives. On procède par essais et erreurs, mais aussi en ciblant des auditoires et en se demandant qui serait le mieux à même de convaincre différents groupes au Canada. Est-ce que ce serait une étoile du hockey? Dans le cas de la région du Grand Toronto, est-ce que ce serait plutôt une chanteuse populaire, par exemple? Il n'y a pas de solution mur à mur. Il faut à la fois apprendre à connaître les communautés pour déterminer qui sont les personnes susceptibles de les convaincre et procéder par ciblage judicieux sur Internet.

M. Seaboyer : La recherche montre — et je pourrai vous fournir des ressources — qu'entre 15 et 25 % de la population, dépendamment du pays, veulent croire à la désinformation. Ces gens y sont disposés et ils sont les plus difficiles à joindre. C'est au plus 25 % de la population. Je ne recommanderais pas de se concentrer principalement sur eux. Il y en a encore 25 % au moins qui sont très susceptibles à la pensée critique et à la sensibilisation. Ce sont ces personnes-là, avec les 50 % restantes, qui peuvent être persuadées.

J'ai évoqué le contrôle réflexif à la russe. Le contrôle réflexif à la russe est très vulnérable à la sensibilisation des gens par rapport à ce qui se passe, au pourquoi et au comment, ainsi qu'à la façon de reconnaître la désinformation. Quand on sait tout cela et qu'on ne veut pas croire à la désinformation, on risque beaucoup moins de s'y faire prendre. C'est l'exception. La sensibilisation est très efficace. Néanmoins, ce que je tenais à vous faire remarquer, c'est que tout cela survient dans un contexte de surcharge informationnelle. La capacité cognitive est surstimulée. La démarche devient trop épuisante et trop désagréable, alors les gens se désintéressent du processus politique. Il faut alors procéder autrement. Selon moi, c'est aussi une question de médiatique: sur quelles sources se base-t-on et combien de temps consacre-t-on à tirer les choses au clair? Il faut aussi se concentrer là-dessus.

Le sénateur Cardozo : Ma première question s'adresse au professeur Seaboyer. Vous avez évoqué la falsification d'ordres militaires. Je me demande quelle est la probabilité que cela se produise en ce moment ou dans un avenir proche, qu'il s'agisse par exemple de faire tirer des chars d'assaut sur leurs propres troupes plutôt que sur l'ennemi, de déployer des chasseurs à réaction dans la mauvaise direction ou d'éviter qu'ils ne fassent ce qu'ils sont censés faire dans tel ou tel contexte. Sommes-nous sur le point d'en arriver là?

M. Seaboyer : Pour ce qui est de la falsification d'ordres, le cas le plus connu est celui d'un hypertrucage créé par les Russes pour donner l'impression que le président Zelensky appelait ses troupes à se rendre à la Russie. On falsifie des documents. Cela n'a rien de nouveau, mais avec l'intelligence artificielle, c'est

capabilities, it's much easier to do this and much more difficult to distinguish from actual or legitimate documents. What you are referring to are hacking operations. In that domain, which is not my field of expertise — I focus on disinformation — the short answer is that the more connected technology is becoming, the more we're having autonomous systems steered from far distances, the more drone swarms, for example, are hackable and potentially their GPS systems can be blocked, their targeting can be blocked or changed. The risks of that are exponentially increasing with further reliance on artificial intelligence, digitization and automated systems.

Senator Cardozo: Professor Matviyenko, you mentioned that in Ukraine people have learned to do fact-checking. That's amazing. What can we learn from that, because I don't think we do that. How do we train young people to fact-check when they just want to see a quick slogan on Instagram and move on with the rest of their day?

Ms. Matviyenko: That is very true. There is a particular way of using technology that very much imposed, popularized, et cetera. This is a very close attachment. Of course, as a teacher, I teach my students what we call media literacy and practice, which is precisely the techniques of detachment. We discuss how media messages are constructed and that there is someone's intention behind the messages.

I think that today we kind of do it almost a little bit less than when we started. There was a time — I would say — maybe 10 years ago, with the popularization of apps, iPhone, et cetera, when there was some kind of fear that this new intimacy with technology would suddenly change us. Then it became normalized. There were definitely more courses, attention and critique. But now, in a certain way, we kind of absorbed it, and we don't have enough conversation about it. We think that it's already understood, but it's not. This intimacy grew and became closer, and that's why every message that is received gives you a sense that it's to you, made for you and it almost encourages a relation of trust. That's definitely the culture of communities who are comfortable. So when there's a threat, this pattern is broken. I am not saying that we need to amplify the threat, but we need to speak more about the seriousness of the situation because the world does go beyond its borders. We're seeing so many events, recently, with infiltration of Russian agents here and there. There are attacks on critical infrastructure everywhere.

So things are happening, and the war is actually very close. We need a very sensible, rational conversation about this, without amplifying fear, as to how using media literacy is important for finding your position and place within this particular situation.

beaucoup plus facile à faire et beaucoup plus difficile à distinguer de documents réels ou légitimes. Vous parlez plutôt d'opérations de piratage. Ce n'est pas mon domaine d'expertise — moi, c'est la désinformation —, mais dans ce cas-là, la réponse simple, c'est que plus l'évolution technologique va dans le sens des produits connectés, plus les systèmes autonomes sont pilotés de loin et plus les essaims de drones, par exemple, peuvent être piratés dans le but de bloquer leur GPS ou d'empêcher la désignation d'objectif, voire de la changer. Plus on compte sur l'intelligence artificielle, le numérique et l'automatisation, plus les risques grandissent, et c'est exponentiel.

Le sénateur Cardozo : Professeure Matviyenko, vous avez dit qu'en Ukraine, les gens ont appris à vérifier les faits. C'est formidable. Je n'ai pas l'impression que c'est le cas ici, alors quelles leçons peut-on tirer de leur expérience? Comment peut-on donner l'habitude aux jeunes de vérifier les faits alors que tout ce qu'ils veulent, c'est lire un bref slogan sur Instagram avant de passer à autre chose?

Mme Matviyenko : C'est très vrai. Il y a une façon particulière d'utiliser la technologie qui s'est tout à fait imposée, popularisée, etc. On y est fortement attaché. Évidemment, en tant que pédagogue, j'enseigne aux étudiants ce qu'on appelle la médiatique ainsi que les techniques des médias afin justement de prendre du recul. Nous discutons de la construction des messages diffusés dans les médias et de l'intention qui se cache derrière.

Je pense qu'aujourd'hui, on le fait presque moins, un petit peu, qu'à mes débuts. À une époque, je dirais il y a une dizaine d'années, à l'avènement des applications, de l'iPhone, etc., il y avait une certaine crainte que notre intimité nouvelle avec la technologie nous transforme soudainement. Ensuite, cela s'est normalisé. Il y avait manifestement plus de cours qu'aujourd'hui. La question suscitait davantage d'attention et de critiques. Aujourd'hui, par contre, cette intimité semble pour ainsi dire aller de soi. C'est quelque chose dont on ne parle pas assez. On pense avoir déjà tout compris, mais ce n'est pas le cas. Parce que l'intimité s'est accrue, qu'elle s'est resserrée, nous avons l'impression que tous les messages s'adressent à nous, qu'ils ont été préparés à notre attention. Ils appellent quasiment à une relation de confiance. C'est ainsi que les choses se présentent dans les sociétés où les gens vivent paisiblement. Toute menace fait alors l'effet d'un électrochoc. Je ne dis pas d'amplifier la menace, mais il faut insister davantage sur la gravité de la situation, car ce qui se passe dans le monde ne s'arrête pas aux frontières. Tellement de choses se déroulent depuis quelque temps. Pensons à l'infiltration d'agents russes ici et ailleurs. Un peu partout, on s'en prend aux infrastructures critiques.

Il y a des choses qui se passent. La guerre nous guette de très près. Il faut discuter de tout cela de manière rationnelle, en gardant la tête froide, sans amplifier la peur. La médiatique, c'est essentiel pour arriver à discerner ce qu'une situation particulière implique pour soi.

Senator Cardozo: Thank you.

Senator Yussuff: Thank you witnesses for being here.

Dr. Erlich, I'll start with you. You used very precise language, which I don't hear very often, when you talk to a parliamentary group. You said, "critical thinking." Given what you've said, that's a daunting stance in the political reality of our country — to teach people critical thinking — but I think if we do want to embark on this, it would be not to learn from the Finns with regard to what they're doing in early high school and university level, because the technology that is available today for us to access information has proliferated, so we're not going to change it. I don't think we have learned the hard way how we can use that technology in a different way.

I thought maybe I would hear your comments, given your analytical research as well as your ongoing research in understanding how we can equip ourselves to respond better.

Mr. Erlich: Thank you for the question. I think Professor Seaboyer will have quite a bit to say about that as well.

It's not just Finland; many of the countries across Eastern Europe have instituted various programs at the primary and university levels, and now have specific ministries or sub-ministries that deal with this issue.

Far be it for me to suggest what government officials should do, necessarily, but it might be a very useful thing to have a study tour of those programs and see what the variety of solutions are. Finland is a very particular example, so what works there might not here, or something from Finland might work, but I wouldn't necessarily say that we can just take one thing off the shelf. Looking at the variety of examples out there and then choosing the ones that best fit in the Canadian context would be an ideal way forward.

I'm sure my colleagues might have something else to add.

Senator Yussuff: Given that cyber warfare is a normal reality of countries that want to disrupt and, more importantly, cause harm, do you think we're equipped as a society to appreciate what we have to do? Equally, on the other side, how well are we learning from Ukraine and other countries that are going through conflicts with other countries, such as in the Middle East and other places?

This is not something that is going to go away any time soon; it seems like it will be the norm. That presents a huge challenge for how democratic societies respond to these challenges. People are becoming less and less trustful of their government to tell them things so basic and fundamental — how society can cope with these issues.

Le sénateur Cardozo : Merci.

Le sénateur Yussuff : Je remercie les témoins d'être parmi nous.

Je commence par vous, monsieur Erlich. Vous avez choisi vos mots avec beaucoup de précision, ce qui est plutôt rare pour quelqu'un qui s'adresse à un groupe parlementaire. Vous avez employé les mots « pensée critique ». Si je me base sur ce que vous avez dit, la réalité politique de notre pays n'a rien de rassurant. Il faut inculquer la pensée critique aux gens. Il me semble néanmoins que si nous nous lancions, ce ne serait pas dans le but de tirer des leçons de ce que les Finlandais font au début du secondaire et à l'université, puisque la technologie qui nous permet actuellement de nous informer a déjà proliféré, alors nous n'y changerons rien. Je ne pense pas que nous ayons appris à la dure comment repenser notre utilisation de la technologie.

Étant donné vos travaux d'analyse ainsi que les recherches que vous menez actuellement afin de comprendre ce qu'il nous faut pour mieux réagir, j'aimerais donc savoir ce que vous pensez.

M. Erlich : Merci de la question. J'ai l'impression que le professeur Seaboyer en aura beaucoup à dire lui aussi.

Il n'y a pas que la Finlande. Beaucoup de pays d'Europe de l'Est ont institué des programmes primaires et universitaires. Ils ont même des ministères ou des sous-ministères qui s'occupent expressément de la question.

Loin de moi l'idée de dire aux fonctionnaires ce qu'ils devraient faire, nécessairement, mais ce serait sans doute très utile d'effectuer une tournée pour étudier les programmes et les diverses solutions qui existent. La Finlande est un exemple très particulier, alors ce qui fonctionne là-bas pourrait ne pas fonctionner ou, dans le cas contraire, on ne pourrait pas nécessairement se contenter de reproduire la formule telle quelle. L'idéal, ce serait d'examiner la multitude d'exemples qui existent, de façon à choisir ceux qui conviennent le mieux au contexte canadien.

Mes collègues auront sans doute quelque chose à ajouter.

Le sénateur Yussuff : Étant donné que la guerre informatique est une réalité banale dans les pays désireux de causer des perturbations, mais surtout de nuire, pensez-vous que notre société dispose des outils nécessaires pour déterminer ce qu'il faut faire? Par ailleurs, à quel point tirons-nous des enseignements de ce qui se passe en Ukraine et dans les pays qui sont en conflit avec d'autres, notamment au Proche-Orient?

Ces conflits ne se régleront pas de sitôt. Ils semblent plutôt vouloir se normaliser, ce qui représente un problème de taille pour les États démocratiques qui entendent y réagir. Les gens font de moins en moins confiance aux gouvernements pour obtenir de l'information on ne peut plus fondamentale. Comment notre société peut-elle composer avec la situation?

Mr. Seaboyer: There are two challenges, one on the side of citizens and one on the side of the government. With the military apparatus, there's the thinking that if it doesn't explode, it's not dangerous. I would argue that cellphones can be more dangerous than aircraft carriers. There needs to be an understanding of impacts and effects of non-kinetic warfare, which is, for example, using information as a weapon, and how it works. We're still learning this, because every few months, there are completely new ways of exploiting information.

On the citizen side, the problem is that we're caught with what is convenient and easy for us. More and more things become faster and easier by using our phone to do them. We don't understand the mechanisms of how that psychologically affects us and our brains. Our phones are, basically, slot machines designed to trigger emotions in ways so that we keep using them.

So to create an understanding of the psychological and biological factors affected by the effective design of these devices — more understanding in that regard is going to definitely help.

Senator Dasko: Thank you to our witnesses for being here. I was asking a question in the last session about salient messages, and I want to continue along that line of thought with Professor Seaboyer.

Messages, to be salient, there's the message side and then messages have to be targeted toward audiences. You mentioned that specifically at the beginning of your comments. You were talking about Russia. I'd like you to elaborate on who is being micro-targeted. Who are the audiences? You can comment on the messages, too, but specifically, who are the audiences that are being targeted from what you've said? So just please elaborate on that.

Mr. Seaboyer: Russia targets individual targeted audiences very specifically in different countries. So if the target, for example, supports the Ukrainian military in Poland, they're going to do with this with different narratives designed to tie into historical experiences, humour and culture. AI enables them to do that much more effectively, because they can scrape the landscape and the target audiences for their preferences — when they're online, how they're online and what they engage with — in much more effective ways. That's the first part.

The second one, which refers to your question to the prior panel, relates to why it is that messages that seem totally ineffective to us can be extremely effective. Messaging can have at least two different goals. One is a direct information goal to achieve direct behavioural change. For example, vote for a politician or not. That's just one side of it.

M. Seaboyer : Il y a deux problèmes, l'un du côté des particuliers et l'autre du gouvernement. Dans le milieu militaire, on se dit que si quelque chose n'explose pas, ce n'est pas dangereux. Or, je dirais qu'un téléphone cellulaire peut s'avérer plus dangereux qu'un porte-avions. Il faut être au fait des conséquences et des effets de la guerre non cinétique, c'est-à-dire, par exemple, l'instrumentalisation de l'information, la façon d'en faire une arme. Notre apprentissage se poursuit, puisque les façons d'exploiter l'information se renouvellent continuellement, au fil des mois.

Pour ce qui est des particuliers, ils sont pris au piège du confort et de la facilité. De plus en plus de choses se font plus rapidement et plus commodément avec un téléphone, sauf que nous ignorons les effets psychologiques de cette réalité, sur nous et sur notre cerveau. Un téléphone, c'est un peu comme une machine à sous conçue pour provoquer des émotions afin de nous inciter à continuer à l'utiliser.

On a de toute évidence intérêt à mieux comprendre les facteurs psychologiques et biologiques que fait intervenir la conception des appareils.

La sénatrice Dasko : Je remercie les témoins de leur présence. J'ai posé une question au dernier panel sur les messages qui ressortent et je veux poursuivre sur la même lancée avec le professeur Seaboyer.

Pour qu'un message ressorte, il doit d'abord communiquer quelque chose, mais aussi cibler un auditoire donné. Vous en avez vous-même parlé au début de votre intervention. Il était question de la Russie. J'aimerais que vous m'en disiez davantage sur le microciblage. Quels auditoires vise-t-on? Vous pouvez parler des messages aussi, mais ce qui m'intéresse, en particulier, ce sont les auditoires en cause dans ce que vous avez dit. Je vous prie de m'éclairer davantage.

M. Seaboyer : La Russie cible individuellement ses auditoires dans différents pays, de façon très précise. Prenons par exemple une cible polonaise qui est favorable à l'armée ukrainienne: on recourra à divers scénarios en faisant appel à des réalités historiques, à l'humour ou à la culture. L'intelligence artificielle permet de le faire avec beaucoup plus d'efficacité, puisqu'on peut moissonner les espaces numériques pour cerner avec précision les préférences des auditoires cibles : à quel moment vont-ils sur Internet, par quel moyen le font-ils et avec quel contenu interagissent-ils? C'est le premier élément.

Le deuxième, et il nous ramène à la question que vous avez posée au panel précédent, c'est qu'il faut comprendre pourquoi des messages qui nous apparaissent tout à fait anodins s'avèrent en fait d'une efficacité redoutable. Un message peut avoir au moins deux objectifs distincts. Le premier, c'est la communication directe d'information dans le but de modifier

A whole different side is spreading so much information that target audiences get overwhelmed and feel that they can't trust information. They feel like they can't find out what's actually going on. Psychologically, we're then set up to believe the largest or loudest voice. That's deliberately created, because the governments of authoritarian regimes have the loudest voice. If people are feeling that they cannot discern the actual truth, they distrust other authorities and will listen to the loudest voice that comes in there.

Micro-targeting is based on very explicit data, individually targeting — it can be individuals, groups, politicians or citizens, depending on what the campaign is interested in achieving — based on very specific data. When are they online? At what time are they most vulnerable to fall for disinformation? That can all be identified with data. Then it is messaging them, going down to the details such as the colour or tone of the messages, or the potential humour they're referring to — all targeted based on knowledge of the individual they're targeting.

With AI-enabled capabilities, there's just so much more data to scrape and use to have much more targeted information attacks.

Senator Dasko: If we were focused on Canada and Russia's efforts in Canada, which are not nearly as great as Russian efforts in many other countries, but which kinds of audiences would they be targeting in Canada with what kinds of messages? Do you have any sense of what that would be?

Mr. Seaboyer: Absolutely.

Senator Dasko: Or others on the panel.

Mr. Seaboyer: Right now, they're targeting support for weapons systems and financial support for Ukraine. They're trying to create the impression that this is leading to a war and that this is basically participation of Canada in a war. They're trying to target civilians. They try to target, for example, people who already have similar beliefs, to an extent, who are more likely to fall for those narratives, but they also target broader audiences and politicians directly and indirectly.

The main goal is to eradicate or stop support for Ukrainian military aid, to change the impression of both Russia and Putin, and undermine democracy in Canada and give the impression

directement le comportement. Un exemple : votez ou ne votez pas pour tel ou tel candidat. Ce n'est cependant qu'un seul aspect du message.

L'autre objectif, et il est complètement différent, c'est de répandre tellement d'information et d'en inonder les auditoires cibles au point de leur faire perdre confiance en elle en leur donnant l'impression qu'il leur est impossible de déterminer ce qu'il se passe vraiment. Du point de vue psychologique, dans une telle situation, l'humain est fait pour croire ce qu'il entend le plus souvent ou la voix la plus forte. On agit donc ainsi de façon délibérée. Après tout, les gouvernements des régimes autoritaires sont ceux dont la voix porte le plus. Lorsque les gens ont l'impression d'être incapables de distinguer le vrai du faux, ils prêtent l'oreille à la voix la plus forte tout en perdant confiance dans les autres autorités.

Le microciblage repose sur des données très explicites et très précises qui visent des auditoires très restreints. Selon l'objectif de la campagne, il peut s'agir de personnes, de groupes, de politiciens ou de citoyens. Quand vont-ils sur Internet? À quelle heure sont-ils le plus vulnérables à la désinformation? Ce sont des choses que les données permettent de déterminer. Le message est ensuite préparé dans les moindres détails, jusqu'à sa couleur, au ton employé ou au recours éventuel à l'humour. On se fonde sur ce que l'on connaît de l'auditoire individuel qui est ciblé.

L'intelligence artificielle permet simplement de moissonner et d'utiliser une quantité de données autrement plus considérable qu'auparavant et de cibler les infoattaques avec beaucoup plus de précision que par le passé.

La sénatrice Dasko : Concentrons-nous sur le Canada et les tentatives de la Russie au Canada, qui ne sont pas aussi intenses que celles qu'elle fait dans bien d'autres pays. Quels types d'auditoires les Russes cibleraient-ils au Canada, et avec quels genres de messages? En avez-vous une idée?

M. Seaboyer : Bien sûr.

La sénatrice Dasko : La question s'adresse aussi aux autres intervenants.

M. Seaboyer : En ce moment, les Russes ciblent le soutien aux systèmes d'armement et l'aide financière à l'Ukraine. Ils cherchent à donner l'impression qu'une guerre se prépare et que le Canada est pour ainsi dire impliqué dans une guerre. Ils tentent de cibler les civils, par exemple des personnes qui croient déjà ce genre de choses, dans une certaine mesure, et qui sont donc plus susceptibles de se laisser convaincre, mais aussi des auditoires plus larges et des politiciens, directement et indirectement.

Leur principal objectif, c'est de faire en sorte que les gens cessent d'être favorables l'aide militaire à l'Ukraine, de changer leur perception à la fois de la Russie et de Poutine, ainsi que de

that our system is unjust and unfair — that elections are manipulated, for example.

Senator Dasko: That's a different kind of message than the Ukraine message. If you're trying to focus on eroding support for Ukraine, that's a little different from what you said at the end. That's a different topic — undermining support for democracy.

Mr. Seaboyer: Absolutely. There are ongoing messages, for example, toward NATO being aggressive and NATO threatening Russia. Those are messages we've been seeing for many years already, so these are ongoing messages they're spreading. There are newer messages directed specifically toward Ukraine.

Senator Dasko: Are these low-information people in Canada? Is that who they're going after?

Mr. Seaboyer: It depends upon the individual campaign we're looking at, but it's much wider.

They go first for people who are more on the fringes of the political spectrum. They largely do not target people in the middle where it's more complicated to radicalize them. They try to radicalize people who have belief systems that are more susceptible to the narratives.

[*Translation*]

Senator Carignan: I'm trying to see how we can get out of this. We don't want to fight fire with fire, we don't want to spread disinformation on the other side or counter-propaganda. If the state starts to spread propaganda or provide information, people will start to distrust information coming from the state.

If we use information that comes from verified independent media sources…. People are also suspicious of the media, the state-funded media, the corporate-funded media.

With all this, we're trying to educate people, give them training and teach them to be critical of information, but sometimes, if we're critical, we start to doubt all information.

When I was reading my notes in preparation for today's meeting, I read some articles about how Europe was countering disinformation; there was a list of about 20 dos and don'ts.

miner la démocratie au Canada en donnant l'impression que notre système est injuste et inéquitable, par exemple parce que les élections sont manipulées.

La sénatrice Dasko : Ce n'est pas le même genre de message qu'en Ukraine. S'efforcer avant tout de miner le soutien envers l'Ukraine, ce n'est pas tout à fait la même chose que ce que vous avez dit en dernier. C'est un autre sujet, le fait de miner le soutien pour la démocratie.

M. Seaboyer : Vous avez parfaitement raison. Il y a des messages continus, par exemple sur le fait que l'OTAN se montre agressive ou qu'elle menace la Russie, des messages qui circulent depuis bien des années déjà. Les Russes les répandent en continu. Il y a aussi d'autres messages, plus récents, qui se rapportent expressément à l'Ukraine.

La sénatrice Dasko : Est-il question des personnes mal informées au Canada? Est-ce que ce sont elles que les Russes ciblent?

M. Seaboyer : Tout dépend de la campagne dont on parle, mais c'est beaucoup plus large.

Tout d'abord, ils ciblent les personnes qui se trouvent aux extrêmes du spectre politique. Dans l'ensemble, ils ne s'intéressent pas à celles qui sont au centre parce qu'elles sont plus difficiles à radicaliser. Ils cherchent à radicaliser les gens qui, à cause de leur système de croyances, sont plus réceptifs.

[*Français*]

Le sénateur Carignan : J'essaie de voir comment on peut s'en sortir. On ne veut pas combattre le feu par le feu, on ne veut pas faire de la désinformation de l'autre côté ou de la contre-propagande. Si l'État commence à faire de la propagande ou à donner de l'information, les gens vont commencer à se méfier de l'information provenant de l'État.

Si on utilise l'information qui vient de sources indépendantes vérifiées et médiatiques... Les gens se méfient aussi des médias, les médias financés par l'État, les médias financés par des compagnies.

Avec tout cela, on essaie d'instruire les gens, de leur donner une formation et de les éduquer à être critiques par rapport à l'information, mais parfois, si on est critique, on se met à douter de toute information.

En lisant mes notes pour me préparer à la réunion d'aujourd'hui, j'ai lu certains articles sur la façon dont l'Europe contrait la désinformation; il y avait une liste d'environ 20 choses à faire ou à ne pas faire.

I wonder how we tackle this problem. In other words, how do we inform our people without sowing doubt in their minds? How can we stop them from believing that everything can be distorted, as this belief can cause them to close in on themselves?

Mr. Seaboyer: That's a good question.

[*English*]

I'm working on research trying to develop ethical influence operations and ethical AI-based influence operations.

What I'm suggesting is complete transparent white operations in the sense that we declare what we're doing, how we're doing it and why we're doing it, fully attributable, but that we exploit vulnerabilities in the information spaces of those adversaries of authoritarian regimes.

A key vulnerability is, for example, the corruption of top leadership. If you identify what China and Russia censor most in the debates of dissidents, you can see that's what they do not want to have talked about.

What I am suggesting is we, of course, do not create disinformation. We do not lie. We don't need to do that.

[*Translation*]

There's absolutely no need for this.

[*English*]

All we need to do is talk about the reality of living conditions, contrast that to our living conditions. In Canada, you can post — within the law — whatever you want online. You never go to jail. In China, you go to jail for 20 years if you post content critical of the government. Those things we can talk about. We can make sure that communities who are interested in this are better informed of this, and that creates an effect.

I'm suggesting what we call complete white operations, meaning we officially say what we're doing, how and why we're doing it. We message about the living conditions in those countries. There are many vulnerabilities in their information spaces.

Senator M. Deacon: My question is, looking at information and disinformation, more countries in the world, we think, are having less support for Ukraine. I'm trying to work through the impact of the disinformation on behalf of Russia in this question of sustained support. Is there anything you'd like to comment on that, because we can't pinpoint everything, cause and effect? I wonder where the disinformation is fitting on some countries beginning to reduce their support based on what they hear.

Je me demande de quelle façon on attaque ce problème. Autrement dit, comment informe-t-on nos gens sans leur mettre le doute dans la tête? Comment les empêcher de croire que tout peut être déformé, avec le résultat qu'ils se referment sur eux-mêmes?

M. Seaboyer : C'est une bonne question.

[*Traduction*]

Mes travaux actuels visent à mettre au point des campagnes d'influence éthiques, y compris à l'aide de l'intelligence artificielle.

Je propose de mener des opérations blanches parfaitement transparentes. Il s'agit d'annoncer ce que l'on fait, comment on le fait et pourquoi on le fait, à visage entièrement découvert, mais dans le but d'exploiter les vulnérabilités dans les espaces d'information des régimes autoritaires adverses.

En fait de vulnérabilité majeure, pensons entre autres à la corruption des plus hauts échelons de l'État. Une fois que l'on sait ce que la Chine et la Russie censurent le plus dans les discours dissidents, ce qu'elles veulent taire devient évident.

Je dis donc de ne pas créer de désinformation, évidemment, de ne pas mentir. Ce n'est pas nécessaire.

[*Français*]

Ce n'est absolument pas nécessaire.

[*Traduction*]

Il suffit de parler des conditions de vie réelles en les comparant aux nôtres. Au Canada, on peut publier ce qu'on veut sur Internet. Du moment qu'on respecte les limites de la loi, on ne sera jamais emprisonné. En Chine, par contre, quand on critique le gouvernement sur Internet, on fait 20 ans de prison. Nous pouvons parler de ce genre de choses. Nous pouvons faire le nécessaire pour mieux informer les gens qui s'intéressent à la question. Il y aura un effet boule de neige.

Je propose de lancer des opérations strictement blanches en annonçant officiellement ce que l'on fait et en expliquant le pourquoi et le comment. Parlons de conditions de vie dans les pays visés. Il y a beaucoup de vulnérabilités dans leurs espaces d'information.

La sénatrice M. Deacon : Je m'interroge. Quand on analyse l'information et la désinformation, on a l'impression que le soutien envers l'Ukraine perd du terrain dans le monde. Je cherche à comprendre quel est l'effet de la désinformation prorusse sur le soutien à long terme. Avez-vous quelque chose à dire à ce sujet? Après tout, nous ne pouvons pas cerner précisément toutes les causes et tous les effets. Je me demande dans quelle mesure la désinformation convainc certains pays de réduire leur soutien.

Mr. Erlich: One quick thing and then I will hand it over to my colleagues.

We often see these campaigns piggybacking off whatever domestic constituencies are anti-Ukraine. They take whoever is on the political spectrum who is not advocating for support for Ukraine and will then double down on it and proliferate that message.

They don't start with their own message. They find whatever message is already being popularized locally, and whatever constituency or country that is — and there is almost always one, often because it is expensive; it's not cheap. There are always those constituencies. That was very clear in the U.S. with the congressional funding package.

Mr. Seaboyer: There are two sides to this.

We cannot effectively measure behavioural change based on disinformation. We can see who engages with messages, spreads and comments on them. But who actually changes their behaviour on that is not measurable at this point. That said, we see a lot of correlation. Is it causation? That's difficult to tell. Based on my research, I would certainly say it seems like it is. It's hard to prove that, though.

We see where that campaigns are most effective, most concentrated, we also see changes in support. I would argue that some of the messages are effective. Russia doesn't know which messages are effective. We don't know. They spread so many, some of them stick. That's the approach they use.

The Chair: Thank you. This brings us to the end of the panel.

Thank you, Ms. Matviyenko, Mr. Seaboyer and Mr. Erlich for this informative exchange. We appreciate the time you've spent with us. You can tell from the questions around the room that you have provoked considerable thought and brought us very relevant information for what has been a several-week deep dive into matters in Ukraine. This has certainly been among the most important of them. You've added considerably to our understanding of this complex situation.

Thank you. We wish you all the very best. We appreciate the time that you took with us.

Colleagues, we now have our final panel of the meeting.

M. Erlich : Je vais répondre brièvement avant de laisser la parole aux autres.

Les campagnes de cette nature se greffent souvent à des intérêts politiques nationaux qui sont déjà défavorables à l'Ukraine. On se sert des acteurs politiques, peu importe leur mouvance. Du moment qu'ils n'expriment aucun soutien envers l'Ukraine, on en ajoute une couche tout en diffusant le message voulu.

On ne commence pas en véhiculant son propre message. Il s'agit d'en trouver un qui est déjà populaire sur le terrain, quels que soient les intérêts politiques ou le pays en cause, et on y arrive presque toujours. C'est parce que c'est généralement coûteux. Il faut mettre la main à la poche. Il y a toujours des intérêts politiques particuliers. C'était tout à fait limpide dans le cas du plan de financement du Congrès des États-Unis.

M. Seaboyer : Il y a deux côtés à la médaille.

C'est impossible de mesurer concrètement à quel point la désinformation influence les comportements. Nous pouvons déterminer qui interagit avec les messages, qui les relaie et qui les commente, mais pas qui sont les personnes dont le comportement a changé en conséquence. Pour l'instant, ce n'est pas mesurable. Cela dit, il y a une certaine corrélation. Peut-on parler de causalité? C'est difficile à dire. Cependant, d'après mes travaux, j'ai vraiment l'impression que oui, quoique ce soit difficile à démontrer.

Nous voyons où les campagnes sont le plus efficaces et où elles sont concentrées, et nous observons aussi l'évolution du soutien. Je dirais que certains messages sont efficaces. La Russie ne sait pas quels messages sont efficaces. Nous non plus. Elle en diffuse tellement, alors certains frappent la cible. C'est l'approche que la Russie emploie.

Le président : Voilà qui conclut ce panel, merci beaucoup.

Je vous remercie, madame Matviyenko, monsieur Seaboyer et monsieur Erlich, de ces échanges riches en information. Nous vous savons gré de nous avoir consacré du temps. Comme vous avez pu le constater, vous avez considérablement alimenté nos réflexions en nous fournissant de l'information très pertinente dans le cadre de notre examen en profondeur de la question ukrainienne, que nous avons entamé depuis plusieurs semaines. Ce panel a assurément été l'un des plus édifiants. Grâce à vous, nous comprenons beaucoup mieux les tenants et les aboutissants de la situation complexe de l'Ukraine.

Je vous remercie donc en vous souhaitant une excellente continuation à tous. Merci d'avoir pris le temps de venir.

Chers collègues, venons-en maintenant à notre dernier panel pour aujourd'hui.

For those joining across Canada, our meeting tonight is examining disinformation and cyber operations in the context of Russia's war against Ukraine. For this next hour, we welcome Jean-Christophe Boucher, Associate Professor, School of Public Policy at the University of Calgary; and Anatoliy Gruzd, Professor and Co-Director, Social Media Lab, Toronto Metropolitan University. We welcome the return of Mr. Marcus Kolga, Director, DisinfoWatch and Senior Fellow at the Macdonald-Laurier Institute.

Thank you all for being with us today. I now invite you to provide your opening remarks, to be followed by questions from our members. We're starting off with Mr. Jean-Christophe Boucher.

Mr. Boucher, welcome and begin whenever you're ready.

Jean-Christophe Boucher, Associate Professor, School of Public Policy, University of Calgary, as an individual: I know I only have five minutes, so I'll be quite brief.

At the University of Calgary, I run a research team funded by the Department of National Defence and Social Sciences and Humanities Research Council that does a range of studies on foreign interference and we look at far-right Chinese or Russian disinformation. Most of our team are a data analytics team, so we scrape Twitter, social media and we use machine learning and AI to kind of understand this.

When we look at Russian disinformation, we focus on three big things. One, looking at Russian propaganda on Twitter, and we've done a study on this at the beginning of the war. We also look right now at Russian strategic communication on social media, on Telegram, Facebook and Twitter. We also did a survey in 2022 on Canadian vulnerability to Russian disinformation. That's basically what's going to be the backbone of what I'm doing. If you're interested in the papers, I'll be happy to share them with anyone.

The first thing I want to say is that Russian strategic communication disinformation campaigns in Canada are strategic, meaning what? Two things. On the one hand, they have a fairly comprehensive and coherent and consistent way of engaging in the information space. Some people call this the chaos theory. I think that's incorrect. The Russians are strategic as they're trying to advance three things. On the one hand, they're trying to advance strategic objectives which are long-term objectives, looking at and emphasizing Russian's confrontation with the West, Russia's place in the international system, emphasizing anti-U.S. and anti-NATO narratives. They

Pour la gouverne des personnes à l'écoute, aux quatre coins du Canada, je rappelle que notre réunion de ce soir porte sur la désinformation et les cyberopérations dans le contexte de la guerre contre l'Ukraine menée par la Russie. Pour la prochaine heure, nous accueillons Jean-Christophe Boucher, professeur agrégé à l'École de politiques publiques de l'Université de Calgary, et Analtoliy Gruzd, professeur et co-directeur du Laboratoire des Médias Sociaux à l'Université métropolitaine de Toronto. Nous souhaitons par ailleurs bon retour parmi nous à Marcus Kolga, directeur de DisinfoWatch et chercheur principal à l'Institut Macdonald-Laurier.

Je vous remercie tous de votre présence et je vous invite maintenant à prononcer votre déclaration liminaire, qui sera suivie d'une période de questions. Commençons par Jean-Christophe Boucher.

Bienvenue, monsieur Boucher. Allez-y quand vous voulez.

Jean-Christophe Boucher, professeur agrégé, École de politiques publiques, Université de Calgary, à titre personnel : Je sais que je ne dispose que de cinq minutes, alors je ferai très court.

À l'Université de Calgary, je dirige une équipe de recherche financée par le ministère de la Défense nationale et le Conseil de recherches en sciences humaines qui réalise diverses études sur l'ingérence étrangère tout en se penchant sur la désinformation issue de l'extrême droite chinoise et russe. Notre équipe se compose majoritairement d'analystes de données, alors nous moissonnons Twitter et d'autres réseaux sociaux, puis nous nous servons de l'apprentissage automatique et de l'intelligence artificielle pour tirer les choses au clair.

En ce qui a trait à la désinformation russe, nous nous concentrons sur trois grands volets. Nous examinons la propagande russe sur Twitter. Nous avons d'ailleurs mené une étude à ce sujet au début de la guerre. Nous examinons aussi, en ce moment, la stratégie de communication de la Russie dans les réseaux sociaux, sur Telegram, Facebook et Twitter. Nous avons également réalisé une enquête en 2022 sur la vulnérabilité du Canada à la désinformation russe. C'est en gros la base de mon travail. Si les rapports de recherche vous intéressent, je me ferai un plaisir de vous les transmettre.

La première chose que je voudrais dire, c'est que les campagnes russes de communication stratégique et de désinformation au Canada sont stratégiques. Qu'est-ce que cela signifie? Deux choses. D'une part, elles ont une façon assez exhaustive, cohérente et constante d'intervenir dans l'espace informationnel. Certains appellent cela la théorie du chaos. Je pense que c'est inexact. Les Russes sont stratégiques, car ils essaient de promouvoir trois choses. D'une part, ils essaient de faire avancer des objectifs stratégiques à long terme, en mettant l'accent sur la confrontation de la Russie avec l'Occident, sur la place de la Russie dans le système international, et sur des

do this across the world consistently and it's no different in Canada.

The second part is they're also pushing operational objectives, which are what I call midterm objectives. This is really to undermine society, promote mistrust in democratic institutions. This is where we see them emphasizing essentially an amplifying message that goes against Canadian narratives, anti-LGBTQ, those kinds of things.

In the short term, they have tactical objectives which focus on the Ukraine war. They push disinformation on the Ukraine war to try to negotiate and advance their views of that war. They're fairly consistent in those three kinds of messages. If we want to do counter-narratives, we will have to tackle those systematically.

They're also strategic because they have a clear understanding of Canadian audiences, in fact, probably better than the Canadian government itself. They are exploiting our ecosystems in their strategic way. They are focused on two groups: The far right and the far left.

On the far right, they're amplifying messages — both in French and English — that promotes populist views, anti-immigration and anti-LGBTQ views. We've seen this. We have data on this, showing them coming into the information space, amplifying these voices and, in some ways, amplifying the inauthenticity of it.

We see they also engage with the far left. They create content for them. They collaborate with some of the far left in Canada who follow ministers around and have been to Russia. They participate in RT programs. They are ideologically connected to these views. The Russians are interested in pushing this. That's a good way of understanding how the Russians are doing this in terms of the audience segmentation.

When we look at Canadian vulnerabilities, my concern now is when we look at surveys on Russian disinformation — who are the Canadians most vulnerable to Russian disinformation — unfortunately, in our data we see a couple of things. On the one hand, younger Canadians have a harder time understanding Russian disinformation. People from rural communities or with less education also have difficulty recognizing Russian disinformation.

When we look at political parties and affiliation, unfortunately, people on the right of the spectrum, PPC voters and, in some respects, Conservatives have a harder time recognizing Russian disinformation. This is a concern for MPs and MLAs in my own province of Alberta who come to me and ask how can they fight this? They tell me they're finding these

discours antiaméricains et anti-OTAN. C'est ce qu'ils font partout dans le monde, et il en va de même au Canada.

La deuxième chose, c'est qu'ils poursuivent également des objectifs opérationnels, que j'appelle des objectifs à moyen terme. Il s'agit en fait de fragiliser la société, de promouvoir la méfiance à l'égard des institutions démocratiques. C'est là que nous les voyons essentiellement accentuer un message amplificateur qui va à l'encontre des discours canadiens; par exemple, des positions anti-LGBTQ.

À court terme, ils ont des objectifs tactiques axés sur la guerre en Ukraine. Ils diffusent de la désinformation sur la guerre en Ukraine pour essayer de négocier et de promouvoir leur point de vue sur cette guerre. Ils sont assez constants dans ces trois types de messages. Si nous voulons nous inscrire en faux contre ces messages, nous devrons nous y attaquer de manière systématique.

Les Russes sont également stratégiques parce qu'ils comprennent bien le public canadien; en fait, ils le comprennent probablement mieux que le gouvernement canadien lui-même. Ils exploitent nos écosystèmes de manière stratégique. Ils se concentrent sur deux groupes : l'extrême droite et l'extrême gauche.

À l'extrême droite, ils amplifient des messages — en français et en anglais — qui prônent des opinions populistes, anti-immigration et anti-LGBTQ. Nous l'avons observé. Nous disposons de données à ce sujet, montrant qu'ils entrent dans l'espace informationnel, qu'ils amplifient ces opinions et, d'une certaine manière, qu'ils en amplifient l'inauthenticité.

Nous constatons qu'ils dialoguent également avec l'extrême gauche. Ils créent du contenu pour eux. Ils collaborent avec certains membres de l'extrême gauche au Canada qui suivent les ministres et qui sont allés en Russie. Ils participent aux programmes de RT. Ils sont idéologiquement liés à ces opinions. Les Russes sont intéressés par la promotion de ces idées. C'est une bonne façon de comprendre comment les Russes procèdent pour segmenter le public.

En ce qui concerne les vulnérabilités des Canadiens, je m'intéresse maintenant aux enquêtes sur la désinformation russe, qui portent sur les Canadiens les plus vulnérables à la désinformation russe. Malheureusement, dans nos données, nous constatons deux choses. D'une part, les jeunes Canadiens ont plus de mal à comprendre la désinformation russe. D'autre part, les personnes issues de milieux ruraux ou moins éduquées ont également du mal à reconnaître la désinformation russe.

Quand on regarde les partis politiques et l'affiliation, malheureusement, les gens de droite, ceux qui votent pour le Parti populaire du Canada et, à certains égards, les conservateurs ont plus de mal à reconnaître la désinformation russe. C'est une préoccupation pour les députés fédéraux et provinciaux de ma province, l'Alberta, qui viennent me voir pour me demander

things more and more when they do canvassing. It's a greater concern.

To conclude, what we're seeing now is that the Russians are engaged in the information space. They have been effective, especially on the right, to push their narratives. Some of the far-right groups are parroting their narratives now.

Right now polling data suggests that, more and more, we're seeing Canadians — especially on the right of the spectrum — influenced by those kinds of narratives. In the long run, it will have an adverse impact on our capacity to engage with and support Ukraine in the long run.

Thank you very much.

The Chair: Thank you.

Anatoliy Gruzd, Professor and Co-Director, Social Media Lab, Toronto Metropolitan University, as an individual: Thank you for the opportunity to discuss the threat of Russian disinformation in the context of the Russia-Ukraine war. I am Anatoliy Gruzd, a Canada Research Chair and professor at Toronto Metropolitan University.

Today, my comments are my own. They are grounded in research I have conducted with my collaborator, Philip Mai and colleagues at the Social Media Lab where we study the spread of misinformation, information privacy and how social media impacts society.

The Kremlin has a long history of using information operations domestically and internationally. In recent years, we've seen how Russia has expanded such efforts to include the use of bots, trolls, hackers and other proxies to create a more favourable environment for their information operation.

Their influence campaigns are often across multiple digital platforms and rely on techniques such as creating fake personas and websites, as well as impersonating politicians, journalists and public agencies, attacking activists' accounts and amplifying polarizing topics.

Canadians are not immune to Russian disinformation. According to our 2022 national survey, 51% of Canadians actually reported seeing pro-Russian narratives on social media in the context of the Russia-Ukraine war. We find a strong link between exposure to such narratives and belief in them.

comment ils peuvent lutter contre ce phénomène. Ils me disent qu'ils découvrent de plus en plus de choses de ce genre lorsqu'ils font du porte-à-porte. C'est une préoccupation de plus en plus importante.

En conclusion, nous constatons que les Russes sont impliqués dans l'espace informationnel. Ils ont réussi, surtout à droite, à faire passer leurs idées. Certains groupes d'extrême droite reprennent aujourd'hui leur discours.

À l'heure actuelle, les données des sondages laissent penser que, de plus en plus, les Canadiens — en particulier ceux de droite — sont influencés par ce type de discours. À long terme, cela nuira à notre capacité à nous investir pour l'Ukraine et à la soutenir.

Merci beaucoup.

Le président : Merci.

Anatoliy Gruzd, professeur et codirecteur, Laboratoire des médias sociaux, Université métropolitaine de Toronto, à titre personnel : Merci de nous donner l'occasion de discuter de la menace de la désinformation russe dans le contexte de la guerre entre la Russie et l'Ukraine. Je m'appelle Anatoliy Gruzd, et je suis titulaire d'une chaire de recherche du Canada et professeur à l'Université métropolitaine de Toronto.

Aujourd'hui, mes propos n'engagent que moi. Ils s'appuient sur les recherches que j'ai menées avec mon collaborateur Philip Mai et mes collègues du Laboratoire des médias sociaux, où nous étudions la diffusion de mésinformation, la confidentialité de l'information et les incidences des médias sociaux sur la société.

Le Kremlin a depuis longtemps recours à des opérations d'information à l'échelle nationale et internationale. Ces dernières années, nous avons vu que la Russie a étendu ces efforts à l'utilisation de robots, de trolls, de pirates informatiques et d'autres intermédiaires afin de créer un environnement plus favorable à ses opérations dans le domaine de l'information.

Leurs campagnes d'influence se déroulent souvent sur plusieurs plateformes numériques et s'appuient sur des techniques telles que la création de faux profils et de faux sites Web, ainsi que l'usurpation d'identité de politiciens, de journalistes et d'organismes publics, l'attaque de comptes d'activistes et l'amplification de sujets polarisants.

Les Canadiens ne sont pas à l'abri de la désinformation russe. Selon notre enquête nationale de 2022, 51 % des Canadiens ont déclaré avoir vu des discours prorusses sur les médias sociaux dans le contexte de la guerre entre la Russie et l'Ukraine. Nous constatons qu'il existe un lien étroit entre l'exposition à de tels discours et la croyance en ceux-ci.

We also find that a person's prior beliefs and politically motivated reasoning make them more susceptible to disinformation. For example, Canadians — as we heard — with right-leaning views, and those who trust partisan media, are more likely to believe in pro-Kremlin information.

Left unchallenged, the state-sponsored information operations can undermine Canadian democracy. The question we want to discuss is: What can we do to mitigate such risks?

Blocking state-run media outlets like RT News is only partially effective, as the Kremlin circumvents such sanctions by copying content and disseminating it through other channels. In fact, they also rely on social media accounts of their diplomatic services, like the Russian embassy in Ottawa, and sympathetic media personalities in the West, directly or indirectly.

To fight state-sponsored disinformation, digital platforms should be mandated to expand their partnerships with fact-checking organizations and facilitate access to credible news.

Unfortunately, as we have seen in recent years, the digital platforms essentially have retreated from these areas. With newsrooms closing or downsizing across Canada, more Canadians will turn to social media influencers rather than journalists. This is concerning because our research indicates that individuals who trust mainstream media are less susceptible to pro-Kremlin disinformation. Therefore, investing in a strong journalistic community, and enhancing trust in mainstream media outlets, could effectively combat information operations here in Canada.

Another line of defence I would like to discuss is implementing proactive or prebunking strategies to inoculate Canadians against future disinformation campaigns. We heard about some of them today already. For instance, running public service announcements and educational games that incorporate known false claims, tactics and sources used by foreign adversaries can reduce the perceived persuasiveness of information operations.

We have also seen an increasing use of generative AI to create disinformation about the Russia-Ukraine war. Again, we've heard some examples of it today.

Nous avons également constaté que les croyances antérieures et le raisonnement politique d'une personne la rendent plus sensible à la désinformation. Par exemple, les Canadiens — comme nous l'avons entendu — qui ont des opinions de droite et ceux qui font confiance aux médias partisans sont plus susceptibles de croire aux renseignements favorables au Kremlin.

Si elles ne sont pas contrecarrées, les opérations d'information parrainées par des États étrangers peuvent miner la démocratie canadienne. La question que nous souhaitons aborder est la suivante : que pouvons-nous faire pour atténuer les risques?

Le blocage des médias étatiques comme RT News n'est que partiellement efficace, car le Kremlin contourne les sanctions en copiant le contenu et en le diffusant par d'autres canaux. En fait, le Kremlin s'appuie également sur les comptes de médias sociaux de ses services diplomatiques, comme l'ambassade de Russie à Ottawa, et sur des personnalités médiatiques occidentales qui lui sont favorables, directement ou indirectement.

Pour lutter contre la désinformation orchestrée par des États, les plateformes numériques devraient être obligées de développer leurs partenariats avec des organismes de vérification des faits et de faciliter l'accès à des nouvelles crédibles.

Malheureusement, comme nous l'avons vu ces dernières années, les plateformes numériques se sont essentiellement retirées du secteur de l'information. Avec la fermeture ou la réduction des effectifs des salles de presse dans tout le pays, davantage de Canadiens se tourneront vers les influenceurs des médias sociaux plutôt que vers les journalistes. Cette situation est préoccupante, car nos recherches indiquent que les personnes qui font confiance aux médias traditionnels sont moins sensibles à la désinformation pro-Kremlin. Par conséquent, investir dans une communauté journalistique forte et renforcer la confiance dans les médias traditionnels permettrait de lutter efficacement contre les opérations d'information au Canada.

Une autre ligne de défense que j'aimerais aborder est la mise en œuvre de stratégies proactives ou de « prebunking », c'est-à-dire éduquer les Canadiens et les prévenir des campagnes de désinformation en ligne. Nous avons déjà entendu parler de certaines de ces stratégies aujourd'hui. Par exemple, la diffusion de messages d'intérêt public et de jeux éducatifs reprenant les fausses allégations, les tactiques et les sources utilisées par nos adversaires étrangers peuvent réduire la force de persuasion perçue des opérations d'information.

Nous avons également constaté une utilisation croissante de l'intelligence artificielle générative pour créer de la désinformation au sujet de la guerre entre la Russie et l'Ukraine. Là encore, nous en avons entendu quelques exemples aujourd'hui.

While most recent AI fakes were quickly debunked, I expect an increase in usage, frequency and scale of such usage, specifically in the areas of social engineering and reputational attacks.

Therefore, we must enhance and educate not only the general public on the danger of disinformation and the importance of cybersecurity, but also policy-makers and civil servants who are often the targets of such attacks; also, conducting readiness assessments for these groups would identify existing vulnerabilities.

In conclusion, we must not underestimate the potential of the Kremlin's information operations to undermine public trust in government institutions over time. Deplatforming individual sources may not be as effective, as it could also undermine trust toward government and legitimize censorship.

A more nuanced approach should consider the various forms of information operations that they take, and develop strategies to address them more directly. This could include requiring large social media platforms to expand their trust and safety teams here in Canada, share data with researchers and journalists to increase transparency and support independent audits.

Schools must update digital literacy programs to address the challenges of today, such as generative AI. For the general public, the government should develop prebunking campaigns to educate Canadians about foreign interference. Aspects of such educational campaigns must focus on and be informed by diaspora communities in Canada, as they are more likely to be targeted by foreign states.

Thank you.

The Chair: Thank you.

Marcus Kolga, Director, DisinfoWatch, and Senior Fellow, Macdonald-Laurier Institute, as an individual: Thank you for inviting me here today.

I'm a practitioner and an activist who has been monitoring and trying to expose Russian information operations since 2007 when this new phase of Russia's information operations started targeting Estonia.

The broad primary objective of Russian information and influence operations is, of course, to distort our understanding of the world around us and to ultimately manipulate and affect our democratic processes and policy decisions. This isn't new.

Bien que la plupart des récentes contrefaçons par intelligence artificielle aient été rapidement démystifiées, je m'attends à une augmentation de l'utilisation, de la fréquence et de l'ampleur de cette utilisation, plus particulièrement dans les domaines de l'ingénierie sociale et des attaques visant à nuire à la réputation.

Par conséquent, nous devons sensibiliser et éduquer au danger de la désinformation et à l'importance de la cybersécurité non seulement le grand public, mais aussi les décideurs et les fonctionnaires qui sont souvent la cible de telles attaques; en outre, la réalisation d'évaluations de l'état de préparation de ces personnes permettrait de recenser les vulnérabilités existantes.

En conclusion, nous ne devons pas sous-estimer la capacité des opérations d'information du Kremlin à saper la confiance du public dans les institutions gouvernementales au fil du temps. Le sociomuselage de sources individuelles n'est peut-être pas aussi efficace, car il pourrait également saper la confiance envers le gouvernement et légitimer la censure.

Une approche plus nuancée devrait prendre en compte les différentes formes d'opérations d'information qu'elles prennent, et élaborer des stratégies pour les combattre plus directement. Il pourrait s'agir d'exiger des grandes plateformes de médias sociaux qu'elles renforcent leurs équipes chargées de la confiance et de la sécurité au Canada, qu'elles partagent leurs données avec les chercheurs et les journalistes afin d'accroître la transparence, et qu'elles soutiennent des audits indépendants.

Les écoles doivent mettre à jour les programmes de culture numérique pour faire face aux défis d'aujourd'hui tels que l'intelligence artificielle générative. Pour le grand public, le gouvernement doit élaborer des campagnes afin d'éduquer les Canadiens sur l'ingérence étrangère. Certains aspects de ces campagnes éducatives doivent être axés sur les diasporas au Canada et en tenir compte, car elles sont plus susceptibles d'être ciblées par des États étrangers.

Merci.

Le président : Merci.

Marcus Kolga, directeur, DisinfoWatch et chercheur principal, Institut Macdonald-Laurier, à titre personnel : Merci de m'avoir invité ici aujourd'hui.

Je suis un praticien et un activiste qui surveille et tente de dénoncer les opérations d'information russes depuis 2007, année où, dans une nouvelle phase de ses opérations d'information, la Russie a commencé à cibler l'Estonie.

L'objectif principal des opérations d'information et d'influence russes est, bien entendu, de fausser notre compréhension du monde qui nous entoure et, en fin de compte, de manipuler et d'influencer nos processus démocratiques et nos décisions politiques. Ce n'est pas nouveau.

In 1945, a Soviet intelligence clerk serving in the Soviet embassy in Ottawa defected. He outlined the scale of this work when he identified dozens of Canadians who were working with the Soviets to influence our democratic processes. For the Kremlin, those operations are more important, of course, today than ever before. That threat, in terms of information warfare and the assault on our cognitive sovereignty, is persistent and growing.

Disinformation campaigns that once took years to execute now take minutes with the help of social media, artificial intelligence and an army of pro-Kremlin influencers that amplify Russian information narratives in Canada.

Inside Russia, the Kremlin uses information operations against its own people in order to consolidate power and silence critics. Putin is constructing a virtual Iron Curtain around Russia's information environment, which the state controls; it controls all media. The Kremlin has criminalized most independent media outlets and civil society organizations as either undesirable or terrorists. This list includes the entire LGBTQ community in Russia and even Canada's Macdonald-Laurier Institute.

Abroad, the Kremlin seeks to divide, confuse and sow chaos wherever possible. The breakdown of cohesion within our international alliances NATO has been a Kremlin objective for 75 years. Inside Western nations, Russia aims to divide us by exploiting both sides of sensitive political issues, with the goal of eroding trust in democratic institutions, media, leaders, civil society and ultimately among each other.

In Canada, we've observed Russian information operations amplifying vaccine hesitancy, even before COVID, targeting MMR and other children's vaccinations. Extremist far-right anti-government voices within the "Freedom Convoy" movement were platformed by Russian state media in 2022. Russian anti-LGBTQ narratives are amplified by far-right extremists and platforms in Canada as well.

On the Canadian far left, anti-Ukrainian influencers continue to write for and appear on sanctioned Russian state media and Kremlin-controlled think tanks. Ukraine, of course, has been the primary target of Russian information and influence operations for the past few years, with the objective of eroding public and government support for Ukraine. That includes false claims about corruption and the resale of the weapons that the West has donated to Ukraine. It also includes Orwellian claims by Vladimir Putin that Russia didn't start the war, and that it is attacking Ukraine to end it. They also include narratives intended

En 1945, un employé des services de renseignement soviétiques en poste à l'ambassade soviétique à Ottawa a fait défection. Il a souligné l'ampleur de ce travail en identifiant des dizaines de Canadiens qui travaillaient avec les Soviétiques en vue d'influencer nos processus démocratiques. Pour le Kremlin, ces opérations sont bien sûr plus importantes aujourd'hui que jamais. Cette menace, sous la forme d'une guerre de l'information et d'une atteinte à notre souveraineté cognitive, est persistante et croissante.

Les campagnes de désinformation, dont l'exécution prenait autrefois des années, se déroulent désormais en quelques minutes grâce aux médias sociaux, à l'intelligence artificielle et à une armée d'influenceurs pro-Kremlin qui amplifient les discours d'information russes au Canada.

En Russie, le Kremlin utilise des opérations d'information contre son propre peuple afin de consolider le pouvoir et de faire taire les critiques. Poutine est en train de construire un rideau de fer virtuel contrôlé par l'État autour de l'environnement d'information de la Russie; il contrôle tous les médias. Le Kremlin a criminalisé la plupart des médias indépendants et des organisations de la société civile en les qualifiant d'indésirables ou de terroristes. La liste comprend l'ensemble de la communauté LGBTQ en Russie, et même l'Institut Macdonald-Laurier du Canada.

À l'étranger, le Kremlin cherche à diviser, et à semer la confusion et le chaos partout où cela est possible. La rupture de la cohésion au sein de nos alliances internationales, comme l'OTAN, est un objectif du Kremlin depuis 75 ans. En Occident, la Russie cherche à nous diviser en exploitant les deux côtés de questions politiques sensibles, dans le but d'éroder notre confiance envers nos institutions démocratiques, nos médias, nos dirigeants, notre société civile et, en fin de compte, notre confiance les uns envers les autres.

Au Canada, nous avons observé des opérations d'information russes qui amplifient l'hésitation face aux vaccins, même avant la pandémie de COVID-19, en ciblant le vaccin ROR et d'autres vaccins pour enfants. Des voix antigouvernementales extrémistes d'extrême droite au sein du mouvement du convoi pour la liberté ont été diffusées par les médias publics russes en 2022. Au Canada aussi, des extrémistes et des plateformes d'extrême droite amplifient les discours anti-LGBTQ de la Russie.

Du côté de l'extrême gauche canadienne, des influenceurs anti-ukrainiens continuent d'écrire pour des médias d'État russe sanctionnés et des groupes de réflexion contrôlés par le Kremlin, et d'apparaître dans ces médias. L'Ukraine, bien sûr, a été la cible principale des opérations d'information et d'influence russes au cours des dernières années, avec pour objectif d'éroder le soutien du public et du gouvernement envers l'Ukraine. Ces opérations comprennent de fausses allégations sur la corruption et la revente des armes que l'Occident a données à l'Ukraine. Cela inclut également les affirmations orwelliennes de Vladimir

to incite hate toward Ukrainians. That includes baseless accusations about President Zelenskyy, his government and Ukrainians being neo-Nazis.

Canadian human rights legal expert Yonah Diamond at the Raoul Wallenberg Centre for Human Rights says that this narrative is part of the Kremlin's accusations and a mirror tactic by which Russia frames and presents Ukraine and Ukrainians as an existential threat, which makes hate and violence against Ukrainians appear to be defensive and justifiable. Those narratives are repeated by far-right and far-left platforms in Canada, and they continue to be spread in parts of the Russian diaspora community in Canada, threatening radicalization through Canadian online streaming services that evade Canadian restrictions of Russian state media and possibly our sanctions as well.

Those narratives are also impacting Canadians. According to the Ukrainian congress, incidents of hate and violence toward Canadians of Ukrainian heritage have been rising over the past two years. Last year, a letter was sent to the Estonian Honorary Vice Consul in Toronto, threatening to spread anthrax if the Estonian community continued to support Ukraine.

The impact of such narratives is intensified when they ricochet between far left and far right platforms and influencers.

At the bottom of the political horseshoe are U.S. far-right politicians like Marjorie Taylor-Greene, who regularly amplifies these false claims about Ukraine, and on the far left, platforms like Montréal's Global Research.

It is seemingly impacting Western opinions and policy toward Ukraine. Polling among Conservative voters indicates that support for Ukraine has significantly dropped over the past two years. In 2022, just 20% of Conservative voters believed that Canada was giving too much to Ukraine, versus 43% in February 2024. In the U.S., 48% of Republican voters believe the U.S. is giving too much to Ukraine today, versus just 9% in March of 2022.

While Canada has taken major steps to defend our cognitive sovereignty, there's still much to learn from our allies in Ukraine and the Baltic region to challenge these narratives and the influencers who amplify them in Canada and the Western world.

Poutine selon lesquelles la Russie n'a pas commencé la guerre et qu'elle attaque l'Ukraine pour y mettre fin. Il s'agit également de discours visant à inciter la haine à l'égard des Ukrainiens. De plus, ces discours véhiculent des accusations sans fondement selon lesquelles le président Zelenski, son gouvernement et les Ukrainiens seraient des néonazis.

Selon l'expert juridique canadien en droits de la personne Yonah Diamond, du Centre Raoul Wallenberg pour les droits de la personne, ce discours fait partie des accusations du Kremlin et constitue une tactique miroir par laquelle la Russie définit et présente l'Ukraine et les Ukrainiens comme une menace existentielle, ce qui fait que la haine et la violence à l'égard des Ukrainiens semblent avoir un caractère défensif et justifiable. Ces idées sont reprises par des plateformes d'extrême droite et d'extrême gauche au Canada, et elles continuent d'être diffusées dans certaines parties de la diaspora russe au Canada, ce qui constitue une menace de radicalisation par la voie de services de diffusion en ligne canadiens qui échappent aux restrictions imposées aux médias d'État russes au Canada, et peut-être aussi à nos sanctions.

Ces discours ont également une incidence sur les Canadiens. Selon le Congrès ukrainien, les incidents de haine et de violence à l'encontre des Canadiens d'origine ukrainienne ont augmenté au cours des deux dernières années. L'an dernier, le vice-consul honoraire d'Estonie à Toronto a reçu une lettre menaçant de répandre de l'anthrax si la communauté estonienne continuait à soutenir l'Ukraine.

La portée de ces messages est d'autant plus grande qu'ils circulent entre les plateformes et les influenceurs d'extrême gauche et d'extrême droite.

Au bas du fer à cheval du spectre politique, on retrouve des politiciens américains d'extrême droite comme Marjorie Taylor-Greene, qui amplifie régulièrement ces fausses affirmations sur l'Ukraine, et des plateformes d'extrême gauche comme Global Research de Montréal.

Cela semble avoir une incidence sur les opinions et les politiques de l'Occident à l'égard de l'Ukraine. Selon un sondage réalisé auprès des électeurs conservateurs, le soutien envers l'Ukraine a considérablement diminué au cours des deux dernières années. En 2022, seulement 20 % des électeurs conservateurs croyaient que le Canada était trop généreux envers l'Ukraine, contre 43 % en février 2024. Aux États-Unis, 48 % des électeurs républicains estiment aujourd'hui que leur pays est trop généreux envers l'Ukraine, contre seulement 9 % en mars 2022.

Bien que le Canada ait pris des mesures majeures pour défendre notre souveraineté cognitive, nous avons encore beaucoup à apprendre de nos alliés en Ukraine et des pays baltes pour combattre ces discours et les influenceurs qui les amplifient au Canada et dans le monde occidental.

I'll leave it there for now. I look forward to your questions.

The Chair: Thank you very much. We'll now go to questions. You know the rules. You have four minutes for the question and answer both. We'll move through this as briskly as we can.

[*Translation*]

Senator Dagenais: My first question is for Mr. Boucher. I'd like to talk to you about one aspect of the use of social media like Twitter — which has become X — in terms of their real impact on disinformation. Take the phenomenon of people retweeting, which is very important on these platforms. Aren't we always reaching the same people by doing this, which diminishes the real impact of the Russians in their attempts to spread disinformation through this means of communication?

Mr. Boucher: I would say yes and no. Yes, insofar as it's true that when you start looking at influencers, those who retweet have more influence on the platform. However, what we see in the data is that these people generally have millions of followers. In some cases, some of these influencers don't necessarily focus on Ukraine, but work on masculinism, for example. So their reach is sometimes greater than you might think.

Twitter is very 2022, and the platform is less relevant to them. However, we are beginning to see other platforms, such as Telegram, TikTok, Reddit, Facebook and YouTube, forming part of the information arsenal of agents associated with the regime in Moscow. For example, surveys now show that young people are increasingly saying that their main source of information is YouTube, a social media on which there is virtually no moderation. There are recommendations made through algorithms where people come across content that has not been retransmitted on Twitter, and this is having an increasingly effective impact on young people.

In our survey, we saw that young people were less able to identify disinformation than older people. Older people are always criticized for not understanding the social media environment and that's why they're misinformed. In my surveys, I see young people having trouble distinguishing between what's true and what's false. So we need to focus on that. I would focus less on X and more on the organization as a whole. The major problem we have in Canada is our capacity to collect data and monitor the environment; it's virtually non-existent. The Canadian government, apart from the intelligence services, has very little capacity, so we don't know what's going on in social media and we're always lagging behind in this environment.

Je vais m'arrêter là pour l'instant. Je suis impatient de répondre à vos questions.

Le président : Merci beaucoup. Nous passons aux questions. Vous connaissez les règles. Vous disposez de quatre minutes, et cela englobe à la fois les questions et les réponses. Nous allons procéder aussi rapidement que possible.

[*Français*]

Le sénateur Dagenais : Ma première question s'adresse à M. Boucher. J'aimerais vous parler d'un aspect de l'utilisation des médias sociaux comme Twitter — qui est devenu X — par rapport à leur véritable portée sur la désinformation. Prenons le phénomène qui fait que les gens vont « retweeter » et qui est très important sur ces plateformes. Est-ce qu'on ne rejoint pas toujours les mêmes personnes en faisant cela, ce qui diminue l'impact réel des Russes dans leurs tentatives de désinformation au moyen de ce moyen de communication?

M. Boucher : Je dirais oui et non. Oui, dans la mesure où c'est vrai que lorsqu'on commence à regarder les influenceurs, ceux qui retweetent ont plus d'influence sur la plateforme. Toutefois, ce qu'on voit dans les données, c'est que généralement, ces personnes ont des millions de personnes qui les suivent. Dans certains cas, certains de ces influenceurs ne s'attardent pas nécessairement à l'Ukraine mais travaillent sur le masculinisme, par exemple. Donc, leur portée est parfois plus importante que ce que l'on pourrait croire.

Twitter, c'est très 2022, et la plateforme est moins pertinente pour eux. Par contre, on commence à voir d'autres plateformes, comme Telegram, TikTok, Reddit, Facebook et YouTube font partie de l'arsenal informationnel des agents associés au régime à Moscou. Par exemple, maintenant, on voit dans les sondages que les jeunes disent de plus en plus que leur principale source d'information, c'est YouTube. Or, sur YouTube, il n'y a à peu près pas de modération. Il y a des recommandations qui se font à travers les algorithmes où les gens tombent sur du contenu non retransmis sur Twitter, et cela a de plus en plus un impact effectif sur les jeunes.

Dans notre sondage, on a vu que les jeunes étaient moins en mesure d'identifier la désinformation que ceux qui sont plus âgés. On critique toujours les plus vieux en disant qu'ils ne comprennent pas l'environnement des médias sociaux et que c'est pour ça qu'ils sont désinformés. Dans mes sondages, ce que je vois, ce sont des jeunes qui ont de la difficulté à faire la différence entre le vrai et le faux. Il faut donc s'attarder à cela. Je m'attarderais moins à X et plus à l'ensemble de l'organisation. Le problème majeur qu'on a au Canada, c'est notre capacité à collecter des données et à surveiller l'environnement; elle est à peu près nulle. Le gouvernement canadien, à part les services de renseignement, a très peu de capacité, alors on ne sait pas ce qui se passe sur les médias sociaux et on est toujours à la traîne dans cet environnement.

One of the recommendations I would make is to increase the Canadian government's capabilities quite radically. The group that's part of Global Affairs Canada, Rapid Response Mechanism Canada, is the only one really working on this. Its staffing levels are far below what we need. Russia spends $3 billion or $4 billion a year on disinformation. How much does Canada spend? Maybe $20 million or $30 million, if you look at all the departments? That is too little.

Senator Dagenais: Apart from social media, have the Russians managed to infiltrate more traditional media in Canada, such as newspapers and television, to convey certain information or opinions, in order to influence political decision-making or raise public disapproval of certain positions taken by allied countries against the Soviet regime?

Mr. Boucher: That's a good question. I don't know. However, what I do see is that when you read and analyze what people are saying…. In French, in *Le Devoir* and *La Presse*, some journalists sometimes take a pro-Russian and pro-Kremlin position, to the great dismay of all those who work on this issue. I see this more often in French than in English. When I look at the English-language media, I see this tendency more in the right-wing and far-right media. Is there pure infiltration? No, but we are seeing more and more that certain journalists feel free to convey these objectives and these stories. We tried to do a study on the penetration of Russian propaganda stories in the traditional media. The phenomenon is marginal, but the trend is growing. Mr. Kolga mentioned this earlier: It explains the slow erosion of support for Ukraine and it's increasingly difficult to get involved in this area.

Senator Dagenais: Thank you very much.

[*English*]

Senator Boehm: Thank you for being here. I'm following up where Senator Dagenais left off.

Professor Boucher, you and your research group — at least in the 2022 paper — collected more than 6.2 million tweets, as they were then known — they're now postings. You came to the conclusion that the Russian influence on social media was prevalent. I guess the assumption would be that it's even more prevalent now.

What is the probability that an average user of social media in Canada will encounter Russian disinformation through just random doomscrolling, since this is a sort-of doom topic? Also, you mentioned the demographic groups — urban versus rural and young versus old — but are there any other targeted areas that you would see? At the end, I would also like to know if you have an opinion on the reposting by political figures, who are

Une des recommandations que je ferais, c'est d'augmenter de façon assez radicale les capacités du gouvernement canadien. Le groupe qui fait partie d'Affaires mondiales Canada, Mécanisme de réponse rapide du Canada, est le seul qui travaille vraiment là-dessus. Ses effectifs sont largement en deçà de ce dont on a besoin. La Russie dépense 3 ou 4 milliards de dollars par année en matière de désinformation. Combien dépense le Canada? Peut-être 20 millions ou 30 millions, si l'on regarde l'ensemble des ministères? C'est trop peu.

Le sénateur Dagenais : Au-delà des médias sociaux, est-ce que les Russes ont réussi à s'infiltrer dans des médias plus traditionnels au Canada, comme les journaux et la télévision, pour véhiculer certaines informations ou des opinions, afin d'influencer la prise de décisions politiques ou soulever la désapprobation populaire face à certaines prises de position des pays alliés contre le régime soviétique?

M. Boucher : C'est une bonne question. Je ne sais pas. Par contre, ce que je vois, c'est que quand on lit et qu'on analyse ce que les gens disent... En français, dans *Le Devoir* et dans *La Presse*, il y a parfois certains auteurs qui véhiculent une position qui est prorusse et pro-Kremlin, à la grande consternation de tous ceux qui travaillent sur cet enjeu. Je le vois plus souvent en français qu'en anglais. Lorsque je regarde les médias anglophones, je vois cette tendance plutôt dans les médias de droite et d'extrême droite. Est-ce qu'il y a une infiltration pure et dure? Non, mais on voit de plus en plus que certains auteurs se sentent libres de véhiculer ces objectifs et ces récits. On a essayé de faire une étude sur la pénétration des récits de propagande russe dans les médias traditionnels. Le phénomène est marginal, mais la tendance augmente. M. Kolga en parlait plus tôt : cela explique l'érosion lente du soutien à l'Ukraine et c'est de plus en plus difficile de s'engager dans ce terrain-là.

Le sénateur Dagenais : Merci beaucoup.

[*Traduction*]

Le sénateur Boehm : Je vous remercie de votre présence. Je vais poursuivre dans la même veine que le sénateur Dagenais.

Monsieur Boucher, votre groupe de recherche et vous — du moins d'après le document de 2022 — avez recueilli plus de 6,2 millions de gazouillis, comme on les appelait déjà — on parle maintenant de publications. Vous avez conclu que l'influence russe sur les médias sociaux est répandue. Je suppose qu'on peut présumer qu'elle est encore plus répandue maintenant.

Quelle est la probabilité qu'un utilisateur moyen des médias sociaux au Canada rencontre de la désinformation russe en s'adonnant à du défilement morbide, puisqu'il s'agit d'un sujet en quelque sorte morbide? De plus, vous avez mentionné les groupes démographiques — les personnes qui vivent en milieu urbain par rapport à celles qui vivent en milieu rural, et les jeunes par rapport aux personnes plus âgées —, mais avez-vous

perhaps doing it innocently enough in order to make a point but are essentially reposting propaganda.

Mr. Boucher: That is a great question. In the data — both on social media and in the survey — we find that 80% of Canadians are mostly not touched by that kind of narrative. The issue we have is that the 20% fall into that rabbit hole and stay there, and that 20% has a lot of impact on our political life and slowly but surely has more and more influence in the political sphere — especially in my own province, for example. That's the issue. I see this as a vulnerability population problem, where 80% are pretty okay, but there are still 20% stuck there, and they're not getting out. Then, slowly but surely, they're having an impact on the other part.

In terms of prebunking, if I were doing the strategic communication on behalf of the Government of Canada, I would focus on these groups and engage with them. Some MLAs and MPs in my own province — who are Conservative, of course — ask me sometimes if I want to speak to their groups or public speaking to talk about Russian disinformation. They're concerned about the impact it has on our population and on our groups. That would be the kind of argument I have. It's a kind of good and bad story at the same time.

The second question was on Conservatives.

Senator Boehm: I didn't mention —

Mr. Boucher: I agree. However, I still think that's the problem. I think political elites have a massive impact in that environment, to be fair. Network effects are way more influential in spreading disinformation than the information itself. When we look at the data, people who are misinformed are misinformed on everything. It's not about information; it's about in-group/out-group positions. My own position is that political elites have a vested interest in being on top of those issues and carrying that message to everyone. If they speak strongly, then people will follow.

I also think that when we wobble on those issues, we make ourselves and our society more susceptible to Russian disinformation. Foreign interference is a crime of opportunity. You need a suitable target, a malicious actor and a lack of enforcement. The malicious actors will do this anyway. We don't have a lot of enforcement right now on foreign interference, but what we can do is make the suitable target less and less important. For example, if parties come together and say, "We are steadfast in our support for Ukraine. We don't care what you

observé d'autres groupes ciblés? J'aimerais également connaître votre opinion au sujet de la republication par les politiciens, qui le font peut-être innocemment pour soutenir leur point de vue, mais qui, essentiellement, republient de la propagande.

M. Boucher : C'est une excellente question. Les données — tant celles recueillies sur les médias sociaux que celles issues du sondage — montrent que 80 % des Canadiens ne sont pas touchés par ce genre de discours. Le problème, c'est que 20 % des Canadiens se font enfirouaper et n'en dérogent plus, et ces 20 % ont une grande incidence sur notre vie politique et leur influence s'accroît lentement mais sûrement dans la sphère politique — surtout dans ma province. Voilà le problème. Une partie de la population est vulnérable. Quatre-vingts pour cent des gens sont intouchés, mais il n'en demeure pas moins que 20 % des gens se laissent prendre au piège et n'en ressortent pas, puis, lentement mais sûrement, ils ont une incidence sur les autres.

Au chapitre de la démystification préventive, si j'étais responsable des communications stratégiques au nom du gouvernement du Canada, je concentrerais mes efforts sur ces groupes. Certains députés provinciaux et fédéraux de ma province — qui sont conservateurs, bien entendu — me demandent parfois si j'aimerais donner une présentation à des groupes ou une allocution publique au sujet de la désinformation russe. Ils sont préoccupés par l'incidence de celle-ci sur la population et les groupes qu'ils représentent. C'est un peu ce que je présenterais. Il y a à la fois du bon et du mauvais.

La deuxième question portait sur les conservateurs.

Le sénateur Boehm : Je n'ai pas mentionné...

M. Boucher : Je suis d'accord. Toutefois, je crois tout de même que c'est là le problème. Selon moi, il faut admettre que l'élite politique a une incidence massive dans ce milieu. L'influence des réseaux est beaucoup plus efficace pour propager la désinformation que l'information elle-même. Quand on regarde les données, on constate que les gens mal renseignés sont mal renseignés à propos de tout. L'information a peu d'importance; tout dépend des positions adoptées selon qu'on fait partie ou non du groupe. Ma propre position est que l'élite politique a tout intérêt à être à l'affût de ces questions et à communiquer ce message à tout le monde. Si elle s'exprime d'une voix forte, les gens vont l'écouter.

Je crois également que lorsque nous sommes ambivalents à l'égard de ces questions, nous devenons et rendons la société plus vulnérable à la désinformation russe. L'ingérence étrangère est un crime commis parce que l'occasion se présente. Il faut une cible adéquate, un acteur malveillant et de la négligence dans l'application de la loi. Les acteurs malveillants vont commettre ces actes de toute manière. À l'heure actuelle, nous appliquons peu la loi en matière d'ingérence étrangère. Toutefois, ce que nous pouvons faire, c'est rendre la cible adéquate de moins en

will do and try to say in our information environment. We'll do this."

My own perspective — and that's what I ask of my colleagues in Alberta — is that you should speak more strongly about those issues, and you shouldn't be afraid to support Ukraine, and say, "This is a question of values. We support democracy and the rule of law, and we don't really care which party you vote for. This is just a fundamental value and principle." Just stand on those. That would be my answer.

Senator Cardozo: I have a couple of questions.

Professor Boucher, in terms of what is going on in the discussion, my sense is that it's more the far right than the far left. I would put some of the far-left examples you gave me in the far-right column, in a sense — people are supporting the Russian regime.

I'm wondering why mainstream conservatives in the U.S. are pulling away from Ukraine. We're getting a bit of that in Canada. Why is that happening?

Mr. Gruzd, I'd like to get more details from you on media education programs, I think. They are awfully important. I'd be interested to know what we can be doing more of.

Mr. Boucher: I'll go fast —

Senator Cardozo: Don't go too fast.

Mr. Boucher: I speak like this in French and English, so I'm sorry.

I think the growth audience for Russians right now is the far right and the Conservatives. If I had to put any money on it, I would put my money there. It seems like on the far left right now — if we are speaking about Iranian or Iranian-backed proxies right now, I would talk about the far left. I think this is where they're making a lot of inroads. However, on Russian disinformation, it seems like that's the ecosystem. Some of it is because of the Americans. They have been able to convince a large part of the American electorate and influencers like Tucker Carlson or Marjorie Taylor Greene of their narratives. That, unfortunately, has an impact in Canada. Our ecosystems are roughly the same. The Canadian far-right groups are integrated with American far-right groups, and that matters.

There are a lot of reasons why that happens. One of those is polarization. When we do surveys on polarizations, we sometimes find that people have an effective relationship with their parties, and it really is up to the parties to decide what they're going to say. In the U.S., the party has steered toward the right, and the Make America Great Again, or MAGA, elements

moins importante. Par exemple, si les partis unissent leur voix pour dire: « Nous appuyons résolument l'Ukraine. Quoi que vous fassiez ou que vous tentiez de raconter dans notre environnement d'information, nous ne changerons pas d'idée. »

À mon avis — et c'est ce que je demande à mes collègues d'Alberta —, vous devez vous exprimer plus fort à propos de ces questions. Vous ne devez pas avoir peur d'appuyer l'Ukraine. Vous devez dire : « C'est une question de valeurs. Quel que soit le parti que nous appuyons, nous soutenons la démocratie et la primauté du droit. Ce sont des valeurs et des principes fondamentaux. » Défendez ces derniers. Voilà ma réponse.

Le sénateur Cardozo : J'ai quelques questions.

Monsieur Boucher, je crois comprendre que l'extrême droite est plus touchée que l'extrême gauche. Je classerais certains des exemples de l'extrême gauche que vous avez donnés dans la catégorie de l'extrême droite, en quelque sorte. Les gens soutiennent le régime russe.

Je me demande pourquoi les conservateurs traditionnels aux États-Unis délaissent l'Ukraine. Nous observons un peu la même chose au Canada. Pourquoi cela se produit-il?

Monsieur Gruzd, j'aimerais que vous nous donniez plus de détails sur les programmes d'éducation sur les médias. Ils sont extrêmement importants. Que pouvons-nous faire davantage?

M. Boucher : Je vais répondre rapidement...

Le sénateur Cardozo : Ne vous précipitez pas trop.

M. Boucher : Je parle ainsi en français comme en anglais. Je suis désolé.

Je crois qu'à l'heure actuelle, l'auditoire de croissance pour les Russes est l'extrême droite et les conservateurs. Je serais prêt à parier là-dessus. Il semble qu'à l'heure actuelle, c'est au niveau de l'extrême droite qu'ils gagnent le plus de terrain. Si nous parlions de l'Iran ou des factions parrainées par l'Iran, je parlerais de l'extrême gauche, mais en ce qui concerne la désinformation russe, c'est ce qui semble être l'écosystème. C'est en partie en raison des Américains. Les Russes ont réussi à convaincre une grande partie de l'électorat américain et des influenceurs tels que Tucker Carlson ou Marjorie Taylor Greene de croire leur discours. Malheureusement, cela a des répercussions au Canada. Nos écosystèmes sont sensiblement les mêmes. Les groupes canadiens de l'extrême droite sont intégrés aux groupes américains de l'extrême droite, et cela a de l'importance.

Cela se produit pour bien des raisons. L'une d'elles est la division. Lorsque nous effectuons des sondages sur la division, nous constatons parfois que les gens ont une relation efficace avec leur parti, et il appartient en réalité aux partis de déterminer quels messages ils vont véhiculer. Aux États-Unis, le parti s'oriente vers la droite, et les éléments du mouvement Make

have mostly gone far right. Now we're seeing that there's a rise of illiberal values of autocracy and being against pluralism in the far right, and that is concerning. The Russians find equal ways into this.

In Canada, we're starting to see that a lot. Slowly but surely, the Conservative Party — unfortunately in my province — is getting more and more influenced by the far right. It's harder and harder sometimes to know the difference, and the information ecosystems are slowly but surely starting to converge in such a way that we're having issues within those ecosystems. My sense is that what we're seeing in the U.S., we'll see in Canada — unless political leads decide otherwise.

Mr. Gruzd: The question was about media education. Before getting there, I want to briefly answer the previous question. About 51% of Canadians were exposed to pro-Kremlin information. The previous question asked us about it. I would love to give statistics based on platforms, but, unfortunately, platforms don't give us researchers the data. That's another concern I will be happy to discuss if we have time.

Going back to the media literacy program, I hear a lot from previous panels about digital literacy and the importance of critical thinking. It's true, but I don't want this to be the only take away from this committee — from these hearings — because it's putting all responsibilities on individual users. Social media platforms are very complex and are regulated by algorithms. Essentially, they're black boxes. We can't really just rely on individuals, but we need to put effort in that as well.

Regarding the generative AI's particular challenge right now to the digital literacy programs, where we see audio generated by AI, you cannot really tell whether it's authentic or not nowadays. Therefore, no matter what literacy you provide, it's impossible for the human ear to separate the two. I think that with technology, some issues can be addressed with digital literacy and for some, we would really need to talk to platforms.

Senator M. Deacon: Thank you all for being here today. Mr. Gruzd, I'm wondering if you could go back and talk a little bit more about — you said a lot very quickly on some of the pieces, which is fine — the readiness assessments you referred to.

Mr. Gruzd: The idea is that we're trying to think about who are the main targets of information operations — in this context, Russian information operations. The policy-makers, politicians

America Great Again, ou MAGA, se situent pour la plupart à l'extrême droite. On observe maintenant une montée des valeurs antilibérales de l'autocratie et de l'antipluralisme au sein de l'extrême droite, ce qui est inquiétant. Les Russes trouvent autant de moyens de s'en mêler.

Au Canada, cela s'observe de plus en plus. Lentement mais sûrement, le Parti conservateur — notamment dans ma province, malheureusement — est de plus en plus influencé par l'extrême droite. Il devient parfois de plus en plus difficile de faire la distinction, et les écosystèmes d'information commencent lentement mais sûrement à converger, si bien que des problèmes surviennent au sein de ces écosystèmes. J'ai l'impression que ce que nous observons aux États-Unis, nous l'observerons au Canada, à moins que les dirigeants politiques en décident autrement.

M. Gruzd : La question portait sur l'éducation sur les médias, mais d'abord, j'aimerais répondre brièvement à la question précédente. Environ 51 % des Canadiens ont été exposés à de l'information pro-Kremlin. Je serais ravi de donner des statistiques en fonction de chaque plateforme, mais malheureusement, les plateformes ne fournissent pas les données aux chercheurs comme nous. D'ailleurs, c'est une autre préoccupation dont je serais ravi de discuter avec vous si le temps le permet.

Je reviens au programme d'éducation sur les médias. D'autres témoins ont beaucoup parlé de littératie numérique et de l'importance de la pensée critique. C'est vrai, mais je ne veux pas que ce soit la seule chose que le comité retienne de ces témoignages, car cela place toute la responsabilité sur les épaules de l'utilisateur. Les plateformes de médias sociaux sont très complexes et sont régies par des algorithmes. Essentiellement, ce sont des boîtes noires. On ne peut simplement se fier aux particuliers, quoiqu'il fasse faire des efforts là aussi.

À l'heure actuelle, l'intelligence artificielle générative pose un défi particulier aux programmes de littératie numérique. De nos jours, lorsqu'un clip audio est généré par intelligence artificielle, on ne peut pas vraiment en confirmer ou en nier l'authenticité. Donc, on a beau éduquer les gens, il est impossible pour l'oreille humaine de faire la différence entre les deux. Je crois qu'en ce qui concerne les technologies, certains problèmes peuvent se régler au moyen de la littératie numérique, mais d'autres nécessitent que l'on discute avec les plateformes.

La sénatrice M. Deacon : Merci d'être ici aujourd'hui. Monsieur Gruzd, vous avez donné beaucoup de renseignements en peu de temps par rapport à certains aspects, ce qui est tout à fait correct, mais pourriez-vous parler un peu plus longuement des évaluations de l'état de préparation que vous avez mentionnées?

M. Gruzd : L'idée est de réfléchir à qui sont les principales cibles des opérations d'information, en l'occurrence, les opérations d'information russes. Les décideurs, les politiciens et

and civil servants would be the primary targets. My concern is that if we're only thinking about interventions for the general public, we're actually missing the most important critical group here. In my opening remarks, when I was referring to readiness assessment, I had in mind that group of individuals who actually have a strong following base online and off-line and who may retweet something accidentally — or not — and the impact will have an outsized effect.

The question that we're concerned about is the general public, but we should be focused on whether our elected officials and others are ready to be attacked by an information operation.

Senator M. Deacon: Thank you for that.

Mr. Kolga, I think we might know the answer in this room, but based on your experience and how you introduced yourself, I would be curious to know what it looked like inside Russia during the recent election.

Mr. Kolga: With regard to the information environment, it's completely sealed off. There are only a few platforms that are still able to penetrate into Russia: One is YouTube and the other is Telegram, but most Russians have been conditioned over the past 24 years to believe that the state only tells the truth and that it is surrounded by enemies, whether that is the United States, NATO or the European Union, and now inside Russia, the LGBTQ community is an enemy. So if you're inside Russia, you're surrounded by all of these enemies and you're presented with only one option of someone — an individual — who might run the government and protect you from those enemies. That's Vladimir Putin. Russians would have been bombarded with this sort of messaging and also anti-Ukrainian messaging, which one would characterize as being an incitement to hate. Russians are regularly bombarded with anti-Ukrainian messaging as well. Considering all of these things together, it's a completely different reality or parallel universe that most Russians are living in, and the state controls that. That's intentional.

Senator M. Deacon: Is there any way out?

Mr. Kolga: There is a way out. The way out is that Western democracies should come together to support independent Russian media. There's a large community that's living in Latvia right now and in Vilnius as well. Those governments are giving support to these communities. All the major independent media outlets are operating from abroad, so working with them to help penetrate that Iron Curtain with which Putin has surrounded his country is one way we can do that. Also by supporting Russian civil society organizations are also living in exile right now — supporting them and funding their work to prepare for that day when this regime will come to an end. It will come to an end one day, but now is the opportunity to support those pro-democratic

les fonctionnaires seraient des cibles de premier ordre. Je crains que si nous intervenons uniquement auprès du grand public, nous allons rater le groupe le plus important. Dans mon discours liminaire, lorsque j'ai parlé d'évaluations de l'état de préparation, je parlais de ce groupe de personnes qui ont beaucoup d'abonnés à leurs publications en ligne et que beaucoup de gens écoutent hors ligne, car s'ils republient un message, accidentellement ou pas, cela aura des effets démesurés.

La question qui nous préoccupe est le public général, mais nous devrions nous attarder sur l'état de préparation des représentants élus et d'autres s'ils devaient faire face à une opération d'information.

La sénatrice M. Deacon : Merci.

Monsieur Kolga, je crois que les sénateurs ici présents connaissent peut-être déjà la réponse, mais étant donné la manière dont vous vous êtes présenté, et d'après votre expérience, je serais curieuse de savoir quelle était la situation en Russie pendant les récentes élections.

M. Kolga : L'environnement d'information est complètement coupé du reste du monde. Seules quelques plateformes peuvent toujours pénétrer en Russie, YouTube et Telegram, mais la plupart des Russes sont conditionnés depuis 24 ans à croire que seul l'État dit la vérité, qu'il est entouré d'ennemis, qu'il s'agisse des États-Unis, de l'OTAN ou de l'Union européenne, et qu'à l'intérieur du pays, la communauté LGBTQ est un ennemi. Ainsi, si vous vous trouvez en Russie, vous êtes entouré de tous ces ennemis et on vous présente une seule option, une seule personne qui puisse diriger le gouvernement et vous protéger de ces ennemis : Vladimir Poutine. Les Russes sont bombardés de ce genre de message et de messages anti-Ukraine que l'on caractériserait d'incitation à la haine. Tout cela mis ensemble crée une réalité complètement différente. La plupart des Russes vivent dans un univers parallèle contrôlé par l'État. C'est intentionnel.

La sénatrice M. Deacon : Y a-t-il un moyen d'y remédier?

M. Kolga : Oui. La solution serait que les démocraties occidentales s'unissent pour soutenir les médias russes indépendants. Une communauté importante vit en Lettonie à l'heure actuelle, de même qu'à Vilnius. Ces gouvernements offrent un soutien à cette communauté. Tous les grands médias indépendants mènent leurs activités depuis l'étranger, alors une solution serait de collaborer avec eux pour pénétrer le rideau de fer derrière lequel Poutine isole son pays. Nous pouvons également appuyer les organismes de la société civile russes, qui vivent également en exil à l'heure actuelle. Nous pouvons les soutenir et financer leurs activités en préparation pour le jour où ce régime n'existera plus. Car, il cessera d'exister un jour, mais

forces that align with our values so they can succeed when that moment does appear.

Senator McNair: Thank you to the witnesses tonight. It's hard to be the third panel in an evening, and you've covered the topic very well and kept the interest of the group. My question is to Mr. Kolga. You talked about some of Russia's disinformation campaigns here at home trying to impact Canadian public opinion toward Ukraine. I'm curious: How does your organization measure these disinformation operations and what parameters are you using to identify whether a campaign has been successful or not?

Mr. Kolga: Thank you for that question, senator. It's very difficult to measure whether an operation has been successful, but we try to use what is called the "breakout scale," and this was proposed by an expert named Ben Nimmo a few years ago, who is now the head of Facebook's threat assessment unit.

What this basically does is to allow us to quickly assess a narrative. As soon as we see it, we can keep an eye on it and determine the impact that it could be having and is having. For example, you might take this narrative about Ukraine being a government run by neo-Nazis. Initially, that narrative would have appeared on Russian state media — a single platform — and may have appeared on some fringe platforms, but at that point we're not really too concerned about it because the impact is probably quite limited. We start to get a little bit more concerned when that breaks out to various other platforms. So it might break out from Russian state media to Twitter, Facebook or Instagram, and then we become a little more concerned and start paying closer attention to that narrative. We really start to become concerned when that narrative jumps into mainstream media. When you have TV, Canadian television, or perhaps a newspaper columnist or radio reporting on that narrative, then we become extremely concerned, especially when we have an elected official, an influencer or a major journalist who is also repeating that narrative, and that then impacting policy decisions or provoking some sort of political action. That's the scale that we look at, and when we see those narratives moving in those different phases, we determine what sort of action to take, whether to expose it or whether to address it. Nothing replaces the kind of work that my colleagues do in diving deep into data and that sort of quantitative research. But this is a quick way of — again — determining what the impact of these narratives might be and where we might be in the life cycle of those narratives.

Senator McNair: Another quick question if I may. Mr. Kolga, I'm curious to hear your thoughts briefly on the impact that disinformation is having on the Russian diaspora

en ce moment, nous avons l'occasion d'appuyer ces forces prodémocratie qui s'alignent avec nos valeurs afin qu'elles puissent prospérer le moment venu.

Le sénateur McNair : Je remercie les témoins d'être ici ce soir. Il n'est pas facile d'être le troisième groupe de témoins de la soirée. Vous avez très bien couvert le sujet et avez su maintenir l'attention du groupe. Ma question s'adresse à M. Kolga. Vous avez dit que la Russie mène des campagnes de désinformation au Canada pour tenter d'influencer l'opinion publique des Canadiens à l'égard de l'Ukraine. Je suis curieux. Comment votre organisme mesure-t-il ces opérations de désinformation et quels paramètres utilisez-vous pour déterminer si une campagne est un succès ou un échec?

M. Kolga : Je vous remercie de la question, monsieur le sénateur. Il est très difficile de mesurer si une opération est un succès, mais nous tentons d'utiliser ce qu'on appelle la « Breakout Scale » ou « échelle de propagation », laquelle a été proposée il y a quelques années par un expert nommé, Ben Nimmo, qui est aujourd'hui à la tête du service d'évaluation des risques de Facebook.

Essentiellement, cela nous permet d'évaluer rapidement un discours. Dès que nous l'apercevons, nous le surveillons et déterminons l'impact qu'il pourrait avoir et qu'il a. Prenons par exemple, le discours selon lequel le gouvernement de l'Ukraine serait dirigé par des néonazis. Initialement, ce discours serait apparu dans un média d'État russe — une seule plateforme — et a peut-être été observé sur certaines plateformes marginales, mais alors, il ne nous préoccupe pas trop parce que l'impact est probablement assez limité. Il nous préoccupe un peu plus lorsqu'il se propage à d'autres plateformes. En effet, lorsque le discours qui s'observait sur un média d'État russe se retrouve sur Twitter, Facebook ou Instagram, cela devient un peu plus préoccupant, et nous commençons donc à le surveiller de plus près. Nous devenons très préoccupés lorsque ce discours fait le saut vers les médias traditionnels. Lorsque ce discours est repris par la télévision canadienne ou par un chroniqueur dans un journal ou par une chaîne de radio, cela devient extrêmement préoccupant, surtout lorsqu'un représentant élu, un influenceur ou un journaliste important le répète et que cela a une incidence sur les décisions stratégiques ou provoque une intervention politique quelconque. Voilà l'échelle que nous utilisons, et lorsque nous voyons ces discours progresser d'une phase à l'autre, nous déterminons quel genre de mesure prendre, si nous l'exposons au grand jour ou si nous tentons de le combattre. Rien ne remplace le genre de travail que font mes collègues en analysant à fond les données et en effectuant ce genre de recherche quantitative. Toutefois, comme je l'ai dit, c'est une façon rapide de déterminer quel pourrait être l'impact de ces discours et à quelle étape de leur cycle de vie ils en sont.

Le sénateur McNair : J'ai une autre brève question, si je puis. Monsieur Kolga, quelles sont, selon vous, les conséquences de cette désinformation pour la diaspora russe au Canada. Je

here in Canada. I understand there are still some streaming services that are giving Russian air time to state media. Are you concerned about this?

Mr. Kolga: I'm extremely concerned about that. There are 500,000 individuals in Canada who identify as Russians. The Canadian government has done a good job of sanctioning all Russian state media. We've also banned Russian state media from our public airwaves. It's still available, unfortunately, online, but it's also available through streaming services that are based in Canada. These are services that are like Amazon Fire Stick or Roku. Basically, you can go to a shop in Toronto, buy a little device that has a USB connector behind it, and plug that into your television. You pay $12 or $15 a month, and this allows viewers to stream all Russian state media into their homes. There was a report recently published in *The Logic* by a journalist named Martin Patriquin, in which he interviewed a well-known Russian-speaking journalist here in Canada, Alla Kadysh, who estimated that at least one third of Russian homes in Canada use this service. That means that one third of those Canadians are being exposed to the extremely toxic Russian state media that is being pumped into the minds of Russians on a daily basis. This includes those incitement to hate against Ukraine, among other narratives. So I'm very concerned about these services, and I wonder if there's any violation of our sanctions in terms of these organizations generating revenue from rebroadcasting Russian state media. I think the government and our authorities need to take a very close look at these services and whether they're compliant at all with our laws.

[*Translation*]

Senator Carignan: Mr. Boucher, in 2022, you did a study on propaganda, particularly on Twitter. In short, 75% of this propaganda was pro-Ukrainian and 25% was pro-Russian. So it was 35% content, even though 25% of the tweets were pro-Russian.

Has the situation changed? What is the Canadian government doing to resolve the situation, or at least to lessen its impact? In your 2022 article, you were quite critical of the Canadian government, talking about what it wasn't doing, or rather what it should be doing.

I'd also like to hear what you have to say about the fact that a prime minister said that foreign interference in the elections wasn't serious, that only a few MPs lost their jobs, but that it didn't change the result in terms of the government that was elected.

Mr. Boucher: I'll go slowly. What's interesting is that when we did this study in 2022, the war was in its first few months; we knew nothing about the ecosystem and we didn't know how the

crois savoir que des services de diffusion en continu accordent toujours du temps d'antenne aux médias d'État russes. Cela vous préoccupe-t-il?

M. Kolga : Cela me préoccupe énormément. Quelque 500 000 personnes au Canada s'identifient comme étant Russes. Le gouvernement canadien a fait du bon travail en imposant des sanctions à tous les médias d'État russes. Nous avons également banni ces derniers de nos ondes publiques. Malheureusement, ils sont toujours accessibles en ligne, mais ils le sont également par la voie de services de diffusion en continu situés au Canada, comparables à l'Amazon Fire Stick ou à Roku. Essentiellement, on peut aller dans une boutique de Toronto, acheter un petit dispositif doté d'un connecteur USB et brancher celui-ci à son téléviseur. Pour 12 $ ou 15 $ par mois, le téléspectateur peut visionner en continu tous les médias d'État russes dans son salon. Dans un article publié récemment dans *Logic*, le journaliste Martin Patriquin a interviewé, ici au Canada, Alla Kadysh, une journaliste connue qui parle russe. Celle-ci estime qu'au moins le tiers des foyers russes au Canada utilisent ce service. Cela signifie que le tiers de ces Canadiens sont exposés au contenu extrêmement toxique que les médias d'État russes injectent quotidiennement dans l'esprit des Russes, dont les messages d'incitation à la haine contre l'Ukraine. Je suis donc très préoccupé par ces services, et je me demande s'ils ne vont pas à l'encontre de nos sanctions, puisque ces organismes génèrent un revenu en rediffusant les médias d'État russes. Je crois que le gouvernement et nos autorités doivent examiner de près ces services et déterminer s'ils sont même conformes à nos lois.

[*Français*]

Le sénateur Carignan : Monsieur Boucher, en 2022, vous avez fait une étude sur la propagande, particulièrement sur Twitter. En résumé, 75 % de cette propagande était pro-ukrainienne et 25 % était prorusse. C'était donc 35 % de contenu, même si 25 % des gazouillis étaient prorusses.

Est-ce que la situation a évolué? Qu'est-ce que le gouvernement canadien fait pour régler la situation, ou du moins pour en diminuer l'impact? Dans votre article de 2022, vous étiez assez critique par rapport au gouvernement canadien, en parlant de ce qu'il ne faisait pas ou plutôt de ce qu'il devrait faire.

J'aimerais également vous entendre sur le fait qu'un premier ministre a mentionné que l'ingérence étrangère sur le vote n'était pas grave, qu'il y a seulement quelques députés qui ont perdu leur poste, mais que cela n'a pas changé le résultat du gouvernement élu.

M. Boucher : Je vais y aller doucement. Ce qui est intéressant, c'est que lorsqu'on a fait cette étude en 2022, c'était les premiers mois de la guerre; on ne connaissait rien de

situation would develop — my colleague, Mr. Kolga, also worked on this.

Today, it's much the same. The players we identified then are the same as they are today. They are exactly the same. It's quite astonishing and it surprised us. Every year it's the same people, we know them and we know what they're going to say.

This has given us a better understanding of the ecosystem. In my opinion, today, the far-left ecosystem has not grown and is starting to work more on in-depth stories about Iran and anti-Semitic groups. However, the far right continues to grow; in a way, I'm under the impression that this small 25% is a little stronger and more important today.

The second question concerned the measures being taken by the Canadian government to resolve the situation. I remain just as critical. Frankly, the Canadian government and its civil servants are working very hard and they are competent. It amazes me how seriously they take their work in all the departments, such as Global Affairs Canada, National Defence and the Privy Council. However, they don't have the tools or the policies to help them do anything.

What emerges from my conversations with people at Global Affairs Canada is that they want to provide answers. Yes, but answers about what, how and where? In reality, they're not really doing that. Despite two years of war, events have occurred with the government of India, Iran, Hamas and China. There is a whole host of players who are interfering and polluting our information space and trying to influence our fellow citizens, but there's no real response from the Canadian government.

What worries me a lot is that when I have conversations about the 2025 election, it's not clear whether Canada has a plan and whether it knows what to do. As Mr. Gruzd was saying, the tools that are being developed today, such as deepfakes or generative artificial intelligence, both in audio/video and in text, will be four times more effective in a year's time.

This is the year of the big test. Everyone talks about the four billion people who will take part in elections, but that's not so important; what's important are the 300 million voters who will cast their ballots in the United States. All the players will be putting their resources into trying to influence this group, because they are the ones who will have the greatest impact on the war in Ukraine. This means that for a year, they will be testing all the artificial intelligence and generative artificial intelligence tools.

l'écosystème et on ignorait comment la situation se développerait — mon collègue M. Kolga a travaillé là-dessus lui aussi.

Aujourd'hui, c'est à peu près la même chose. Les acteurs qu'on a identifiés à l'époque sont les mêmes qu'aujourd'hui. Ce sont exactement les mêmes. C'est assez étonnant et cela nous a surpris. Chaque année, ce sont les mêmes personnes, on les connaît et on sait ce qu'elles vont dire.

Cela nous a permis d'avoir une meilleure compréhension de l'écosystème. À mon avis, aujourd'hui, l'écosystème de l'extrême gauche n'a pas grossi et il commence à travailler davantage sur des récits plus poussés au sujet de l'Iran et des groupes antisémites. Cependant, l'extrême droite continue de grandir; d'une certaine façon, j'ai l'impression que ce petit 25 % est un peu plus fort et important aujourd'hui.

La deuxième question était la suivante : que fait le gouvernement canadien? Je reste tout aussi critique. Franchement, le gouvernement canadien et les fonctionnaires travaillent très fort et ils sont compétents. Cela m'étonne de voir à quel point ils prennent leur travail au sérieux dans tous les ministères, comme Affaires mondiales Canada, la Défense nationale et le Conseil privé. Toutefois, ils n'ont ni les outils ni les politiques nécessaires pour les aider à faire quoi que ce soit.

Les conversations que j'ai avec les gens d'Affaires mondiales Canada, c'est qu'on veut donner des réponses. Oui, mais des réponses sur quoi, comment et où? Dans les faits, on ne le fait pas vraiment. Malgré deux ans de guerre, des événements se sont produits avec le gouvernement de l'Inde, l'Iran, le Hamas et la Chine. Il y a plein d'acteurs qui s'immiscent et polluent notre espace informationnel et tentent d'influencer nos concitoyens, mais il n'y a pas vraiment de réponse du gouvernement canadien à cet effet.

Ce qui m'inquiète beaucoup, c'est que lorsque j'ai des conversations sur les élections de 2025, ce n'est pas clair si le Canada a un plan et s'il sait quoi faire. Comme le disait M. Gruzd, les outils qui se développent aujourd'hui, comme le *deepfake* ou l'intelligence artificielle générative, tant qu'en audio et en vidéo qu'en texte, seront quatre fois plus efficaces dans un an.

Cette année, c'est celle du grand essai. Tout le monde parle de 4 milliards de personnes qui participeront à des élections, mais ce n'est pas si important; ce qui est important, ce sont les 300 millions d'électeurs qui voteront aux États-Unis. Tous les acteurs vont mettre les ressources requises pour essayer d'influencer ce groupe, parce que ce sont eux qui auront le plus d'impact sur la guerre en Ukraine. Cela veut dire que pendant un an, ils vont tester tous les outils d'intelligence artificielle et d'intelligence artificielle générative.

When the 2025 elections are held in Canada, we'll end up with a group that will have spent a year training to try to manipulate the information space in the United States, and we'll still be there. I know that people in the Canadian government are very serious and concerned about this event, but I can't see any plans or manpower yet. The teams at Global Affairs Canada are very small. There are three or four people working very hard, but managing 83 files; they spend their time briefing ministers and coordinating people within departments. At the end of the day, there isn't really a program that's put forward to say, "Here's what's being done and how we're doing it. Here's what we're doing and how we're measuring it". I think that's a problem.

The feedback I get from inside government is that everyone thinks it's a problem. The Prime Minister says it's not serious. I think he's wrong. I think all political parties in Canada should unanimously criticize any interference from anyone, be it the far right, the Russians, the Chinese, the Iranians or the Indians. Canadians have the right to decide their future between themselves, and the Canadian government and all political parties should make this a position of principle, and say that they don't care whether the interference comes from the United States, the far left or the far right, they have to protect Canada's cognitive space.

I disagree with the Prime Minister. I also disagree with the Conservatives, who are a bit indolent in the face of the extreme right coming from the Americans. They think, "Well, are we going to do anything about that?" Yes, what's good for the Liberals is good for the New Democrats and the Conservatives. I think that as a society, we have to tackle the problem.

[*English*]

Mr. Kolga: A couple of very brief comments. As far as the far left is concerned, Russia is truly exploiting this group. They are advancing anti-NATO narratives, anticolonialism narratives and they're also picking up Russian narratives which blame Ukraine for starting this war that they are prolonging the suffering of Ukrainians. This is having an impact on mainstream debate about what to do with Ukraine, whether that's to impose peace or to continue supplying weapons. They're coming at it from a different angle, and it is clearly having an impact. I think we've all heard those narratives in mainstream media.

What Canada should be doing, I completely agree with all of Mr. Boucher's comments. I would only say that the Europeans are doing a lot on our behalf with the Digital Services Act. This is holding those large social media companies to account. Maybe what we should be doing is looking at how we can support that European effort.

Lorsque les élections de 2025 se tiendront au Canada, on se retrouvera avec un groupe qui passera un an à s'entraîner pour essayer de manipuler l'espace informationnel aux États-Unis et on en sera encore là. Je sais que les gens au gouvernement canadien sont très sérieux et concernés par cet événement-là, mais je ne vois pas encore de plan ni d'effectifs. Les équipes d'Affaires mondiales Canada sont toutes petites. Ce sont trois ou quatre personnes qui travaillent très fort, mais qui gèrent 83 dossiers; ils passent leur temps à breffer les ministres et à coordonner les gens au sein des ministères. Au final, il n'y a pas vraiment de programme qui est mis de l'avant pour dire : « Voici ce qui se fait et comment on le fait. Voici nos actions et comment on les mesure. » Je pense que c'est un problème.

Les échos que j'ai de l'intérieur du gouvernement, c'est que tout le monde pense que c'est un problème. Le premier ministre dit que ce n'est pas grave. Je pense qu'il a tort. Je pense que tous les partis politiques au Canada devraient critiquer unanimement toute ingérence de qui que ce soit, que ce soit l'extrême droite, les Russes, les Chinois, les Iraniens ou les Indiens. Les Canadiens ont le droit de décider de leur avenir entre eux et le gouvernement canadien et tous les partis politiques confondus devraient en faire une position de principe, c'est-à-dire que l'on se fout d'où vient l'ingérence — que cela vienne des États-Unis, de l'extrême gauche ou de l'extrême droite, il faut protéger l'espace cognitif du Canada.

Je suis en désaccord avec lui. J'ai la même conversation que les conservateurs, qui sont un peu indolents face à l'extrême droite qui vient des Américains. Ils se disent : « Bof, est-ce qu'on va faire quelque chose pour cela? » Oui, ce qui est bon pour les libéraux est bon pour le NPD et les conservateurs. Je pense que comme société, il faut s'attaquer au problème.

[*Traduction*]

M. Kolga : J'aurais quelques observations à formuler brièvement. La Russie exploite réellement l'extrême droite. Cette dernière promeut les discours anti-OTAN et anticolonialisme et répète les discours russes qui accusent l'Ukraine d'avoir déclenché cette guerre et de prolonger la souffrance des Ukrainiens. Cela a des répercussions sur le débat de la majorité à savoir que faire à propos de l'Ukraine, que ce soit imposer la paix ou continuer de fournir des armes. On présente la chose sous un angle différent et cela a manifestement des répercussions. Je crois que nous avons tous entendu ces discours dans les médias traditionnels.

En ce qui concerne ce que doit faire le Canada, je suis entièrement d'accord avec M. Boucher. J'ajouterais simplement que les Européens font beaucoup pour nous au moyen de leur législation sur les services numériques. Cette dernière exige des comptes des grandes entreprises de médias sociaux. Peut-être devrions-nous examiner comment nous pouvons soutenir ces efforts de l'Europe.

I do want to comment on Global Affairs' Rapid Response Mechanism; it is very effective. I speak to European colleagues all the time, elected officials. They all comment on the effectiveness of RRM in spreading that information, awareness of some of these narratives. So it is doing very good work. What we really need to be doing is working more closely with civil society because civil society is nimble. It can do that work of exposing those narratives so that there is greater awareness. So more work with civil society is definitely needed.

J'aimerais parler du Mécanisme de réponse rapide d'Affaires mondiales. Il est très efficace. Je m'entretiens constamment avec des collègues européens, des représentants élus, et ils me parlent tous de l'efficacité du mécanisme pour diffuser l'information et sensibiliser nos alliés à certains de ces discours. Donc, il fait du bon travail. Nous devons collaborer plus étroitement avec la société civile, car celle-ci est flexible et capable de s'adapter et d'intervenir rapidement. Elle peut dénoncer ces discours pour sensibiliser la population. Il faut absolument collaborer davantage avec elle.

Senator Yussuff: Thank you, witnesses, for being here.

Le sénateur Yussuff : Je remercie les témoins de leur présence.

I'll take you back a bit. Not in the context of Ukraine but, as you know, we went through the pandemic and as we saw that a significant portion of the population that didn't believe in vaccination were disruptive. In time, they disrupted what would be the norm as to how society would respond to a major crisis on something that was so fundamental for many of us. Of course, they use all the tools you were talking about. This is here; this is not Russia. This is our own folks. Where they got the information from and how they spread it was extremely disruptive. We're now looking at it on a larger scale, how malicious actors, state and individuals are posing a major challenge in terms of how democracy can function, including the point that Mr. Boucher made on foreign interference.

Revenons un peu en arrière. Je ne parle pas de l'Ukraine, mais de la pandémie. Comme vous le savez, le fait qu'une portion importante de la population ne croit pas aux bienfaits de la vaccination a causé des perturbations. Cela a perturbé la façon dont la société interviendrait normalement en réponse à une crise majeure. Le mouvement anti-vaccin a attaqué une chose qui, pour beaucoup d'entre nous, est fondamentale. Bien entendu, il a utilisé tous les outils dont vous avez parlé. Cela s'est passé ici, au Canada, et pas à cause de la Russie. C'était l'œuvre de nos propres concitoyens. La source de leur information et la manière dont ils l'ont propagée étaient extrêmement perturbatrices. Nous étudions maintenant la chose à plus grande échelle. Nous constatons que les acteurs, les États et les particuliers malveillants représentent une menace importante pour le fonctionnement de la démocratie. Cela comprend l'ingérence étrangère dont a parlé M. Boucher.

What can we learn from what other countries are doing? Despite the fact this has been with us for some time, Liberal democracies haven't found a proper way in how we can address this and build consensus among citizens. Some people will find any interruption of their ability to have disinformation as part of their lives and other information is their right and you shouldn't restrict them in any way. You have social platforms that on a day-to-day basis have no screens in regard to what you can see or be influenced by.

Quelle leçon pouvons-nous tirer de l'étranger? Même si cette menace n'est pas nouvelle, les démocraties libérales n'ont toujours pas trouvé de solution adéquate pour la combattre et établir un consensus parmi les citoyens. Certaines personnes s'opposent à toute atteinte à ce que la désinformation comme l'information puisse faire partie de leur vie. Ils considèrent qu'ils ont le droit d'y avoir accès et qu'elles ne doivent faire l'objet d'aucune restriction. Des plateformes de médias sociaux ne filtrent aucunement ce que nous pouvons voir ou ce qui peut nous influencer au quotidien.

To put it in context, if we're going to deal with this in a meaningful way as a country, it would seem to me we should learn from somebody else, but I don't know of anybody else I can point to with any significant confidence that they are better than us, other than they are trying extremely hard. There's been some international coordination, to be fair. I think it's been the subject of G7 meetings in other places, but we haven't found a proper solution how we're going to deal with it.

Selon moi, pour combattre efficacement le problème, le Canada devrait s'inspirer des pratiques exemplaires à l'étranger. Or, je ne saurais nommer un pays qui gère la situation assurément mieux que nous. Certes, certains déploient des efforts considérables. Il faut également reconnaître que des efforts de coordination s'effectuent à l'échelle internationale. Je crois que le G7 a tenu des réunions à ce sujet. Quoi qu'il en soit, nous n'avons toujours pas trouvé de solution adéquate.

In the meantime, the people who are extremely good at disrupting our lives in a meaningful way are not stopping their actions. What can be learned and are we really looking at a challenge we have to understand as to how we can best deal with it, other than bring in legislation to restrict certain ways in how

Pendant ce temps, les gens qui excellent à perturber considérablement notre vie poursuivent leurs activités. Quelles leçons pouvons-nous tirer de l'étranger? Pour combattre le problème, nous devons comprendre la meilleure façon de le gérer, et je crois que la société canadienne, et encore moins nos

people will receive information, which I think society is not prepared for that, not in this country much less the neighbour beside us?

Mr. Boucher: The first part is a lot of people are making money at spreading disinformation. There's a fundamental right to be able to express your views and beliefs. There might not be one of making money out of it. I think we can regulate some of this or at least make this more transparent. If you are an influencer or you have a website, your sources funding should be transparent. Who gives you the money, like through GoFundMe? I think that would shed a lot of light in terms of understanding who is spending millions of dollars to spread their views.

The anti-vaccine movement was not just a couple of blokes who had views about the vaccines. They were corporations and groups that spent millions of dollars to advance their ads and tried to convince others to do so.

The anti-LGBTQ narrative is not just a couple of concerned citizens. It's actually groups that are backed through money from the U.S. that spend millions of dollars to promote their views to Canadians.

We can tackle that part. Not police speech but police amplification. You have a right to say whatever you want. You don't have the right to spend a lot of money on it. Or if you do, it should be transparent. You want to spread an anti-vaccine narrative? Who funds you? This billionaire or millionaire from this thing. It's legal, but at least it gives you a better understanding of the space.

The second part is that there are other states that are doing this somewhat as a group. I'm thinking of the Australians, who have set up what they call an ASPI, or Australian Strategic Policy Institute, which is a group that is funded through either the Department of National Defence or Public Safety. They're really good at tackling disinformation, especially with China. We have nothing like this in Canada. They have been very effective, and some of the work they do actually helped us. The "Spamouflage" on public figures from China was their information. We could learn from this and spend that kind of money.

The last part is that we've learned a lot that fact checking actually doesn't work. Much of the research, data and the work we've done on fact checking, all demonstrate that fact checking does not work. If we think it works, it doesn't stick. If we think it works, it actually makes other people more entrenched in their views.

voisins du sud, ne sont pas prêts à ce qu'on restreigne, par la voie législative, la manière dont les gens peuvent recevoir l'information.

M. Boucher : Premièrement, beaucoup de gens profitent de la diffusion de désinformation. Il existe un droit fondamental d'exprimer son point de vue et ses croyances, mais en tirer un revenu ne constitue pas un droit. Je crois que nous pouvons réglementer certains aspects ou, à tout le moins, accroître la transparence. Si vous êtes un influenceur ou que vous avez un site Web, vous devriez divulguer vos sources de financement en toute transparence. Qui vous a donné de l'argent par la voie de GoFundMe, par exemple? Je crois qu'exposer cela au grand jour aiderait beaucoup à comprendre qui dépense des millions de dollars pour propager ces opinions.

Le mouvement anti-vaccination n'était pas simplement quelques personnes ayant une certaine opinion à l'égard des vaccins. Il s'agissait de sociétés et de groupes qui ont dépensé des millions de dollars en publicité pour tenter de rallier d'autres gens à leur cause.

Le discours anti-LGBTQ n'est pas simplement quelques citoyens préoccupés. Ce sont en fait des groupes parrainés par les États-Unis qui dépensent des millions de dollars pour faire valoir leurs opinions auprès des Canadiens.

Nous pouvons nous attaquer à cet aspect. Non pas en censurant le discours, mais en limitant l'amplification. Chacun a le droit de dire ce qu'il veut, mais pas de dépenser beaucoup d'argent pour diffuser cette opinion à grande échelle. Quiconque le fait doit le faire en toute transparence. Vous voulez propager un discours anti-vaccination? Qui vous finance? Ce milliardaire ou ce millionnaire associé à tel groupe ou à telle société ou à tel mouvement. Ainsi, la pratique demeure légale, mais à tout le moins, on comprend mieux le contexte.

Deuxièmement, certains États travaillent en quelque sorte à cela en groupe. Par exemple, les Australiens ont mis sur pied l'Australian Strategic Policy Institute ou institut de politique stratégique de l'Australie, qui est financé soit par le ministère de la Défense nationale, soit par celui de la Sécurité publique, et qui combat très bien la désinformation, en particulier celle qui provient de la Chine. Le Canada n'a pas d'équivalent. Cet organisme australien est très efficace. D'ailleurs, le travail qu'il fait nous aide parfois. C'est lui qui nous a fourni l'information concernant les campagnes de « spamouflage » de la Chine concernant des personnalités publiques. Nous pouvons suivre cet exemple et investir dans un organisme comparable.

Troisièmement, nous avons appris que vérifier les faits ne fonctionne pas. C'est ce qui ressort de la plupart des données que nous avons recueillies et de la plupart des études et des travaux que nous effectuons. Lorsqu'elle fonctionne, le résultat est éphémère, mais la plupart du temps, elle ne fait que renforcer l'opinion des gens.

We think now that pre-bunking is the most effective way to combat misinformation and disinformation, but I haven't seen a lot of good pre-bunking narratives or ways of doing this. We can spend a lot of time and effort in the coming years to do that and see if it's effective in combatting disinformation.

Mr. Gruzd: We can learn a lot from COVID-19 misinformation and interventions that we implemented across various sectors in our society.

Starting with the platforms, they quickly put labels up. Every time there's a message related to the COVID-19 virus, vaccines or future vaccines, there is a link directly to Health Canada, where we can find credible information.

Social media platforms invested into fact checking. I disagree with my colleague; they do work. But studies do show that it does not necessarily translate into a long-term effect.

Fact checking false and misleading claims were implemented across many platforms. We've also seen how YouTube — related to the previous comment — demonetized anti-vaccination videos. We saw that YouTube users immediately started to recommend more pro-vaccine videos than anti-vaccine videos. This is based on our own study.

There are a lot of things we can learn. Things that I list here are what platforms implemented during those times, and mostly on a volunteer basis. When there was no societal pressure, they quickly stopped continuing those efforts across their platforms. Labelling and fact checking disappeared. What remains as potentially still good are the political ad transparency initiatives, where we can actually see who is spending money on which ads, related to politics during elections and issues of significance.

I think we can learn a lot from the COVID period. The question is why those efforts are not sustained. You can see there are different stakeholders in our society that have dropped the ball now and we can re-energize them.

Mr. Kolga: I would say that freedom of expression does not mean freedom from scrutiny. When we have these actors who are spreading disinformation, they need to be exposed. I think that, as a society, we're afraid of doing that. We need to learn from our allies in Europe who do this effectively — expose the platforms and the individuals who are spreading those narratives.

À l'heure actuelle, on estime que la démystification préventive est le moyen le plus efficace de combattre la mésinformation et la désinformation, mais je vois peu de bons discours de démystification préventive ou de bonnes façons de diffuser ces derniers. Nous pouvons consacrer beaucoup de temps et d'efforts à cette fin dans les prochaines années et voir si c'est un moyen efficace de combattre la désinformation.

M. Gruzd : Nous pouvons tirer de nombreuses leçons de la pandémie de COVID-19 en matière de mésinformation ainsi que des mesures d'intervention que nous avons prises dans divers secteurs de notre société.

D'abord, pour ce qui est des plateformes, on a rapidement appris à identifier les sources d'information. Chaque fois qu'on publie un message lié au virus de la COVID-19 ou à de futurs vaccins, on insère un lien menant directement à Santé Canada, où l'on peut trouver de l'information crédible.

Les plateformes de médias sociaux ont investi dans la vérification des faits. Je ne suis pas d'accord avec mon collègue; elles font des efforts. Toutefois, les études montrent effectivement que ces efforts ne donnent pas nécessairement de résultats à long terme.

De nombreuses plateformes ont instauré la vérification des faits pour dénoncer les affirmations fausses ou induisant en erreur. Nous avons également vu que YouTube — dont nous avons parlé précédemment — a démonétisé les vidéos anti-vaccination. Immédiatement, les utilisateurs de YouTube se sont mis à recommander davantage de vidéos pro-vaccination que de vidéos anti-vaccination. C'est ce que notre étude a démontré.

Nous pouvons tirer de nombreuses leçons. Je mentionne les mesures prises, la plupart du temps volontairement, par les plateformes pendant la pandémie. Lorsque les pressions sociétales ont cessé, les plateformes ont rapidement mis fin à ces efforts. L'identification des sources et la vérification des faits ont disparu. Un élément potentiellement positif qui demeure, ce sont les initiatives pour la transparence relativement aux publicités politiques, grâce auxquelles nous pouvons voir qui finance quelles publicités à des fins politiques pendant les campagnes électorales et concernant les dossiers importants.

Je crois que nous pouvons beaucoup apprendre de la pandémie de COVID-19. La question est de savoir pourquoi ces efforts n'ont pas été maintenus. On constate que divers intervenants dans notre société ont abandonné la cause et nous pouvons les motiver à renouveler leurs efforts.

M. Kolga : Selon moi, liberté d'expression ne signifie pas exemption de tout examen. Il faut dénoncer les acteurs qui propagent de la désinformation. Je crois que, en tant que société, nous avons peur de le faire. Nous devons suivre l'exemple de nos alliés européens, qui dénoncent efficacement les plateformes et les particuliers qui propagent ce genre de discours.

Foreign governments such as Russia, China and Iran have no right to express themselves in our country. They have no right to violate our cognitive sovereignty or the sovereignty of our information space. They should be blocked whenever possible. We should, again, learn from our European allies, who have completely blocked them out of the European information space.

Who is doing this well? The European Union is doing it well. EUvsDisinfo is a wonderful platform that combines debunking and fact checking, but it adds contextualization to those narratives. When you're reading it, you understand why these foreign governments are exploiting certain narratives and who they're targeting with them.

I also think fact checking is important for our journalists and our newsroom managers, who are actually looking for that information. Have that information exposed online somehow, as we do on DisinfoWatch — we find it's useful and we know that media does use that service.

Senator Dasko: My question was what our witnesses think should be done, so I feel that's been well answered.

I do have a small question for Professor Gruzd. You said you had done some research and that 51% of Canadians have seen Russian narratives. You didn't ask the question: Have you seen a Russian narrative? You asked about the narratives, right? What were some of the narratives you asked people about?

Mr. Gruzd: We've conducted a couple of national surveys like this. Every time we ask Canadians about the types of narratives they've seen across different social media platforms, we look around and see what's currently trending, what are the narratives we observe as researchers through the data. During that survey, there were narratives about who is to blame. Whether you blame Ukraine for starting the war, so they caused it; whether NATO caused it, the expansion of NATO; the Nazi claim that Ukrainian nationalism is a neo-Nazi movement — those are common narratives that we've observed.

Senator Dasko: So 51% of Canadians have seen one of these narratives, but the number who believed them would be more in the 20% that Professor Boucher has talked about; right?

Mr. Gruzd: Yes. We then followed up to ask to what extent — because it is a range; it is not, do you believe or not, but to what extent do you believe those narratives? That NATO expansion caused Russia to attack in order to defend themselves was the most believable claim in Canada. But around 30% of

Les gouvernements comme ceux de la Russie, de la Chine et de l'Iran n'ont aucun droit de s'exprimer dans notre pays. Ils n'ont aucun droit de porter atteinte à notre souveraineté cognitive ou à la souveraineté de notre environnement d'information. Il faut les bloquer autant que possible. Encore une fois, nous devons suivre l'exemple de nos alliés européens, qui les ont complètement bloqués de leur environnement d'information.

Qui a des pratiques exemplaires? L'Union européenne réussit bien. EUvsDisinfo est une merveilleuse plateforme qui combine la démystification et la vérification de faits, en plus de mettre en contexte ces discours. Quand on la consulte, on comprend pourquoi ces gouvernements étrangers exploitent certains discours et qui sont leurs cibles.

Je crois également que la vérification des faits est importante pour les journalistes et les gestionnaires des salles de nouvelles, qui recherchent en fait cette information. Dénonçons cette information en ligne, comme le fait DisinfoWatch. Nous estimons que c'est utile et nous savons que les médias utilisent bel et bien ce service.

La sénatrice Dasko : Ma question visait à savoir quelles mesures devraient être prises, selon les témoins, et j'estime qu'ils y ont bien répondu.

J'ai toutefois une petite question supplémentaire pour le professeur Gruzd. Vous avez dit avoir réalisé un sondage et que, d'après les résultats, 51 % des Canadiens auraient vu les discours propagés par la Russie. Vous n'avez pas demandé aux gens s'ils avaient vu des discours propagés par la Russie; vous leur avez demandé s'ils avaient vu tel ou tel message, n'est-ce pas? Quels messages avez-vous demandé aux gens s'ils les avaient vus?

M. Gruzd : Nous avons effectué quelques sondages nationaux de ce genre. Chaque fois que nous demandons aux Canadiens quels genres de discours ils ont vus dans diverses plateformes de médias sociaux, nous nous fondons sur les tendances actuelles, sur les discours que nous observons en tant que chercheurs dans les données que nous analysons. Lorsque nous avons réalisé ce sondage, des discours circulaient à savoir qui est responsable de la guerre en Ukraine : l'Ukraine l'a déclenchée, et donc en est la cause; l'OTAN ou l'expansion de l'OTAN en est la cause; l'affirmation nazie selon laquelle le nationalisme ukrainien est un mouvement néo-nazi. Ce sont des discours courants que nous observons.

La sénatrice Dasko : Donc 51 % des Canadiens ont vu l'un de ces discours, et d'après le professeur Boucher, environ 20 % ont cru ces messages. C'est bien cela?

M. Gruzd : Oui. Le sondage demandait ensuite aux répondants dans quelle mesure ils avaient cru ces messages. Ce n'est pas un simple oui ou non, il y a une échelle. Le discours selon lequel l'expansion de l'OTAN a amené la Russie à attaquer l'Ukraine pour se défendre est celui qui est considéré comme

Canadians believe that the Ukrainian nationalism movement is neo-Nazi.

Those are concerning numbers. Of course, this is a scale and we might not reach with our interventions those who extremely believe in that, but we certainly need to address the rest of it.

Senator Dasko: Thank you.

The Chair: Colleagues, this brings us to the end of our panel and the end of today's meeting. I want to extend sincere thanks to Mr. Boucher, Mr. Gruzd and Mr. Kolga for, at this late hour, keeping all of our attention right to the last minute. These discussions have been fulsome, thought-provoking and concerning. There has been an alarm call for stronger reactive strategies. You could all tell the high degree of interest in this room. We thank you very much for contributing to a very important discussion.

Colleagues, our next meeting will be on Monday, April 29, at 4 p.m. eastern, when we will be chatting about tensions in the Middle East.

Thank you again for your participation here today. I wish you all a good evening.

(The committee adjourned.)

étant le plus crédible au Canada. Cependant, environ 30 % des Canadiens croient que le mouvement nationaliste ukrainien est néo-nazi.

Ces statistiques sont inquiétantes. Évidemment, on parle d'une échelle, et il se peut que les personnes qui croient tout à fait à ces discours ne participent pas à nos sondages. Cela dit, nous devons certainement intervenir à l'égard du reste.

La sénatrice Dasko : Merci.

Le président : Chers collègues, cela met fin aux témoignages de ce groupe de témoins ainsi qu'à la réunion d'aujourd'hui. Je tiens à remercier sincèrement M. Boucher, M. Gruzd et M. Kolga d'avoir su capter notre attention jusqu'à la dernière minute, malgré l'heure tardive. Ces discussions approfondies donnent matière à réflexion et sont préoccupantes. On sonne l'alarme et réclame des stratégies d'intervention plus rigoureuses. Vous avez tous pu constater le niveau d'intérêt élevé dans la salle. Merci beaucoup d'avoir contribué à cette très importante discussion.

Chers collègues, notre prochaine réunion aura lieu le lundi 29 avril, à 16 heures, heure de l'Est. Nous y discuterons des tensions au Moyen-Orient.

Encore une fois, je vous remercie de votre participation aujourd'hui. Je souhaite à tous une bonne soirée.

(La séance est levée.)