EVIDENCE

OTTAWA, Monday, March 20, 2023

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 Jean-Guy Dagenais (*Deputy Chair*) in the chair.

[*Translation*]

The Deputy Chair: Welcome to this meeting of the Standing Senate Committee on National Security, Defence and Veterans Affairs. I am Jean-Guy Dagenais, senator from Quebec and deputy chair of the committee. Unfortunately, our chair, Senator Tony Dean, could not join us today. I invite my colleagues to introduce themselves, starting on my left.

Senator Cardozo: Andrew Cardozo, Ontario.

[*English*]

Senator Dasko: Donna Dasko, from Ontario.

[*Translation*]

Senator Boisvenu: Pierre-Hugues Boisvenu, from La Salle, Quebec.

[*English*]

Senator Yussuff: Hassan Yussuff, Ontario.

Senator Boehm: Peter Boehm, Ontario.

[*Translation*]

The Deputy Chair: Thank you, colleagues. For those of you watching live from across Canada, I would like to remind you that today we are focusing on cyber threats to Canada's defence infrastructure. We have three distinguished panels with us today. We'll get started immediately.

For our first panel of witnesses, we are pleased to welcome, from the Communications Security Establishment, Mr. Sami Khoury, Head, Canadian Centre for Cyber Security, and Mr. Daniel Couillard, Director General, Partnerships and Risk Mitigation, Canadian Centre for Cyber Security.

TÉMOIGNAGES

OTTAWA, le lundi 20 mars 2023

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, afin d'examiner, pour en faire rapport, les questions concernant la sécurité nationale et la défense en général.

Le sénateur Jean-Guy Dagenais (*vice-président*) occupe le fauteuil.

[*Français*]

Le vice-président : Bienvenue à cette réunion du Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants. Je suis Jean-Guy Dagenais, sénateur du Québec et vice-président du comité. Malheureusement, notre président, le sénateur Tony Dean, n'a pu se joindre à nous aujourd'hui. J'invite mes collègues à se présenter, en commençant par ma gauche.

Le sénateur Cardozo : Andrew Cardozo, de l'Ontario

[*Traduction*]

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

[*Français*]

Le sénateur Boisvenu : Pierre-Hugues Boisvenu, de la division de La Salle, au Québec.

[*Traduction*]

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

Le sénateur Boehm : Peter Boehm, de l'Ontario.

[*Français*]

Le vice-président : Merci, chers collègues. Pour ceux qui nous regardent en direct de partout au Canada, je rappelle que nous nous concentrons aujourd'hui sur les cybermenaces à l'endroit de l'infrastructure de défense du Canada. Nous avons trois groupes de témoins de renom avec nous aujourd'hui. Nous allons commencer immédiatement.

Pour notre premier groupe de témoins, nous avons le plaisir d'accueillir, du Centre de la sécurité des télécommunications, M. Sami Khoury, dirigeant principal, Centre canadien pour la cybersécurité et M. Daniel Couillard, directeur général, Partenariats et atténuation des risques, Centre canadien pour la cybersécurité.

Welcome, gentlemen, and thank you for being with us today. You have been invited to speak in the context of your *National Cyber Threat Assessment Report 2023-24*, from the Canadian Centre for Cyber Security.

We will begin by inviting you to make your opening remarks, which will be followed by questions from our members. Mr. Khoury, you may begin whenever you are ready.

Sami Khoury, Head, Canadian Centre for Cyber Security, Communications Security Establishment: Thank you very much, deputy chair.

[*English*]

Good afternoon. I am the head of the Canadian Centre for Cyber Security, often referred to as the "Cyber Centre," within the Communications Security Establishment, or CSE. I am pleased to be joined by my colleague Daniel Couillard, Director General of Partnerships and Risk Mitigation at the Cyber Centre.

[*Translation*]

We thank you for the invitation to appear today to discuss cybersecurity and, specifically, our *National Cyber Threat Assessment 2023-24* released on October 28, 2022. You may have noticed there is a lot in the news about cybersecurity, but I am happy to say that our assessment remains as relevant — dare I say "fresh" — today as it was when we released it five months ago. I will refer to this report throughout my remarks by its acronym, the NCTA, or ECMN in French.

[*English*]

I'd like to begin by providing an overview of CSE's Cyber Centre, which serves as a unified source of expert advice, guidance and support on cybersecurity operational matters.

[*Translation*]

We work closely with other government agencies, industry partners, and with the public to improve cybersecurity for Canadians and to make Canada more resilient against cyber threats.

[*English*]

At the Cyber Centre, we deliver world-class defence of Canadian government networks. We defend systems of importance, which are specifically designated by our minister, from malicious cyberactors by deploying sophisticated digital

Bienvenue, messieurs, et merci de votre présence parmi nous aujourd'hui. Vous avez été invités à prendre la parole dans le cadre de votre *Évaluation des cybermenaces nationales 2023-2024*, du Centre canadien pour la cybersécurité.

Nous allons commencer par vous inviter à présenter vos remarques préliminaires, qui seront suivies de questions de la part de nos membres. Monsieur Khoury, vous pouvez commencer quand vous êtes prêt.

Sami Khoury, dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications : Merci beaucoup, monsieur le vice-président.

[*Traduction*]

Bonjour. Je suis le dirigeant principal du Centre canadien pour la cybersécurité, qu'on appelle souvent le « Centre pour la cybersécurité » et qui fait partie du Centre de la sécurité des télécommunications ou CST. Je suis heureux d'être accompagné de mon collègue Daniel Couillard, directeur général des Partenariats et atténuation des risques au Centre pour la cybersécurité.

[*Français*]

Merci de nous avoir invités aujourd'hui pour discuter de cybersécurité, et particulièrement de notre *Évaluation des cybermenaces nationales (ECMN) 2023-2024* parue le 28 octobre 2022. Vous avez peut-être remarqué qu'il est souvent question de cybersécurité dans les nouvelles, mais je suis heureux d'annoncer que notre évaluation demeure aussi pertinente — j'ose même dire « fraîche » — aujourd'hui qu'elle l'était au moment de sa publication, il y a cinq mois. Tout au long de ma déclaration, je désignerai le rapport par son acronyme, ECMN, ou NCTA en anglais.

[*Traduction*]

J'aimerais commencer par faire un petit survol du Centre pour la cybersécurité du CST, qui est une source unifiée de conseils d'experts, d'avis et de soutien sur des questions opérationnelles de cybersécurité.

[*Français*]

Le Centre canadien pour la cybersécurité collabore étroitement avec d'autres organismes gouvernementaux, des partenaires de l'industrie et le public dans le but d'améliorer la cybersécurité des Canadiennes et des Canadiens et d'accroître la résilience du Canada face aux cybermenaces.

[*Traduction*]

Le Centre pour la cybersécurité a recours à des moyens de cyberdéfense de renommée mondiale pour protéger les réseaux gouvernementaux canadiens. Nous défendons les « systèmes d'importance », qui sont spécifiquement désignés par notre

defence protections that are informed by our unique information advantage as part of CSE.

The Cyber Centre supports Canadians and Canadian businesses around the clock by posting threat alerts and advisories, undertaking cybersecurity public awareness campaigns, such as Get Cyber Safe, and even providing the cybersecurity community with free tools like Assemblyline, our malware detection and analysis tool, to ensure all Canadians have access to resources that make them feel safe online. By forming partnerships with stakeholders across the country, from government institutions to critical infrastructure service providers and academia, the Cyber Centre works tirelessly to collectivity raise Canada's cybersecurity bar.

One of the Cyber Centre's roles is to keep Canadians informed about cybersecurity and the possible threats they may encounter. To do this, we monitor the evolution of cyber-threats against Canada and produce assessments and reports. These reports are unclassified, publicly accessible analyses of the threats Canada is facing in the constantly evolving cyberlandscape. I strongly encourage members of this committee, and Canadians more broadly, to read these assessments, as they provide an invaluable look into the threats the Cyber Centre defends against every single day.

[*Translation*]

One of these reports, released every two years and based on both classified and unclassified sources, is the NCTA. Our goal with the NCTA is to inform the public about the threats we expect due to the increasing digitization of all aspects of our lives.

[*English*]

The assessment's findings are based on reporting from classified and unclassified sources, including those related to CSE's foreign intelligence mandate. While the Cyber Centre must protect classified sources and methods, we have tried to provide readers with as much information as possible.

I will now provide a brief breakdown of the Cyber Centre's key findings from the most recent NCTA regarding the cyber-threat landscape. We have chosen to focus on five cyber-threat narratives that we judge are the most dynamic and

ministre, contre les cybercriminelles et cybercriminels malveillants en recourant à des moyens de protection sophistiqués de défense numérique que nous possédons grâce à notre appartenance au CST.

Le Centre pour la cybersécurité soutient la population et les entreprises canadiennes à toute heure du jour et de la nuit en publiant des alertes et des avis de menace, en menant des campagnes de sensibilisation du public à la cybersécurité, comme la campagne Pensez cybersécurité, et même en offrant à la collectivité de la cybersécurité des outils gratuits, comme AssemblyLine, notre outil de détection et d'analyse de maliciels. Nous faisons cela pour que la population canadienne, sans exception, ait accès aux ressources nécessaires pour se sentir en sécurité en ligne. En établissant des partenariats avec des intervenants des quatre coins du pays, que ce soient des établissements gouvernementaux, des fournisseurs de service des infrastructures essentielles ou des membres du milieu universitaire, le Centre pour la cybersécurité travaille d'arrache-pied pour rehausser la cybersécurité du Canada.

Un des rôles confiés au Centre pour la cybersécurité est de renseigner les Canadiennes et les Canadiens sur la cybersécurité et de les informer des menaces qui pourraient peser sur eux. Pour ce faire, nous suivons l'évolution des cybermenaces qui planent sur le Canada et produisons des évaluations et des rapports à ce sujet. Il s'agit d'analyses non classifiées et accessibles au public sur les menaces qui guettent le Canada dans le cyberespace en évolution constante. D'ailleurs, j'encourage fortement les membres du comité, et les Canadiennes et Canadiens en général, à lire ces évaluations, car elles donnent un aperçu unique des menaces contre lesquelles le Centre pour la cybersécurité nous défend au quotidien.

[*Français*]

Un de ces rapports, l'ECMN, est publié tous les deux ans et est fondé sur des sources classifiées et non classifiées. L'objectif de l'ECMN est d'informer la population sur les menaces qui, selon nous, sont liées à la numérisation croissante de tous les aspects de nos vies.

[*Traduction*]

Les conclusions de l'évaluation sont fondées sur des rapports provenant de sources classifiées et non classifiées, dont certaines découlent du mandat de renseignement étranger du CST. Le Centre pour la cybersécurité est tenu de protéger les sources et les méthodes classifiées, mais il s'efforce de fournir autant d'informations que possible au lectorat.

Je vais maintenant expliquer brièvement les principales conclusions de la dernière évaluation des cybermenaces nationales portant sur l'environnement de cybermenace. Nous avons choisi de nous concentrer sur cinq catégories de

impactful and that will continue to drive cyber-threat activity to 2024.

First, ransomware is a persistent threat to Canadian organizations. We reported that cybercrime continues to be the cyber-threat activity most likely to affect Canadians and Canadian organizations. Due to its impact on an organization's ability to function, ransomware is almost certainly the most disruptive form of cybercrime facing Canadians.

Second, critical infrastructure is increasingly at risk from cyber-threat activity. This means that cybercriminals can exploit critical infrastructure. State-sponsored actors target critical infrastructure to collect information through espionage, to pre-position in case of future hostilities and as a form of power projection and intimidation.

Third, state-sponsored cyber-threat activity is impacting Canadians. Notably, the state-sponsored cyber programs of China, Russia, Iran and North Korea pose the greatest strategic cyber-threats to Canada.

Fourth, cyber-threat actors are attempting to influence Canadians and degrade trust in our online spaces. We have observed cyber-threat actors' use of misinformation, disinformation and mal-information evolve over the past two years.

Finally, disruptive technologies bring new opportunities and new threats. Digital assets, such as cryptocurrencies and decentralized finance, are both targets and tools for cyber-threat actors to enable malicious cyber-threat activity. Machine learning can be exploited by cyber-threat actors, and quantum computing has the potential to threaten our current systems of maintaining trust and confidentiality online.

[*Translation*]

Although these trends can be worrisome, our hope is that we can help Canadians stay aware and informed of the potential threats they may encounter online. The good news is that many of the cyber risks we identify in this report can be mitigated. In fact, the vast majority of cyber incidents can be prevented by basic cybersecurity measures. That is why the Cyber Centre has released advice and guidance tailored to the five narratives identified in this report. These companion publications outline

cybermenaces qui sont, à notre avis, les plus changeantes et les plus lourdes de conséquences, et qui continueront de façonner les activités de cybermenace en 2024.

Premièrement, les rançongiciels constituent une menace omniprésente pour les organisations canadiennes. Nous avons signalé que la cybercriminalité continue d'être l'activité de cybermenace la plus susceptible de toucher les Canadiens et les organisations canadiennes. Comme ils perturbent les capacités de fonctionnement des organisations qu'ils touchent, les rançongiciels sont presque certainement la forme de cybercriminalité la plus perturbatrice à laquelle sont confrontés les Canadiens.

Deuxièmement, les infrastructures essentielles risquent de plus en plus d'être visées par des activités de cybermenace. Cela signifie que les cybercriminels peuvent exploiter les infrastructures essentielles. Les acteurs parrainés par des États ciblent les infrastructures essentielles pour recueillir des renseignements par l'entremise de l'espionnage, afin de se prépositionner en cas d'hostilités futures et comme une forme d'intimidation et de projection de la puissance.

Troisièmement, les activités de cybermenace parrainées par des États touchent les Canadiens. Notamment, les cyberprogrammes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord représentent les plus grandes cybermenaces stratégiques pour le Canada.

Quatrièmement, les auteurs de cybermenace tentent d'influencer les Canadiens et de briser la confiance accordée aux espaces virtuels. Au cours des deux dernières années, nous avons observé une hausse du recours à la mésinformation, désinformation et malinformation de la part des auteurs de cybermenace

Enfin, les technologies perturbatrices créent à la fois de nouvelles possibilités et de nouvelles menaces. Les actifs numériques, tels que les cryptomonnaies et la finance décentralisée, sont à la fois des cibles et des outils pour les auteurs de cybermenace. L'apprentissage machine peut être exploité par les auteurs de cybermenace et l'informatique quantique peut menacer nos systèmes actuels de maintien de la confiance et de confidentialité en ligne.

[*Français*]

Ces tendances sont inquiétantes, mais nous espérons pouvoir aider les Canadiens à rester conscients et informés des menaces potentielles auxquelles ils pourraient être confrontés en ligne. La bonne nouvelle, c'est que l'on peut atténuer la plupart des risques liés à la cybersécurité qui sont cernés dans ce rapport. En fait, la grande majorité des cyberincidents peuvent être évités par de simples mesures de cybersécurité. C'est pourquoi le Centre canadien pour la cybersécurité a publié des avis et des

practical steps to mitigate the risks associated with each theme. The Get Cyber Safe website also offers simple and effective cybersecurity tips for individual Canadians.

[*English*]

As technology continues to accelerate with rapid speed, threats also continue to evolve. The Cyber Centre is working hard to bolster cybersecurity capabilities across Canada, in partnership with industry, academia and all levels of government. Although Canada has strong defences in place, our tool kit can be bolstered to better protect our country against the rapidly evolving threats posed by cybercriminals and state-sponsored threat actors.

Moving forward, and as a means to continue to adapt to the evolving threat environment, bolster defences and help better protect Canada and Canadians, we're hopeful to see the continued progress of Bill C-26, An Act respecting cybersecurity, currently in second reading in the House of Commons. This legislation would establish a regulatory framework to strengthen cybersecurity for services and systems that are vital to national security and public safety and give the government a new tool to respond to emerging cyber-threats.

As well, the Government of Canada is currently undertaking a renewal of the National Cyber Security Strategy, which originally launched in 2018. CSE and its Canadian Centre for Cyber Security are important partners in this strategy, and we are continuously monitoring the cyber-threat landscape, evolving trends and proposing new programs and ideas.

In closing, I would underline that Canada is facing a complex and rapidly evolving cyber-threat landscape.

[*Translation*]

Briefings such as this are an important opportunity to discuss the risks we face and the steps we can take to better protect ourselves online.

[*English*]

CSE and the Cyber Centre are working hard to mitigate many of these threats and protect Canadians and their interest.

I am grateful for having had the chance to talk to you about this today. Thank you.

orientations conçus sur mesure pour les cinq catégories de cybermenaces définies dans ce rapport. Ces documents sont complémentaires et présentent des mesures pratiques visant à atténuer les risques liés à chaque catégorie. Le site Web Pensez cybersécurité propose aussi des conseils de cybersécurité simples et efficaces à l'intention de tous les Canadiens.

[*Traduction*]

Les menaces évoluent au même rythme effréné que la technologie. Le Centre pour la cybersécurité s'efforce de renforcer les capacités de cybersécurité en partenariat avec l'industrie, le milieu universitaire et tous les échelons de gouvernement, et ce, partout au Canada. Même si le Canada compte déjà d'efficaces mesures de défense, notre trousse d'outils pourrait être améliorée pour mieux protéger notre pays contre les menaces en constate et rapide évolution que représentent les cybercriminels et les auteurs de menace parrainés par des États.

Afin de continuer à nous adapter à l'environnement de menace qui évolue sans cesse, de renforcer les défenses et d'aider à mieux protéger le Canada et sa population, nous espérons que le projet de loi C-26, Loi concernant la cybersécurité, qui est actuellement en deuxième lecture à la Chambre des communes, continuera d'aller de l'avant. Cette loi établira un cadre réglementaire pour renforcer la cybersécurité des services et systèmes vitaux à la sécurité nationale et publique, et donnera au gouvernement de nouveaux outils pour intervenir contre les cybermenaces émergentes.

De plus, le gouvernement du Canada renouvelle en ce moment la Stratégie nationale de cybersécurité adoptée en 2018. Le CST et le Centre canadien pour la cybersécurité sont des partenaires importants dans cette stratégie, et nous surveillons en permanence le contexte des cybermenaces, l'évolution des tendances et proposons de nouveaux programmes et idées.

Pour conclure, j'insiste sur le fait que le Canada fait face à un contexte de cybermenace complexe et qui évolue rapidement.

[*Français*]

Des séances d'information comme celle-ci sont une occasion importante de discuter des risques auxquels nous sommes confrontés et des mesures que nous pouvons prendre pour mieux nous protéger en ligne.

[*Traduction*]

Le CST et le Centre pour la cybersécurité travaillent sans relâche pour atténuer les menaces et protéger les Canadiennes et Canadiens et leurs intérêts.

Je suis reconnaissant d'avoir eu l'occasion de vous en parler aujourd'hui. Merci.

[*Translation*]

The Deputy Chair: Thank you very much for your statement, Mr. Khoury. Before we proceed, I would like to acknowledge Senator Richards, who has just joined us.

I would also like to ask participants in the room not to lean too closely to the microphone and not to remove their earpieces. This will help avoid sound feedback that could negatively impact committee staff in the room.

Mr. Khoury and Mr. Couillard are with us for approximately one hour. In order for each member of the committee to participate, I will limit the questions and answers to four minutes. I would ask that you keep your questions succinct and identify the person you wish to address.

[*English*]

Senator Boehm: Thank you, Mr. Khoury and Mr. Couillard, for being here and for the important work that you and your teams undertake for Canada.

In the Centre for Cyber Security's *National Cyber Threat Assessment 2023-24*, it states:

> Critical infrastructure is increasingly at risk from cyber threat activity . . . .
>
> State-sponsored actors target critical infrastructure to collect information through espionage, to pre-position in case of future hostilities, and as a form of power projection and intimidation. However, we assess that state-sponsored cyber threat actors will very likely refrain from intentionally disrupting or destroying Canadian critical infrastructure in the absence of direct hostilities.

We are in a situation where we are supporting Ukraine in the war that Russia has started. We are not in direct conflict with Russia, but we are providing military, economic and humanitarian forms of assistance in Ukraine's defence. Do you in the centre consider that our critical and defence infrastructure is at increased risk of cyber-threat activity by Russia, given our support for Ukraine, despite the absence of direct hostilities? Is there an increased risk of cyberattacks on Canada — to name another country — by Iran, given that it is an ally of Russia and that our government and, indeed, Canadians have been very critical of Iran, particularly on human rights within the country?

Mr. Khoury: Thank you, senator, for this question.

We have been paying particular attention to the Russia-Ukraine conflict. Since the early days of the conflict, we have been warning Canadians and Canadian businesses to take every

[*Français*]

Le vice-président : Merci beaucoup de votre présentation, monsieur Khoury. Avant de poursuivre, j'aimerais souligner la présence du sénateur Richards, qui vient de se joindre à nous.

J'aimerais également demander aux participants présents dans la salle de ne pas se pencher trop près du microphone et de ne pas retirer leur oreillette. Cela permettra d'éviter une rétroaction sonore qui pourrait avoir un impact négatif sur le personnel du comité qui se trouve dans la salle.

MM. Khoury et Couillard sont avec nous pour environ une heure. Afin que chaque membre du comité puisse participer, je limiterai les questions et les réponses à quatre minutes. Je vous prierais de poser des questions succinctes et d'identifier la personne à laquelle vous souhaitez vous adresser.

[*Traduction*]

Le sénateur Boehm : Merci, monsieur Khoury et monsieur Couillard, pour votre présence et pour l'important travail que vous et vos équipes accomplissez pour le Canada.

Voici ce qu'on peut lire dans l'*Évaluation des cybermenaces nationales 2023-2024*, du Centre canadien pour la cybersécurité :

> Les activités de cybermenace représentent un risque de plus en plus grand pour les infrastructures essentielles.
>
> 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. Cependant, nous estimons que les auteurs de cybermenaces parrainés par des États s'abstiendront fort probablement de perturber ou de détruire intentionnellement les infrastructures essentielles canadiennes sans qu'il y ait d'hostilités directes.

Nous appuyons l'Ukraine dans la guerre déclenchée par la Russie. Nous ne sommes pas en conflit direct avec la Russie, mais nous fournissons une aide militaire, économique et humanitaire à la défense de l'Ukraine. Au centre, considérez-vous que nos infrastructures essentielles et de défense sont plus à risque de cybermenaces de la part de la Russie, compte tenu de notre soutien à l'Ukraine, malgré l'absence d'hostilités directes? Existe-t-il un risque accru de cyberattaques contre le Canada par l'Iran — histoire de citer un autre pays — qui est allié de la Russie et qui a subi les critiques de notre gouvernement de même que des Canadiens, particulièrement dans le dossier des droits de la personne?

M. Khoury : Je vous remercie pour cette question, sénateur.

Nous avons porté une attention particulière au conflit entre la Russie et l'Ukraine. Depuis le début de ce conflit, nous avertissons les Canadiens et les entreprises canadiennes de

possible precaution to protect their infrastructure from cyberattack, either direct or indirect. We have published alerts and bulletins continuously since the early days of the conflict — the most recent one was in February of this year — where we continue to warn about what our concerns are. We are definitely concerned about critical infrastructure.

We have learned a lot from the Russia-Ukraine conflict. We are an organization that also has an intelligence mandate, and we learn a lot from what we are observing happening in Ukraine. We turn that information around very quickly to warn Canadians.

It is no secret that Russia is a sophisticated adversary, and they have demonstrated that they use their cyber capabilities in a very irresponsible way. Not only do they use them in Ukraine, but they use them against civilian infrastructure beyond just Ukraine — in the case of Viasat, for example. When they do that and cross cyber norms, we call them out, and there have been a number of instances where Canada has joined allies to call out the irresponsible behaviour of Russia.

From a Cyber Centre perspective, we are concerned, and definitely critical infrastructure is top of mind, but we are doing everything we can to share what we know and be on point with our colleagues in the CI space to warn them about any forms of cyberattacks.

Senator Boehm: Do you want to add anything on Iran?

Mr. Khoury: In our national cyber-threat assessment, we call out the four countries: Russia, China, Iran and North Korea. Each one has different motivations in terms of their cyber programs. When necessary, we will put out a bulletin about Iranian activities, and we did that last year jointly with the U.S. to warn against Iranian activities. We learn a lot through our intelligence mission and then turn around that information to warn Canadians about the activities of these four countries.

Senator Boehm: Thank you.

[*Translation*]

Senator Boisvenu: Welcome to our two witnesses. We cannot ignore a subject that is currently much in the news in Canada, namely interference in the electoral process by China or Russia. Has your centre been asked to share any information? In fact, do you have any knowledge of such interference?

prendre toutes les précautions possibles pour protéger leurs infrastructures contre les cyberattaques, directes ou indirectes. Nous publions continuellement des alertes et des bulletins depuis les premiers jours du conflit — le plus récent remontant à février de cette année — où nous faisons régulièrement part de nos préoccupations. Nous nous préoccupons bien sûr des infrastructures essentielles.

Nous avons beaucoup appris du conflit entre la Russie et l'Ukraine. Nous sommes une organisation qui a également un mandat de renseignement, et nous apprenons beaucoup de ce que nous observons en Ukraine. Nous transmettons ces renseignements très rapidement pour avertir les Canadiens.

Ce n'est un secret pour personne que la Russie est un adversaire sophistiqué qui a fait la preuve de sa capacité à déployer sa cybercapacité de façon particulièrement irresponsable. C'est ce qu'elle fait non seulement en Ukraine, mais aussi contre des infrastructures civiles ailleurs dans le monde, comme celles de Viasat, par exemple. Quand tel est le cas, quand la Russie enfreint les normes cybernétiques, nous la dénonçons, et il est arrivé à plusieurs reprises que le Canada fasse corps avec des alliés pour dénoncer le comportement irresponsable de la Russie.

Le Centre pour la cybersécurité est donc préoccupé et, pour lui, les infrastructures essentielles sont bien sûr une priorité. Il fait tout son possible pour communiquer tout ce qu'il sait et pour prévenir ses collègues des infrastructures essentielles de toute forme de cyberattaque anticipée.

Le sénateur Boehm : Voulez-vous ajouter quelque chose au sujet de l'Iran?

M. Khoury : Dans notre évaluation des cybermenaces nationales, nous avons à l'œil quatre pays que sont la Russie, la Chine, l'Iran et la Corée du Nord. Chacun obéit à des motivations différentes par le biais de ses programmes cybernétiques. Au besoin, nous publierons un bulletin sur les activités iraniennes, et nous l'avons fait l'an dernier conjointement avec les États-Unis pour une mise en garde contre les activités iraniennes. Nous apprenons beaucoup grâce à notre mission de renseignement, puis nous exploitons l'information recueillie pour avertir les Canadiens des activités de ces quatre pays.

Le sénateur Boehm : Merci.

[*Français*]

Le sénateur Boisvenu : Bienvenue à nos deux témoins. On ne peut passer sous silence un sujet qui est d'actualité au Canada actuellement, soit l'interférence dans le processus électoral par la Chine ou la Russie. Est-ce que votre centre a été amené à partager certaines informations? En fait, est-ce que vous avez une certaine connaissance de ces interférences?

Mr. Khoury: Thank you for your question. Yes, the centre has been involved, and there are different ways in which the centre gets involved in these types of issues.

First of all, in the report, we have documented publicly that we are concerned about interference in the electoral process in Canada.

During elections, we work very closely with Elections Canada to protect the electoral infrastructure and ensure that it is well secured from a cybersecurity perspective. The CSE is part of the Security and Intelligence Threats to Elections Task Force. This is a non-partisan committee of public servants who, during the election period, manage the risks that are raised; it is their responsibility to decide whether or not the threshold has been met.

In our cybersecurity role, we actually protect the electronic infrastructure of elections, but other government partners inside and outside of CSE are also involved in this committee.

Senator Boisvenu: Can this security operation lead you to make direct interventions in external interference?

Mr. Khoury: If we're talking about technological interference, if we see something of concern on the networks, we work with Elections Canada to manage those concerns, whether they're criminal or otherwise. If it's non-electronic interference, I defer to other departments that have that responsibility.

[*English*]

Senator Dasko: Thank you for being here today. It is a very important and very interesting topic.

I read the background material, and coincidentally there is a piece in *The Globe and Mail* today about cybersecurity where it says the federal government is subject to between three and five billion malicious actions daily. Now, of course, this boggles the mind. I wonder if you can unpack that a little bit. Surely, if we had that many attacks — and I'm not saying that this is wrong, but it would seem that we would be destroyed through such attacks. Just give us a sense of what that looks like.

Another question I would like to throw in is about a great concern I have about your comments with respect to foreign actors attempting to degrade trust in our democratic institutions. I would really like it if you could provide some examples of who and what. What are some of the things that they have done to degrade our trust in our institutions? I have more questions, too.

M. Khoury : Je vous remercie de votre question. Effectivement, le centre a été impliqué, et il y a différents angles pour ce qui est de la façon dont le centre s'implique dans ce genre de dossier.

Premièrement, dans le rapport, nous avons documenté publiquement le fait que nous nous soucions de l'ingérence dans le processus électoral au Canada.

Durant les élections, nous travaillons de très près avec Élections Canada pour protéger l'infrastructure électorale et nous assurer qu'elle est bien sécurisée sur le plan de la cybersécurité. Le CST fait partie du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections. Il s'agit d'un comité non partisan de fonctionnaires qui, durant la période électorale, gère les risques qui sont soulevés; il lui incombe de décider si le seuil a été atteint ou non.

Dans notre rôle de cybersécurité, nous protégeons réellement l'infrastructure électronique des élections, mais d'autres partenaires gouvernementaux, à l'intérieur et à l'extérieur du CST, participent également aux travaux de ce comité.

Le sénateur Boisvenu : Cette intervention sécuritaire peut-elle vous amener à faire des interventions directes en matière d'ingérence externe?

M. Khoury : Si nous parlons d'ingérence technologique, si nous voyons quelque chose de préoccupant sur les réseaux, nous travaillons avec Élections Canada pour gérer ces soucis, qu'ils soient d'origine criminelle ou autre. S'il s'agit d'ingérence non électronique, je m'en remets à d'autres ministères qui ont cette responsabilité.

[*Traduction*]

La sénatrice Dasko : Merci d'être venus à notre rencontre. C'est un sujet très important et très intéressant.

J'ai lu les documents d'information et je suis aussi tombé sur un article du *Globe and Mail* d'aujourd'hui sur la cybersécurité dans lequel on dit que le gouvernement fédéral fait l'objet de trois à cinq milliards d'actes malveillants chaque jour. Bien sûr, cela dépasse l'entendement. Je me demande si vous pourriez nous en dire un peu plus à ce sujet. Si nous subissions autant d'attaques — et je ne dis pas que le chiffre avancé est faux —, il me semble que nous serions anéantis par de telles attaques. Donnez-nous simplement une idée de ce à quoi cela ressemble.

L'autre question que je veux vous poser découle de vos propos au sujet des acteurs étrangers qui tentent de saper la confiance envers nos institutions démocratiques, ce qui n'a pas manqué de m'inquiéter. J'aimerais beaucoup que vous me donniez des exemples de ce dont on parle au juste. Qu'ont-ils fait pour saper notre confiance dans nos institutions? J'aurai ensuite d'autres questions.

[*Translation*]

Daniel Couillard, Director General, Partnerships and Risk Mitigation, Canadian Centre for Cyber Security, Communications Security Establishment: Hello, and thank you for your question. I will answer the first one.

One of the functions of the Canadian Centre for Cyber Security is to protect the federal government's network, in partnership with other departments, such as Shared Services Canada. In this effort, we have deployed an infrastructure that monitors what is happening on government networks.

[*English*]

This infrastructure that we deploy on government networks provides us automated 24-7 monitoring of activities on our network, and we also build in an automatic response to some of these threats. Of course, we're talking about government networks that are operating at very high speed. We are processing lots of information. That results in those huge numbers that you have seen. Not every one of these attacks or actions that we block are necessarily direct high-risk attacks against the networks. Some of these are just reconnaissance activities. Those are all technical activities that any network is subject to. Of course, working with allies, we have a large set of indicators of compromise, which could be many things, and one of them could be an IP address, that we know are nefarious or are associated with some kind of malicious actor in the government. Those are the ones we block. That's how we get to those numbers that we are blocking, and those are daily. They are all automated and keep knocking on our door every day. That's how we get to these numbers.

Senator Dasko: You're just batting them away.

Mr. Couillard: Exactly.

Mr. Khoury: On the second part of your question about disinformation, in our report, we name actors like Russia and China as being active in that space. Case in point, during the conflict last year, Russia put out some information that Canadian soldiers or Canadian involvement in Ukraine was false. We knew it was false, and, as a result, the CSE took the unusual step of declassifying intelligence to make the point. They are flooding the air waves with a lot of misinformation in order to erode trust in our institutions, whether it is the Canadian Forces, the government or others. We need to be vigilant and invite Canadians to be critical of the information that they read, be aware of the sources they get the information from and, when required, we will use our intelligence and declassify it to prove the point.

[*Français*]

Daniel Couillard, directeur général, Partenariats et atténuation des risques, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications : Bonjour et merci pour votre question. Je vais répondre à la première.

L'une des fonctions du Centre canadien pour la cybersécurité est de protéger le réseau du gouvernement fédéral, en partenariat avec d'autres ministères, comme Services partagés Canada. Dans cet effort, nous avons déployé une infrastructure qui permet de surveiller ce qui se passe sur les réseaux du gouvernement.

[*Traduction*]

Cette infrastructure que nous déployons sur les réseaux gouvernementaux nous permet de surveiller les activités de notre réseau 24 heures sur 24, 7 jours sur 7, et nous intégrons également une réponse automatique à certaines de ces menaces. Bien sûr, nous parlons de réseaux gouvernementaux à très grande vitesse. Nous traitons d'énormes volumes de données, ce qui explique les chiffres impressionnants que vous avez vus. Toutes les attaques ou actions que nous bloquons ne sont pas nécessairement à haut risque et menées directement contre les réseaux. Certaines de ces activités ne sont que des activités de reconnaissance. Ce sont toutes des activités techniques auxquelles tout réseau est soumis. Bien sûr, en collaboration avec nos alliés, nous disposons d'un grand nombre d'indicateurs de risque, comme l'adresse IP qui peut être celle d'un opérateur malveillant ou être associée à un acteur étatique malveillant. C'est ce genre de tentative de pénétration que nous bloquons. C'est ainsi que nous arrivons à ces nombres impressionnants d'attaques bloquées quotidiennement. Elles sont toutes automatisées et continuent d'être lancées contre nous tous les jours. C'est ce qui explique ces chiffres.

La sénatrice Dasko : Vous leur fermez la porte au nez.

M. Couillard : Exactement.

M. Khoury : Pour ce qui est de la deuxième partie de votre question sur la désinformation, dans notre rapport, je dirais que nous désignons des acteurs comme la Russie et la Chine comme étant actifs sur ce plan. L'an dernier, par exemple, après le début du conflit, la Russie a publié des informations démentant la participation de soldats canadiens ou du Canada au côté de l'Ukraine. Nous savions que tel était le cas et, par conséquent, le CST a pris la mesure inhabituelle de déclassifier les renseignements pour faire valoir son point de vue. Les Russes saturent les ondes à coups de désinformations visant à saper la confiance envers nos institutions, qu'il s'agisse des Forces canadiennes, du gouvernement ou d'autres. Nous devons être vigilants et inviter les Canadiens à se montrer critiques à propos de ce qu'ils lisent, à être conscients des sources d'information. Au besoin, nous déclassifions nos renseignements pour prouver le bien-fondé de notre position.

Senator Dasko: What would the sources be for the examples you gave? Would it be sources on Twitter or social media? Where are they disseminating this information?

Mr. Khoury: I think it was on Twitter, but I would have to get back to my sources, if you don't mind.

[*Translation*]

The Deputy Chair: Before we continue, I want to acknowledge Senator Deacon, who has just joined us.

[*English*]

Senator Cardozo: I have so many questions to ask, but I wonder if I could talk about the issue of electoral or political interference a little further. Could you give us some examples of the things that are happening? We know some of the stuff out there that we're reading about, but can you give us a handful of examples of actions that foreign governments or foreign players are taking in our electoral and political systems overall?

Mr. Khoury: Thank you for the question.

In my role as the head of the Cyber Centre, our primary focus is to defend the infrastructure of Elections Canada and the infrastructure that is meant to support the conduct of an election. We work with Elections Canada, and we start working with them even before an election to ensure the security of the network and systems, which is very important. That's our role in monitoring the cybersecurity of the infrastructure. If there are cyber-threats that we notice on these networks, we will be able to detect them. Whether they are criminal or whether they are nation states, we will be able to detect them on the networks and neutralize or remove them.

If there are any threats that are not of a cybersecurity nature, other government agencies would then be better-suited to answer your question about the kinds of other threats, whether it's the RCMP, CSIS or other departments.

Senator Cardozo: Is some of the interference people spreading misinformation and disinformation about the electoral system or about political parties?

Mr. Khoury: There could be both. There could be misinformation out there about the election or about the political parties.

During the election, we have worked with the political parties, all of them, to inform them of threats. We've set up a 24-7 hotline where people can call us. The candidates can call if they have any concern from a cybersecurity point of view. We work with Elections Canada, as I mentioned, and we work with the House of Commons to secure the infrastructure there. We're definitely at the cybersecurity of the infrastructure, but if there are additional concerns, they might have to resort to some of our other partners across government.

La sénatrice Dasko : Quelles seraient les sources des exemples que vous avez donnés? Twitter ou les réseaux sociaux? Où cette information est-elle diffusée?

M. Khoury : Je crois que c'était sur Twitter, mais, si vous n'y voyez pas d'inconvénient, il faudrait que je vérifie.

[*Français*]

Le vice-président : Avant de continuer, je veux souligner la présence de la sénatrice Deacon, qui vient de se joindre à nous.

[*Traduction*]

Le sénateur Cardozo : J'ai tant de questions, mais pourrait-on approfondir un peu celle de l'ingérence électorale ou politique? Pourriez-vous nous donner des exemples? Nous sommes au courant de certaines choses grâce aux journaux, mais pourriez-vous nous donner quelques exemples d'interventions de gouvernements ou d'agents étrangers dans notre système électoral et dans notre système politique en général?

M. Khoury : Merci de la question.

Le Centre pour la cybersécurité a pour principal objectif de défendre l'infrastructure d'Élections Canada et l'infrastructure qui est censée étayer l'organisation d'élections. Nous collaborons avec Élections Canada, et notre collaboration commence avant même une élection pour garantir la sécurité du réseau et des systèmes; c'est très important. C'est la responsabilité qui nous incombe dans la surveillance de la cybersécurité de l'infrastructure. Si des cybermenaces pèsent sur ces réseaux, nous serons en mesure de les détecter. Qu'il s'agisse de criminels ou d'États-nations, nous pourrons les repérer sur les réseaux et les neutraliser ou les éliminer.

Quant aux menaces qui ne sont pas liées à la cybersécurité, d'autres organismes gouvernementaux seront mieux à même de répondre à votre question au sujet des autres types de menaces, qu'il s'agisse de la GRC, du SCRS ou d'autres ministères.

Le sénateur Cardozo : Les gens qui font de l'ingérence répandent-ils de la désinformation au sujet du système électoral ou des partis politiques?

M. Khoury : Les deux peuvent se produire. Il pourrait effectivement y avoir de la désinformation au sujet des élections ou des partis politiques.

Pendant la campagne électorale, nous avons communiqué avec tous les partis politiques pour les informer des menaces. Nous avons créé une ligne d'assistance accessible 24 heures sur 24, 7 jours sur 7. Les candidats peuvent appeler s'ils ont des préoccupations en matière de cybersécurité. Nous collaborons avec Élections Canada, comme je l'ai dit, mais nous travaillons aussi avec la Chambre des communes pour y sécuriser l'infrastructure. Notre rôle est de veiller à la cybersécurité de l'infrastructure, mais, s'il y a d'autres préoccupations, il peut y

Senator Cardozo: How many of those cyber-threats would you say come from within Canada or North America as opposed to China or Russia?

Mr. Khoury: Where a cyber-threat comes from does not necessarily point you toward who is behind it because foreign actors will try to cover their tracks by making it appear as if it is coming from elsewhere. Our priority at the Cyber Centre is to block all these cyber-threats to make sure we neutralize them regardless of where they come from. Attribution becomes a secondary effect. We will get there once we make sure that the system is secure and there are no more threats on it. Primarily, our job is to stop the threat or to neutralize it.

Senator Cardozo: Are there bad actors that you think are based in Canada?

Mr. Khoury: It's possible that there are bad actors that are leveraging Canadian infrastructure to attack government systems. That is possible. Determining who is the bad actor behind the keyboard would probably be for RCMP or CSIS to investigate, but it is possible that there are cyber incidents that are originating from Canada or that appear to originate from Canada as opposed to from outside of Canada.

Senator Yussuff: Thank you, witnesses, for being here today.

Given the myriad challenges we face, obviously government infrastructure and defence infrastructure are important. In addition to that, there are the things we hear about every day — hospitals being attacked or retail outlets being hijacked with demands for ransom to be paid. Does that also involve your work in alerting businesses? You said earlier that some of the things that could be done are fairly simple. My question is, if they are simple, why are they not being done, and why are so many institutions still vulnerable to cybersecurity attacks? It seems to me, from what I have read publicly and certainly in regard to these attacks, that we have yet to catch a culprit that is initiating the attacks. Maybe you can elaborate a bit more based on your experience and knowledge.

Mr. Khoury: Thank you for your question.

We live in a world where our IT networks are getting more and more complex. To get to a state that is 100% foolproof is probably very challenging. It sometimes only takes a small vulnerability to exploit a network.

There is a lot of interest in cybercriminals to impact pain on critical infrastructure because that's a pain point for society, whether it's a hospital, an energy sector provider or otherwise. They go after these organizations. We know they have no avoir lieu de faire appel à certains de nos partenaires au gouvernement.

Le sénateur Cardozo : Selon vous, combien de ces cybermenaces proviennent du Canada ou de l'Amérique du Nord plutôt que de la Chine ou de la Russie?

M. Khoury : L'origine géographique d'une cybermenace ne vous indique pas nécessairement sa véritable origine, puisque les agents étrangers tentent de brouiller les pistes en donnant l'impression qu'elle vient d'ailleurs. Le Centre pour la cybersécurité a pour responsabilité première de bloquer toutes ces cybermenaces pour que nous puissions les neutraliser, quelle que soit leur origine. L'attribution devient un effet secondaire. Nous aurons réussi lorsque nous aurons assuré la sécurité du système et éliminé toute menace. Notre travail consiste principalement à mettre fin à la menace ou à la neutraliser.

Le sénateur Cardozo : Selon vous, y a-t-il des agents malveillants basés au Canada?

M. Khoury : Il est possible que des agents malveillants tirent parti de l'infrastructure canadienne pour attaquer les systèmes gouvernementaux. C'est possible. C'est probablement à la GRC ou au SCRS qu'il incomberait de trouver qui est au clavier, mais des cyberincidents peuvent se produire Canada ou peuvent sembler provenir du Canada plutôt que de l'étranger.

Le sénateur Yussuff : Merci aux témoins d'être parmi nous aujourd'hui.

Compte tenu de la kyrielle de défis auxquels nous sommes confrontés, il est évident que l'infrastructure gouvernementale et l'infrastructure de défense sont importantes. Il y a aussi ce dont on entend parler tous les jours — des hôpitaux attaqués ou des magasins rançonnés. Est-ce que vous vous occupez également d'alerter les entreprises? Vous avez dit tout à l'heure que certaines des mesures susceptibles d'être prises sont assez simples. Ma question est la suivante : si c'est simple, pourquoi ne le fait-on pas et pourquoi la cybersécurité de tant d'institutions peut-elle encore être compromise? Il me semble, d'après ce que j'ai lu au sujet de ces attaques, que nous n'avons pas encore trouvé de coupables. Pourriez-vous nous éclairer compte tenu de votre expérience et de vos connaissances?

M. Khoury : Merci de votre question.

Nous vivons dans un monde où les réseaux TI sont de plus en plus complexes. Il est probablement très difficile de créer un système à toute épreuve. Il suffit parfois d'une petite vulnérabilité pour porter atteinte à un réseau.

On s'intéresse beaucoup aux cybercriminels qui s'attaquent aux infrastructures essentielles parce que c'est un souci majeur pour la société, qu'il s'agisse d'un hôpital, d'un fournisseur d'énergie, etc. Ils s'en prennent à ces organisations. Comme on

scruples. They are only in it to get money. They will launch a ransomware campaign against them for whatever money they can get.

We put out a lot of publications to encourage these organizations to up their cybersecurity games. There are simple things, as you mentioned, such as passwords, backups and things like that. In late 2021, we launched an anti-ransomware campaign with a letter signed by four ministers encouraging businesses to take the threat seriously. We have also published a playbook to help organizations defend against ransomware but also recover from a ransomware incident.

There is a lot that is out there in terms of a space where organizations can help defend themselves. Obviously, in some cases, it does require an investment on behalf of these organizations to up their cybersecurity capacity. There is a lot that can be done to raise the bar and raise resilience to make it more challenging for a ransomware actor to perpetrate an act of ransomware.

Senator Yussuff: At the national level, I assume there is some coordination with the provinces and territories in regard to how they are dealing with cybersecurity. They are not simply relying on you to defend their interests; they are going to look at their own interests. How much collaboration happens between your offices and the provincial and territorial offices across the country?

Mr. Khoury: Thank you for this.

We have various levels of engagement with the different provinces. We do talk to our provincial counterparts about cybersecurity. We exchange a lot of information. Between our SOC — security operation centre — and the provinces, there is also operational information that goes back and forth.

It's important to note that, when there is an incident, we hold the privacy of that incident very closely. We don't talk. Whether it's a hospital, municipality or a school board, it is between us and the victim. Unless they decide to pull in other elements within the conversation, we absolutely respect their privacy and keep it very tight to just the two of us.

Senator Richards: Thank you to the witnesses. I apologize if you have answered these questions partially, but I was late.

How complicit and cooperative are these bad actors with one another when it comes to dealing these various blows to Canadian sovereignty? How much more sophisticated, if they are more sophisticated, are the states such as Russia, and especially China, with our own cyber knowledge? Lastly, do we have our

le sait, ils n'ont aucun scrupule. Ils sont là pour l'argent. Ils lancent une campagne de rançongiciel pour obtenir autant d'argent qu'ils le peuvent.

Nous avons publié beaucoup d'articles pour inciter ces organisations à améliorer leurs mesures de cybersécurité. Comme vous l'avez dit, il y a des choses simples à faire, comme les mots de passe, les sauvegardes, etc. À la fin de 2021, nous avons lancé une campagne anti-rançongiciels en distribuant une lettre signée par quatre ministres invitant les entreprises à prendre la menace au sérieux. Nous avons également publié un guide pour aider les organisations à se défendre contre les rançongiciels, mais aussi à se remettre d'une attaque par rançongiciel.

Les organisations ont accès à de nombreux moyens de défense. Dans certains cas, elles doivent évidemment investir pour accroître leur capacité de cybersécurité. De nombreuses mesures peuvent être prises pour relever la barre et accroître la résilience afin d'entraver l'action des rançonneurs.

Le sénateur Yussuff : À l'échelle nationale, je suppose que les provinces et les territoires coordonnent leurs modes de gestion de la cybersécurité. Ils ne comptent pas seulement sur vous pour défendre leurs intérêts et veillent à leurs propres intérêts. Quelle est l'ampleur de la collaboration entre vos bureaux et les bureaux provinciaux et territoriaux à l'échelle du pays?

M. Khoury : Merci de votre question.

Nous avons divers niveaux de collaboration avec les différentes provinces. Nous discutons de cybersécurité avec nos homologues provinciaux. Nous échangeons beaucoup d'information. Entre notre COS — le Centre des opérations de sécurité — et les provinces, il y a aussi des échanges de renseignements opérationnels.

Je rappelle que, en cas d'incident, nous en protégeons absolument le caractère confidentiel. Nous ne divulguons rien. Qu'il s'agisse d'un hôpital, d'une municipalité ou d'un conseil scolaire, cela se passe entre nous et la victime. À moins qu'ils décident d'informer d'autres intervenants, nous respectons absolument le caractère privé de la situation et nous nous en tenons strictement à ce dialogue à deux.

Le sénateur Richards : Merci aux témoins de leur présence. Excusez-moi si vous avez répondu en partie à ces questions, mais je suis arrivé en retard.

Dans quelle mesure ces agents malveillants sont-ils complices et collaborent-ils entre eux quand il s'agit de compromettre la souveraineté canadienne? Dans quelle mesure, s'il y a lieu, des États comme la Russie et surtout la Chine ont-ils des connaissances cybernétiques à la mesure des nôtres? Enfin,

own collaborative firewalls with the U.S. and other NATO allies? I assume we do.

Mr. Khoury: Thank you very much for the question.

These cyber actors are getting more and more sophisticated. What we are seeing is that capabilities that used to be in the nation-state category are seeping into the criminal organizations. Criminal cyber capabilities are moving up in sophistication. They are seeping from the nation state down. We are also seeing that, in some case, nation states are using cybercriminal capabilities to hide their tracks so that it doesn't point in their direction.

As far as our knowledge of these actors, we have good knowledge about them. We have good collaboration with the U.S., for sure. Our critical infrastructure is connected in many cases. We have to collaborate with our allies to the south, but also with our international partners. There is a good level of collaboration in the cybersecurity space, not just within Canada but between Canada and the U.S., between Canada, the U.S. and the U.K., our Five Eyes partner and the international community.

Senator Richards: Would you say that China, in dealing blows to us, is more sophisticated than our ability to stop them at the moment, or do you think we're on par and we can rebuff these attacks?

Mr. Khoury: I think it is difficult to compare one actor to the other. At the Cyber Centre, our priority is to stop them all, regardless of their sophistication.

Senator Richards: Sure.

Mr. Khoury: Whether it's China, Russia, Iran or North Korea, we work tirelessly to make sure that we stop them all.

Senator Richards: Thank you.

Senator M. Deacon: I am going to backtrack. I know there are a number of timely topics that are relevant and near and dear to us, but I'm going to go back and remind us how we felt during the Rogers outage last summer. In that area, I'm referring to the question around the resilience of our telecommunications network. We learned a lot. Certainly, it lay bare how disruptive prolonged internet outages are to our lives, spanning the spectrum from inconvenient to actual security issues, and pretty dangerous for some.

This afternoon, I'm curious to what extent you can share with this committee what that day meant for our national security network. Were government installations also affected? Perhaps there may have been some learning, stepping back and watching, saying, "We were okay but …" If you could help me with that, that would be great.

avons-nous nos propres pare-feu en collaboration avec les États-Unis et d'autres alliés de l'OTAN? Je suppose que oui.

M. Khoury : Merci beaucoup de la question.

Ces cyberagents sont de plus en plus avertis. Nous constatons que les capacités qui étaient auparavant le propre des États-nations sont acquises par des organisations criminelles. Les cybercapacités criminelles sont de plus en plus développées. Elles s'échappent de la sphère gouvernementale. Nous constatons également que certains États-nations utilisent des capacités cybercriminelles pour brouiller les pistes et éviter d'être repérés.

Nous connaissons bien ces agents. Nous avons une bonne collaboration avec les États-Unis, évidemment. Notre infrastructure essentielle est connectée dans bien des cas. Nous devons collaborer avec nos alliés du Sud, mais aussi avec nos partenaires internationaux. Il y a un bon niveau de collaboration dans le domaine de la cybersécurité, non seulement au Canada, mais aussi entre le Canada et les États-Unis, entre le Canada, les États-Unis et le Royaume-Uni, avec le Groupe des cinq et avec la communauté internationale.

Le sénateur Richards : Diriez-vous que la Chine a plus de moyens de nous porter des coups que nous en avons de les bloquer en ce moment ou pensez-vous que nous sommes à égalité et que nous sommes aptes à repousser ces attaques?

M. Khoury : Je pense qu'il est difficile de comparer les situations. Au Centre pour la cybersécurité, notre priorité est de les neutraliser toutes, quel que soit leur degré de raffinement.

Le sénateur Richards : Je comprends.

M. Khoury : Qu'il s'agisse de la Chine, de la Russie, de l'Iran ou de la Corée du Nord, nous travaillons sans relâche pour nous assurer de les neutraliser toutes.

Le sénateur Richards : Merci.

La sénatrice M. Deacon : Je vais revenir en arrière. Certains sujets d'actualité sont importants et nous tiennent à cœur, mais je vais revenir en arrière et nous rappeler ce que nous avons ressenti pendant la panne de Rogers l'été dernier. Je fais référence à la question concernant la résilience de notre réseau de télécommunications. Nous avons beaucoup appris. Cela révèle à quel point les pannes prolongées d'Internet perturbent nos vies, du simple inconvénient à de réels problèmes de sécurité susceptibles de se révéler dangereux.

En cet instant précis, que pouvez-vous dire au comité sur ce que cette journée a signifié pour notre réseau de sécurité nationale? Les installations gouvernementales ont-elles également été touchées? Peut-être avez-vous appris quelque chose et que, avec le recul, vous vous êtes dit, par exemple : « On s'en est sorti, mais… » Si vous pouvez m'éclairer, ce serait vraiment bien.

Mr. Couillard: Thank you for the question. Absolutely, that was a unique event.

First of all, immediately when that started, we were in communication with Rogers, because obviously the question of whether this was a cybersecurity-driven event was on everybody's mind. We at the Cyber Centre have a great relationship with all of the telecom service providers in Canada. That comes in handy. I know they were talking to Sami right away. Obviously, they kept us informed of the event. Immediately, they made it clear that so far as the incident was involved — those are always dynamic. When they start, it's never clear what happened at the first moment, but clearly, the indication was that this was a non-cyber-related event. Lucky for us, that was the case.

What it did, though, to your point, absolutely, is showed the importance of how critical, essential infrastructure is dependent on one another. Obviously, some financial institutions were affected by this. It shows that resilience is a job that is never finished.

I cannot speak for Rogers on what happened, obviously, in their activity. There have been a few places where they came forward and explained that it was really — I would say for this place — a configuration issue of their network. How did that happen? Obviously, this merits a discussion with them, for sure.

The reality is that it showed a great step up by the various telecom service providers, realizing that they needed to work together and they needed to work in partnership with other federal entities. ISED, Innovation, Science and Economic Development Canada, also worked with us to engage the telecom service providers, and Rogers, to understand what happened and then learn from that. Our friends at ISED have been leading an activity where all the telecom service providers are now actively learning from this event and implementing — Minister Champagne was clearly demanding action by a Call to Action by the telecom service providers. That has been documented, and they are now delivering this. The industry stepped up to the plate and worked with us to address these things. There is a new protocol in place calling for action, and we are part of this. Of course, again, this was not a cyber event, but it could be a cybersecurity event in the future. The Cyber Centre has been part of those discussions and is included in the protocol for future events.

Senator M. Deacon: Thank you.

My colleague, Senator Dasko, asked a question related to today's *The Globe and Mail* article. With regard to cybersecurity in our Crown corporations, they noted that while the organizations are independent of government, they still operate

M. Couillard : Merci de la question. Cela a été, en effet, un événement unique.

Je dois dire tout d'abord que nous avons aussitôt communiqué avec Rogers, parce que la question de savoir si cela touchait la cybersécurité préoccupait tout le monde. Le Centre pour la cybersécurité entretient d'excellentes relations avec tous les fournisseurs de services de télécommunications au Canada. C'est bien pratique. Je sais qu'ils se sont immédiatement adressés à M. Khoury. Ils nous ont évidemment tenus au courant. Et ils ont clairement expliqué que ce genre d'incident est toujours évolutif. C'est-à-dire que, au début, on ne sait pas ce qui l'a déclenché, mais on savait que ce n'était pas un incident d'ordre cybernétique. Heureusement pour nous.

Mais, pour revenir à ce que vous disiez, cela nous a effectivement fait comprendre à quel point les infrastructures essentielles et cruciales dépendent les unes des autres. Certaines institutions financières ont bien entendu été touchées. Cela montre aussi que la résilience est une capacité que l'on n'a jamais fini d'améliorer.

Je ne peux pas parler pour Rogers, évidemment. Dans certains endroits, ils ont été proactifs en expliquant que c'était vraiment — pour l'endroit en question — un problème de configuration du réseau. Comment cela a-t-il pu se produire? Cela mériterait effectivement une discussion avec eux.

En fait, cela a incité les divers fournisseurs de services de télécommunications à prendre des mesures parce qu'ils se sont rendu compte qu'ils devaient travailler ensemble et en partenariat avec d'autres entités fédérales. ISDE, c'est-à-dire Innovation, Sciences et Développement économique Canada, a également collaboré avec nous pour faire participer les fournisseurs de services de télécommunications et Rogers, afin de comprendre ce qui s'était passé et d'en tirer des leçons. Nos amis d'ISDE ont organisé une activité permettant à tous les fournisseurs de services de télécommunications de tirer activement des leçons de cet événement et de prendre des mesures — le ministre Champagne a clairement formulé un appel à l'action à l'intention de ces fournisseurs. Cela a été documenté, et c'est ce qu'ils sont en train de faire. Les entreprises ont répondu à l'appel et ont travaillé avec nous. Un nouveau protocole, auquel nous sommes parties, a été élaboré pour passer à l'action. Je rappelle qu'il ne s'agissait pas d'un incident d'ordre cybernétique, mais cela pourrait toucher la cybersécurité un jour ou l'autre. Le Centre pour la cybersécurité a participé à ces discussions et est partie au protocole pour l'avenir.

La sénatrice M. Deacon : Merci.

Ma collègue, la sénatrice Dasko, a posé une question au sujet d'un article paru aujourd'hui dans le *Globe and Mail*. On peut y lire que, en matière de cybersécurité, nos sociétés d'État, quoique indépendantes du gouvernement, fonctionnent toujours

on the same network, acting as a kind of back door to more sensitive information. It was also said that just 5 of the 50 such federal entities use Enterprise Internet Service, which incorporates the technology from the CSE to better protect against threat. Could you comment on the implication in this article that this could act as a soft underbelly in cyberdefence?

Mr. Khoury: Thank you for the question.

We live in a more connected society, so making sure that our networks are secure is key. From a Cyber Centre perspective, besides government or core departments, we work with small departments, agencies and Crown corporations. We are available to provide cybersecurity support to any Crown corporation that reaches out to us, and we have done so in the past. It's more of a bilateral engagement on that front. The Treasury Board and CSE are trying to bring the collective of Crown corporations together, but in the interim, we are more than happy to work individually with any one of those Crown corporations.

Senator M. Deacon: Thank you.

[*Translation*]

The Deputy Chair: Before we get to the second round, I'm going to take the liberty of asking a very short question. Because of its proximity to the United States, could Canada be used as a computer base for cyberattacks targeting Americans?

Mr. Couillard: Thank you for your question. Obviously, Canada and the United States share a tremendous amount of critical infrastructure on the continent. We've mentioned before that the point of origin of an attack is not necessarily related to who is conducting that attack.

[*English*]

Based on that premise, it's possible that a foreign actor would leverage some infrastructure in Canada to launch an attack against the U.S. This is where we are building those relationships with a lot of our colleagues from the U.S. government. We have also built relationships with critical infrastructure operators, such as energy and telecommunications, where there is extensive connection with the U.S. infrastructure. We've also built relationships with private sector associations to build resilience together. That's a key priority for us during this time of the war in Ukraine. We gave advice to our critical infrastructure operators to proactively increase the level of awareness and security in relation to this threat and in thinking about these scenarios.

Senator Boehm: Mr. Khoury, you have answered the question in different ways. When they think of interference of this kind, most Canadians think of malign state actors. The state actors, as you have said, will cover up what they have done and

sur le même réseau et donnent ainsi accès indirectement à des renseignements plus confidentiels. On y apprend également que seulement 5 de ces 50 entités fédérales utilisent le Service Internet d'entreprise, qui intègre la technologie du CST pour mieux se protéger. L'article laisse entendre que cela pourrait constituer le ventre mou de la cyberdéfense : qu'en pensez-vous?

M. Khoury : Merci de la question.

Nous vivons dans une société plus connectée que jamais, de sorte qu'il est essentiel de veiller à ce que nos réseaux soient sécurisés. Outre le gouvernement et les principaux ministères, le Centre pour la cybersécurité collabore avec les petits ministères et organismes et avec les sociétés d'État. Nous pouvons fournir un soutien en matière de cybersécurité aux sociétés d'État qui nous le demandent, et c'est déjà arrivé. Il s'agit davantage d'un engagement bilatéral. Le Conseil du Trésor et le CST essaient de regrouper les sociétés d'État, mais entretemps, nous sommes plus qu'heureux de travailler individuellement avec l'une ou l'autre de ces sociétés.

La sénatrice M. Deacon : Merci.

[*Français*]

Le vice-président : Avant de passer au second tour, je vais me permettre de poser une très courte question. À cause de sa proximité avec les États-Unis, le Canada pourrait-il servir de base informatique pour des cyberattaques visant les Américains?

M. Couillard : Merci de votre question. Évidemment, le Canada et les États-Unis partagent énormément d'infrastructures critiques sur le continent. Nous avons déjà mentionné que le point de provenance d'une attaque n'est pas nécessairement lié à la personne qui mène cette attaque.

[*Traduction*]

Il est donc possible qu'un agent étranger utilise une infrastructure au Canada pour lancer une attaque contre les États-Unis. C'est pour cela que nous nouons ces relations avec beaucoup de nos collègues du gouvernement des États-Unis. Nous avons également créé des liens avec des exploitants d'infrastructures essentielles, par exemple dans les secteurs de l'énergie et des télécommunications, qui sont étroitement liés à l'infrastructure américaine. Nous avons également des relations avec des associations du secteur privé pour consolider la résilience avec eux. C'est une priorité fondamentale pour nous en cette période de guerre en Ukraine. Nous avons conseillé à nos exploitants d'infrastructures essentielles de relever proactivement le niveau de conscientisation et de sécurité à l'égard de cette menace et de réfléchir à ces éventualités.

Le sénateur Boehm : Monsieur Khoury, vous avez répondu à la question de diverses façons. Quand ils pensent à ce genre d'ingérence, la plupart des Canadiens pensent à des agents étatiques malveillants. Comme vous l'avez dit, les agents

perhaps push it into the direction of rogue actors. The rogue actors, in turn, might pretend that they are state actors. Through all of this, I guess you have to find the path as to what is what. Do you have a sense that the rogue actors — who may or may not be acting on behalf of state actors — are actually increasing their activities? Are there any related Canadian vulnerabilities, particularly in our defence sector, to that end?

Mr. Khoury: Thank you for the question.

I would say there are three camps. There is the purely cybercriminal camp, there is the nation-state camp, and there is the state-aligned rogue actor, so criminal organizations that are state-aligned. At the Cyber Centre, we have to defend against all of them. Whether it's a cybercriminal motivated by money, a nation-state motivated by espionage or stealing international property, or a rogue actor motivated by ideology, we have to defend against all three of them, and possibly more. The goal of the Cyber Centre is to make sure that we inform Canadians and Canadian businesses of the threat and adjust our publications to cater to the various types of attack actors we might see.

Senator Boehm: Would you also inform our closest allies and say, "Hey, we've found a new one here. Do you know about this one?" And would they do the same with us?

Mr. Khoury: We work closely with our allies — the U.S., U.K. and international partners. Our deepest partnerships are with the U.S., U.K. and Five Eyes partners. A lot of sharing takes place amongst the five of us in terms of intelligence sharing and cyberdefence. When it comes to cyberdefence, for the good of the community and for the good of Canadians, we push out as much information as possible.

Senator Boehm: Thank you.

[*Translation*]

Senator Boisvenu: You know this committee is conducting a study on Arctic security. Canada is poised to invest heavily in protecting the Arctic, especially in technology.

Are your ties with the Americans consistent? Will the exchange of information allow you, as an autonomous entity — even though you have ties to the Americans — to have a good view of what goes on in the Arctic, after the modernization and increased presence of technologies that are much more at risk than what we have today?

Mr. Khoury: Thank you for the question.

étatiques camouflent leurs actions et redirigent peut-être les projecteurs vers des agents voyous. Ces derniers, à leur tour, peuvent prétendre qu'ils sont des agents étatiques. Dans tout cela, je suppose que vous devez trouver le moyen de savoir qui fait quoi. Avez-vous l'impression que les agents voyous — susceptibles d'agir ou non au nom d'agents étatiques — sont en train de multiplier leurs activités? Y a-t-il des vulnérabilités connexes au Canada, notamment dans notre secteur de la défense, à cet égard?

M. Khoury : Merci de la question.

Disons qu'il y a trois camps. Il y a celui des cybercriminels à proprement parler, celui des États-nations et celui des agents voyous alignés sur un État, c'est-à-dire des organisations criminelles alignées sur un État. Le Centre pour la cybersécurité doit défendre le Canada contre tous ces agents. Qu'il s'agisse d'un cybercriminel motivé par l'argent, d'un État-nation faisant de l'espionnage politique ou industriel ou d'un agent voyou animé par une idéologie, nous devons nous défendre contre les trois, voire plus. L'objectif du Centre pour la cybersécurité est d'informer les Canadiens et les entreprises canadiennes de la menace et d'adapter nos publications en fonction des divers types d'agents à l'œuvre.

Le sénateur Boehm : Est-ce que vous informez nos alliés les plus proches en leur signalant un nouvel agent ou en leur demandant si tel autre leur est connu? Et font-ils la même chose avec nous?

M. Khoury : Nous travaillons en étroite collaboration avec nos alliés — les États-Unis, le Royaume-Uni et nos partenaires internationaux. Nos partenariats les plus étroits sont avec les États-Unis, le Royaume-Uni et les membres du Groupe des cinq. Les cinq partagent beaucoup de renseignement et de données sur la cyberdéfense. En matière de cyberdéfense, nous diffusons le plus d'information possible pour le bien de la collectivité et pour le bien des Canadiens.

Le sénateur Boehm : Merci.

[*Français*]

Le sénateur Boisvenu : Vous savez que ce comité mène une étude sur la sécurité dans l'Arctique. Le Canada s'apprête à investir massivement dans la protection de l'Arctique, surtout sur le plan technologique.

Vos liens avec les Américains sont-ils constants? Est-ce que l'échange d'information vous permettra, comme entité autonome — même si vous avez des liens avec les Américains —, d'avoir une bonne vision de ce qui va se passer dans l'Arctique après l'épisode de modernisation et de présence accrue de technologies qui sont beaucoup plus à risque que ce que nous avons aujourd'hui?

M. Khoury : Merci pour la question.

Indeed, in all of the government's technology projects, we try to bring in the cybersecurity component to support those developments and make them as secure as possible. We also participate in public forums with the private sector to invite companies to invest in cybersecurity. We try to make sure that cybersecurity is included in the definition of the problem, and not something that is added at the last minute. How do we make sure that cybersecurity is built into the development of a project so we don't regret its omission later? With that in mind, we hope that any investment projects in the North or in Indigenous communities, in particular, will be projects that have a good foundation in terms of cybersecurity.

Senator Boisvenu: Thank you.

[*English*]

Senator Dasko: I want to keep pursuing the topic of efforts to degrade our democratic institutions with disinformation. You gave one example. Could you give a few more examples of how this has happened and in which instances?

I also want to ask you this: What is it you do with this information? Do you do a risk analysis? Do you inform, let's say, government departments? Do you take on activities to answer the misinformation with correct information? How do you handle the information? Where does it go, and what happens to it in terms of the actions that might ultimately be taken, or not?

Mr. Khoury: Thank you, senator, for the question.

From a Cyber Centre perspective, we are definitely concerned about cybersecurity and the protection of Canadian information, government information and Canadian privacy. We work in concert with other partners, both inside CSE or with defence, with other agencies or departments within the government.

We are not a regulator, so in a sense we're not here to regulate what goes into cyberspace in terms of information content, but the CSE and other government departments have taken the sometimes rare measures to declassify intelligence to prove that information that is out there is not correct. From a Cyber Centre perspective, we want to make sure that the Canadian government infrastructure, or that of others, is not used in a malicious way or not used to promote that sort of misinformation. We have put out advice and guidance for Canadians. We have put out advice and guidance for social media applications. We are informing Canadians of the threat that some of these environments out there, social media apps and others, can pose to their privacy and security. That's the contribution of the Cyber Centre.

Effectivement, dans tous les projets technologiques du gouvernement, nous essayons d'amener le volet de la cybersécurité pour soutenir ces développements et les rendre les plus sécuritaires possibles. Nous participons aussi à des forums publics avec le secteur privé pour inviter les entreprises à investir dans la cybersécurité. Nous tentons de nous assurer que la cybersécurité est incluse dans la définition du problème et que ce n'est pas quelque chose qui est ajouté à la dernière minute. Comment nous assurons-nous que la cybersécurité est intégrée dans le développement d'un projet pour ne pas le regretter plus tard? Dans cette optique, nous espérons que tous les projets d'investissement dans le Nord ou dans les communautés autochtones, notamment, seront des projets qui auront une bonne fondation sur le plan de la cybersécurité.

Le sénateur Boisvenu : Merci.

[*Traduction*]

La sénatrice Dasko : J'aimerais poursuivre la conversation sur les actions visant à détériorer nos institutions démocratiques par la désinformation. Vous avez donné un exemple. Pourriez-vous nous parler d'autres incidents et de leur contexte?

Je voudrais aussi vous demander ceci : que faites-vous de cette information? Faites-vous une analyse des risques? Par exemple, informez-vous les ministères? Prenez-vous des mesures pour réagir à la désinformation en fournissant de l'information exacte? Comment traitez-vous l'information? Où va-t-elle et qu'en advient-il du point de vue des mesures susceptibles d'être prises?

M. Khoury : Je vous remercie de votre question, sénatrice.

Le Centre pour la cybersécurité se préoccupe évidemment de la cybersécurité et de la protection de l'information canadienne, de l'information gouvernementale et de la vie privée des Canadiens. Nous collaborons avec d'autres partenaires, au CST et à la Défense, et avec d'autres organismes ou ministères du gouvernement.

Nous ne sommes pas un organisme de réglementation et nous ne sommes donc pas chargés de réglementer le contenu d'information dans le cyberespace, mais le CST et d'autres ministères ont pris des mesures parfois rares pour déclassifier le renseignement afin de prouver que l'information diffusée n'était pas exacte. Le Centre pour la cybersécurité veut s'assurer que l'infrastructure du gouvernement canadien ou d'autres ne sevent pas à des fins malveillantes ou à la promotion de ce genre de désinformation. Nous avons publié des conseils et des recommandations à l'intention des Canadiens. Nous avons publié des conseils et des recommandations pour les applications des réseaux sociaux. Nous informons les Canadiens de la menace que certains de ces espaces, notamment les applications des réseaux sociaux, peuvent représenter pour leur vie privée et leur sécurité. C'est cela, la contribution du Centre pour la cybersécurité.

Senator Dasko: That would be at a high level that you're warning Canadians.

Mr. Khoury: Yes.

Senator Dasko: With regard to specific information, where does that go? When you collect the information about instances, whether it be within elections or I am thinking mainly outside elections when disinformation is disseminated, where does the information you pick up go?

Mr. Khoury: We would only pick up the technical information that supports or indicates that there has been a malicious cyber event. Other types of information would be picked up by other departments. I would probably defer to other departments to bring the content element of that information together and maybe answer that question.

Senator Dasko: I see. It would be handled by other departments.

Mr. Khoury: Yes.

Senator Cardozo: I want to come back to the domestic scene. In past decades, security forces have looked at terrorism as being something that would come from the outside. In the past few years, they have begun to understand that certainly there are forces within Canada, White supremacist being probably at the top of the list. Is it your sense that forces like that are active in the cyberworld? Do you watch groups within Canada as sources from where cyber-threats might come?

Mr. Khoury: Thank you.

To answer your question directly, no, we don't watch groups. The Cyber Centre is primarily concerned with the infrastructure layer and making sure that the infrastructure layer is secure from cyberattack. I would defer to other departments who have the mandate to monitor or to watch activities by groups. If the cyber event comes from outside of Canada, we can sometimes categorize it as cybercriminal or nation state. When nation states are behind a cyber event, if they cross those lines of cyber norms, the government might choose to call them out, but we don't look domestically at who is behind the keyboard.

Senator Cardozo: Your first focus is the hardware of the cyber system?

Mr. Khoury: Yes.

Senator Cardozo: But you also do look at where it's coming from?

La sénatrice Dasko : Les mises en garde que vous adressez aux Canadiens sont de haut niveau.

M. Khoury : Oui.

La sénatrice Dasko : Où vont certains renseignements précis? Quand vous recueillez des renseignements portant sur des cas précis, dans le cadre d'élections, mais surtout, je dirais, au sujet de la désinformation diffusée en dehors des élections, où vont les renseignements que vous recueillez?

M. Khoury : Nous ne recueillons que les renseignements techniques qui prouvent ou indiquent un cyberincident malveillant. Les autres types de renseignements sont recueillis par d'autres ministères. Il faudrait probablement s'adresser à eux pour réunir le contenu de cette information et peut-être répondre à cette question.

La sénatrice Dasko : Je vois. Cela incomberait à d'autres ministères.

M. Khoury : Oui.

Le sénateur Cardozo : Je voudrais revenir à la situation au pays. Au cours des dernières décennies, les forces de sécurité ont considéré que le terrorisme venait de l'extérieur. Dans les dernières années, elles ont commencé à comprendre qu'il y avait aussi des forces de ce genre au Canada, la suprématie blanche étant probablement en tête de liste. Avez-vous l'impression que ces forces sont actives dans le cyberespace? Est-ce que vous surveillez des groupes au Canada qui pourraient être la source de cybermenaces?

M. Khoury : Merci de la question.

Pour y répondre directement, non, nous ne surveillons pas de groupes. Le Centre pour la cybersécurité s'occupe principalement de l'infrastructure et veille à ce qu'elle soit protégée contre les cyberattaques. D'autres ministères sont chargés de surveiller les activités de groupes. Si le cyberincident a son origine à l'extérieur du Canada, nous pouvons parfois le classer parmi les incidents attribuables à des cybercriminels ou à des États-nations. Si ce sont des États-nations qui sont à l'origine de l'incident et s'ils franchissent les limites des normes cybernétiques, le gouvernement peut décider de les dénoncer, mais nous ne cherchons pas à déterminer qui se trouve au clavier à l'échelle nationale.

Le sénateur Cardozo : Vous vous concentrez d'abord sur le matériel informatique?

M. Khoury : Oui.

Le sénateur Cardozo : Mais vous voulez également savoir d'où vient l'argent, n'est-ce pas?

Mr. Khoury: Our first concern is the security of the infrastructure layer, so the network and hardware that underpins, but malicious cyber activities can come from anywhere in terms of who is behind those cyber activities. In some cases, we know that Russia, China, Iran and North Korea are perpetrators of some of these cyber activities, and they each have a different signature that informs us as to this is a typical Russian attack or typical Chinese attack. That's how we learn about how to better defend government systems and how to share that information with our partners to make sure that we stay on top of the threat that they pose.

Senator Yussuff: A very biased question to you directly: Given your responsibility, how would you say we're performing on the broader question of cybersecurity? This is something that is obviously very much topical to Canadians these days, given the issue of election interference.

Mr. Couillard: Thank you for the question.

It's a difficult question to answer. How do we perform? Our focus is to protect the Canadian government, Canadian infrastructure and Canada at large. That's the focus we have. It would be difficult for me to compare us to any other nation or institution like that.

We have a group of people dedicated to do this. We work collectively with our colleagues from the federal government, the provinces and our international partners, and we're committed to this. We are investing our time and effort to stay in line with the threat. As the threat evolves, we want to be moving forward and constantly blocking those threats and continuing our mission.

I think we're doing a good job, obviously. The Canadian taxpayers are getting something good out of us, and we're committed to this. Where we rank against others would be difficult for me to answer that.

Mr. Khoury: If I can add a few comments, over the years we have developed what I believe to be world-class cyberdefence capabilities that we circle the Canadian government with. These capabilities are the envy of many of our partners. They look to us on how we wrapped our hand around government departments with cyberdefence capabilities. From a GC perspective, I'm extremely proud of the work of the Cyber Centre. Everything we learn across the government or everything we learn from these 5 billion events that we see every day, we turn around and share with critical infrastructure and with small-to-medium-sized businesses as a way of taking that knowledge and putting it out there to raise the collective cyber resilience. We have some work to do, for sure, since we continue to see cyber incidents pretty much every day, but we are committed to supporting Canadians

M. Khoury : Notre première préoccupation est la sécurité de l'infrastructure, c'est-à-dire le réseau et le matériel informatique, mais les activités cybernétiques malveillantes peuvent venir de n'importe où. Dans certains cas, nous savons que la Russie, la Chine, l'Iran et la Corée du Nord sont responsables de certaines de ces activités cybernétiques, et chacune d'elles a une signature différente qui nous permet de savoir qu'il s'agit en fait d'une attaque russe ou chinoise classique. C'est ainsi que nous apprenons comment mieux défendre les systèmes gouvernementaux et comment partager cette information avec nos partenaires pour nous assurer de garder de l'avance sur la menace.

Le sénateur Yussuff : J'ai une question très tendancieuse à vous poser directement : compte tenu de votre responsabilité, comment, d'après vous, nous en tirons-nous généralement en matière de cybersécurité? C'est évidemment une question d'actualité pour les Canadiens en raison de l'enjeu de l'ingérence électorale.

M. Couillard : Merci de la question.

C'est une question à laquelle il est difficile de répondre. Comment nous en tirons-nous? Notre objectif est de protéger le gouvernement canadien, l'infrastructure canadienne et le Canada dans son ensemble. C'est ce sur quoi nous nous concentrons. Il me serait difficile de nous comparer à un autre pays ou à une autre institution.

Nous avons un groupe de personnes qui se consacrent à cette tâche. Nous travaillons en collaboration avec nos collègues du gouvernement fédéral et des provinces et avec nos partenaires internationaux; c'est notre engagement. Nous investissons temps et efforts pour rester en phase avec la menace. À mesure que celle-ci évolue, nous évoluons aussi et nous sommes déterminés à la bloquer et à poursuivre notre mission.

Je pense que nous faisons du bon travail, évidemment. Nous donnons et nous continuerons de donner de bons résultats aux contribuables canadiens. Il serait difficile pour moi de vous dire où nous nous situons par rapport à d'autres.

M. Khoury : Si vous me permettez d'ajouter quelques commentaires, nous avons progressivement développé ce que je crois être des capacités de cyberdéfense de calibre mondial qui protègent le gouvernement canadien. Ces capacités font l'envie de beaucoup de nos partenaires. Ils se tournent vers nous pour savoir comment nous protégeons les ministères grâce à ces capacités. Du point de vue du gouvernement du Canada, je suis extrêmement fier du travail du Centre pour la cybersécurité. Tout ce que nous apprenons au sein du gouvernement et tout ce que nous apprenons de ces 5 milliards d'incidents que nous constatons tous les jours est partagé avec les responsables des infrastructures essentielles et avec les petites et moyennes entreprises pour que ces connaissances soient diffusées et permettent d'accroître la cyberrésilience collective. Il est certain

and Canadian businesses as much possible to raise their collective cybersecurity.

Senator Yussuff: Quickly, I was going to ask you a question. Canadians take the internet for granted, like riding a bicycle or drinking a glass of water, but it's not so innocent in that regard. What level of confidence do we need to give Canadians about how we can better collectively deal with the reality? It's not as simple as what we would like to believe anymore?

Mr. Khoury: We have put out a lot of advice about how to better protect yourself on our website, and Canadians should pay attention to some of the advice and guidance that we put out: better passwords, enable multifactor authentication, patch. All these things will make us a more secure society. That advice is out there, and I would invite everybody to visit our website and have a quick peek at it.

[*Translation*]

The Deputy Chair: This brings us to the end of our first panel. Mr. Khoury and Mr. Couillard, thank you for your input and for taking the time to share your expertise on cybercrime with us. We greatly appreciate it.

We now turn to our second panel. For those of you joining us live, this meeting is about cyber threats to Canada's defence infrastructure. For this second panel, we are pleased to welcome Ms. Kristen Csenkey, Fellow, North American and Arctic Defence and Security Network, and PhD candidate, Balsillie School of International Affairs; Mr. Alex Wilner, Associate Professor of International Affairs, Norman Paterson School of International Affairs, Carleton University; and finally, via video conference, we welcome Dr. Christian Leuprecht, Professor, Department of Political Science and Economics, Royal Military College of Canada.

Thank you for joining us today. We will begin by asking you to make your opening remarks, followed by questions from the committee. I remind you that you each have five minutes for your opening statements. Ms. Csenkey, you have the floor.

[*English*]

Kristen Csenkey, Fellow, North American and Arctic Defence and Security Network, PhD Candidate, Balsillie School of International Affairs, as an individual: Good evening to the chair, deputy chair, committee members and other

que nous avons encore du travail à faire, puisqu'il se produit des cyberincidents presque tous les jours, mais nous sommes déterminés à aider les Canadiens et les entreprises canadiennes, dans toute la mesure du possible, à renforcer leur cybersécurité collective.

Le sénateur Yussuff : J'aurais une brève question à vous poser. Les Canadiens tiennent Internet pour acquis, comme faire de la bicyclette ou boire un verre d'eau, mais ce n'est pas si innocent à cet égard. Quel niveau de confiance devons-nous accorder aux Canadiens quant à la façon dont nous pouvons mieux composer collectivement avec la réalité? Ce n'est plus aussi simple que ce que nous aimerions croire, n'est-ce pas?

M. Khoury : Nous avons publié beaucoup de conseils sur la façon de mieux se protéger sur notre site Web, et les Canadiens devraient prêter attention à certains de ces conseils, par exemple de meilleurs mots de passe, l'authentification multifactorielle et les correctifs. Toutes ces mesures feront de nous une société plus sûre. Ces conseils sont publiés, et j'invite tout le monde à consulter notre site Web.

[*Français*]

Le vice-président : Cela nous amène à la fin de notre premier groupe. Messieurs Khoury et Couillard, je vous remercie de votre contribution et du temps que vous avez pris pour partager avec nous votre expertise en matière de cybercriminalité. Nous l'apprécions grandement.

Nous passons maintenant à notre deuxième groupe de témoins. Pour ceux qui nous rejoignent en direct, cette réunion porte sur les cybermenaces à l'endroit de l'infrastructure de la défense du Canada. Pour ce deuxième groupe de témoins, nous avons le plaisir d'accueillir Mme Kristen Csenkey, associée, Réseau sur la défense et la sécurité nord-américaines et arctiques, et candidate au doctorat, Balsillie School of International Affairs; M. Alex Wilner, professeur agrégé en matière d'affaires internationales à la Norman Paterson School of International Affairs de l'Université Carleton; enfin, par vidéoconférence, nous accueillons M. Christian Leuprecht, professeur au Département de science politique et d'économique du Collège militaire royal du Canada.

Je vous remercie de vous être joints à nous aujourd'hui. Nous allons commencer par vous demander de présenter vos remarques préliminaires, qui seront suivies de questions de la part des membres du comité. Je vous rappelle que vous disposez chacun de cinq minutes pour vos déclarations préliminaires. Madame Csenkey, vous avez la parole.

[*Traduction*]

Kristen Csenkey, associée, Réseau de défense et de sécurité de l'Amérique du Nord et de l'Arctique, candidate au doctorat, Balsillie School of International Affairs, à titre personnel : Je salue le président, le vice-président, les membres

experts called to this meeting. I thank you for the invitation to address the committee, and I am honoured to participate in the important discussion on cyber-threats to Canada's defence infrastructure.

I am a PhD candidate at the Balsillie School of International Affairs through Wilfrid Laurier University and a fellow with the North American and Arctic Defence and Security Network. My remarks are based on my academic research on cyber governance and the management of emerging technologies. It is through my research and previous publications where I situate my approach to the discussion topic for the committee.

My remarks on the topic of cyber-threats to Canada's defence infrastructure are organized around two themes: complexity and interoperability. I will link these two themes by using the conceptual image of a chain to think about threats and solutions. These themes highlight the challenges that Canada faces today, and I hope this will aid in your examination of the issue.

To begin, when we talk about infrastructure, whether defence, critical or civilian, we are talking about complex cyber-physical systems. Broadly, these infrastructures are comprised of different technologies, devices, software, hardware and information, but also of services, people and other connected things requiring energy sources and physical locations. Each one of these things in cyber-physical systems are similar to links in a chain. They each have their place, but they are also fastened to other links in the chain. Links can connect in many ways and become weaved together to create bigger structures. Complexity comes as these interconnections comprise large infrastructures, bringing challenges especially from a defence perspective.

Defence infrastructures are complex, and their connections, or links, go beyond a single field, but they also have sector-specific challenges, for example, the defence-specific challenge of secure cloud computing for distributed command and control. These systems can enable effective communication and coordination across an operating environment, yet they require more than secure cyber systems to make them functional. Among other requirements, they need a reliable and safe power source that can function in diverse and extreme locations, such as a portable high-performance microgrid. This infrastructure is not unique to defence, as these technologies could be used in other contexts and for other purposes. In addition, each of these things may need to connect to older or legacy technologies and systems still in use today. The interoperability of these new technologies and systems is an issue not only from a functional standpoint, but also because it provides opportunity for malicious cyber-threat actors to disrupt systems that link multiple infrastructures.

du comité et les autres experts convoqués à cette réunion. Je vous remercie de m'avoir invitée à prendre la parole devant vous et je suis honorée de participer à cette importante discussion sur les cybermenaces visant l'infrastructure de défense du Canada.

Je suis doctorante à la Balsillie School of International Affairs de l'Université Wilfrid Laurier et membre du Réseau de défense et de sécurité de l'Amérique du Nord et de l'Arctique. Mes observations s'appuient sur mes recherches concernant la cybergouvernance et la gestion des technologies émergentes. Mes recherches et mes publications antérieures m'ont permis de circonscrire ma perspective sur le sujet de discussion du comité.

Mes observations sur les cybermenaces visant l'infrastructure de défense du Canada s'articulent autour de deux thèmes : la complexité et l'interopérabilité. Je vais lier les deux en utilisant l'image conceptuelle d'une chaîne pour réfléchir aux menaces et aux solutions. Ces thèmes éclairent les enjeux auxquels le Canada est confronté aujourd'hui, et j'espère que cela vous aidera dans votre examen de la question.

Pour commencer, quand on parle d'infrastructure, qu'il s'agisse de défense, de services essentiels ou de services civils, on parle de systèmes cyberphysiques complexes. Ces infrastructures comprennent généralement des technologies, des appareils, des logiciels, du matériel et de l'information différents, mais aussi des services, des personnes et d'autres éléments connectés qui nécessitent des sources d'énergie et des emplacements physiques. Les éléments des systèmes cyberphysiques ressemblent aux maillons d'une chaîne. Ils ont chacun leur place, mais ils sont aussi attachés à d'autres maillons. Les maillons peuvent être reliés de bien des façons et former de plus grandes structures. La complexité tient au fait que ces interconnexions composent de grandes infrastructures et rendent la tâche difficile, surtout du point de vue de la défense.

Les infrastructures de défense sont complexes, et leurs connexions, ou leurs maillons, ne relèvent pas d'un seul domaine, mais engagent aussi des enjeux sectoriels, par exemple celui de la défense de l'informatique en nuage pour le commandement et le contrôle distribués. Ces systèmes facilitent une communication et une coordination efficaces dans un environnement opérationnel, mais ils nécessitent plus que des cybersystèmes sécurisés pour être fonctionnels. Entre autres exigences, ils ont besoin d'une source d'énergie fiable et sûre qui puisse fonctionner dans des lieux aussi divers qu'extrêmes, comme un microréseau portatif à haut rendement. Ce genre d'infrastructure n'est pas propre à la défense, puisque ces technologies peuvent être employées dans d'autres contextes et à d'autres fins. Par ailleurs, chacun de ces éléments pourrait devoir être relié à des technologies et systèmes plus anciens ou hérités encore utilisés aujourd'hui. L'interopérabilité de ces nouveaux systèmes et technologies est un problème non seulement du point de vue fonctionnel, mais aussi parce qu'elle permet aux agents malveillants de cybermenaces de perturber des systèmes reliant de multiples infrastructures.

With the challenges of complexity and interoperability in mind, how can Canada protect against cyber-threats to defence infrastructures? The interconnectedness of systems, technologies, people, etc., is our current reality as services and interactions are increasingly digitalized and interdependent. This also poses unique capabilities and capacity challenges from a defence perspective, especially in protecting against threats targeted at the individual links in the metaphorical chain. The chain must be flexible and strong. It must be built to adapt to the changing environment and allow for pivots. This can mean resiliency by strengthening the links through cooperation in trusted partnerships. In the cloud computing system example, cooperation through standardization can ensure secure networked integration of the connected technologies shared between partners and across sectors. This solution is akin to transforming each link in the complex defence infrastructure into a strong chainmail, thereby enhancing Canada's ability to remain strong and safe.

I thank you for your time, and I look forward to your questions.

[*Translation*]

The Deputy Chair: Thank you very much, Ms. Csenkey. Now we'll hear from Mr. Wilner. Mr. Wilner, you may begin.

[*English*]

Alex Wilner, Associate Professor of International Affairs, Norman Paterson School of International Affairs, Carleton University, as an individual: Honourable senators, colleagues and friends, my opening statement will provide insights along two general themes. First, I want to provide a synopsis of contemporary cyber challenges with lessons from authoritarian use of cyberspace and the conflict in Ukraine, and second, I want to briefly explore two elements of Canadian cyber deterrence, largely based on my research, which is funded by SSHRC, DND and the Government of Ontario.

Cybersecurity is our era's defining challenge. Most national security and intelligence bodies have placed cybersecurity well ahead of other concerns, including transnational terrorism. Indeed, recently, the meaning of "cyber" itself, especially when used as a prefix, has expanded. A broadened understanding of cyber now includes humans and their societies; machines, computers, and networks; and the digital spaces and the ideas shared within them. Indeed, several emerging trends are shaping contemporary cybersecurity and, by extension, informing the future of conflict.

Compte tenu des enjeux liés à la complexité et à l'interopérabilité, comment le Canada peut-il se protéger contre les cybermenaces visant les infrastructures de défense? L'interconnectivité des systèmes, des technologies, des personnes, etc., est notre réalité actuelle, puisque les services et les interactions sont de plus en plus numérisés et interdépendants. Cela soulève également des questions nouvelles en matière de capacité de défense, surtout du côté de la protection contre les menaces visant les maillons individuels de la chaîne métaphorique. La chaîne doit être à la fois souple et solide. Elle doit pouvoir s'adapter à l'évolution du contexte et permettre des articulations. La résilience pourrait ainsi passer par la consolidation des maillons grâce à la coopération dans le cadre de partenariats de confiance. Dans le cas de l'informatique en nuage, la coopération par la normalisation peut assurer l'intégration en réseau sécurisé des technologies connectées que partagent des partenaires et des secteurs. Cette solution revient à transformer chaque maillon de l'infrastructure complexe de défense en une cotte de mailles solide, améliorant ainsi la capacité du Canada à rester fort et en sûreté.

Je vous remercie du temps que vous m'avez accordé et je me ferai un plaisir de répondre à vos questions.

[*Français*]

Le vice-président : Merci beaucoup, madame Csenkey. Maintenant, nous allons entendre M. Wilner. Monsieur Wilner, vous pouvez commencer.

[*Traduction*]

Alex Wilner, professeur agrégé des affaires internationales, Norman Paterson School of International Affairs, Université Carleton, à titre personnel : Honorables sénateurs, chers collègues et amis, mon exposé préliminaire portera sur deux thèmes généraux. J'aimerais d'abord vous parler brièvement des enjeux cybernétiques contemporains en évoquant l'utilisation autoritaire du cyberespace et le conflit en Ukraine. J'aborderai ensuite rapidement deux éléments de la cyberdissuasion canadienne, surtout à partir de ma recherche, qui est financée par le CRSH, le MDN et le gouvernement de l'Ontario.

La cybersécurité est l'enjeu décisif de notre époque. La plupart des organismes de sécurité nationale et de renseignement placent la cybersécurité bien au-dessus des autres préoccupations, y compris le terrorisme transnational. De fait, le sens du préfixe « cyber » s'est récemment élargi. Pour mieux comprendre la cybernétique aujourd'hui, il faut inclure les êtres humains et leurs sociétés, les machines, les ordinateurs et les réseaux, ainsi que les espaces numériques et les idées partagées dans ces espaces. On constate que plusieurs tendances émergentes donnent forme à la cybersécurité contemporaine et, par extension, éclairent l'avenir des conflits.

First, open-source data of state-sponsored cyber incidents show that since 2005, over 30 countries have launched offensive cyber operations, and yet China, Russia, Iran and North Korea are responsible for over 75 percent of these events. Cyberspace may be open to everyone, but its malicious use is reserved to a few.

Second, different authoritarian regimes prefer certain types of cyber aggression. Russia largely uses cyber to sow disinformation in the hope of shaping foreign behaviour and beliefs. It does the same domestically to impede political challenges. Conversely, China favours using cyber for espionage, data theft and intelligence-gathering purposes. Finally, North Korea, a relative cyber minnow, uses cyber aggression to generate state revenue through financial theft, ransomware and other forms of extortion. Of course, besides these regimes, democratic states also show patterns of cyber behaviour. Nearly 30 percent of known American cyber operations, for instance, are conducted with allies, something that should resonate with us.

A third series of cyber trends emanate from Russia's war of aggression against Ukraine. It is, to my mind, the first truly modern war, pitting two hi-tech societies against one another. Four lessons stand out.

First, the war has shifted Russia's cyber preferences. Before the war, less than a quarter of Russia's cyberattacks might have been deemed destructive in nature, whereas today, more than two thirds are meant to be.

Second, despite this, Russia's vaunted cyber capabilities have largely fallen flat. NATO observers have been warning of a cyber Pearl Harbor for a decade. Something like it seemed almost imminent in the weeks preceding Russia's invasion of Ukraine, but clearly that didn't happen. At the onset of the war, Russia's cyber campaign didn't come close to landing a knockout punch. Ukrainian preparations for it, following a decade of collaboration with the U.S., Canada and many others, helped to prevent it. This past winter, Russia failed again to knock Ukraine's energy systems offline, something it did repeatedly and rather easily in the past. Instead, since October 2022, Russia has resorted to massive physical destruction rather than cyber disruption of Ukrainian energy infrastructure.

Third, the conflict has brought entire commercial industries not generally accustomed to warfare to the very frontline of a shooting war. Tech companies like Microsoft have helped Ukraine fend off hacks by providing it with security services and

Premièrement, les données de sources ouvertes sur les cyberincidents attribuables à des États révèlent que, depuis 2005, plus de 30 pays ont lancé des cyberopérations offensives, mais que la Chine, la Russie, l'Iran et la Corée du Nord sont responsables de plus de 75 % de ces incidents. Le cyberespace est peut-être ouvert à tout le monde, mais son utilisation malveillante est réservée à quelques-uns.

Deuxièmement, les régimes autoritaires ont leurs préférences en matière de cyberattaque. La Russie utilise largement la cybernétique pour semer de la désinformation dans l'espoir de façonner les comportements et les croyances à l'étranger. Elle fait la même chose chez elle pour écarter les problèmes politiques. De son côté, la Chine préfère utiliser la cybernétique pour faire de l'espionnage, voler des données et recueillir du renseignement. Enfin, la Corée du Nord, petit joueur dans le domaine, passe par la cyberagression pour augmenter les recettes de l'État par le vol financier, le rançongiciel et d'autres formes d'extorsion. Les États démocratiques affichent eux aussi, bien sûr, des modèles de cybercomportement. Par exemple, près de 30 % des cyberopérations américaines connues concernent leurs alliés, ce qui devrait nous interpeller.

La guerre d'agression de la Russie contre l'Ukraine révèle une troisième série de tendances. À mon avis, c'est la première véritable guerre moderne, qui oppose deux sociétés de haute technologie. Quatre leçons ressortent.

Premièrement, la guerre a modifié les préférences cybernétiques de la Russie. Avant la guerre, moins du quart des cyberattaques de la Russie auraient pu être considérées comme ayant des visées destructrices, alors qu'aujourd'hui, plus des deux tiers le sont.

Deuxièmement, malgré cela, les capacités cybernétiques vantées par la Russie sont en grande partie en échec. Depuis une décennie, les observateurs de l'OTAN nous avertissent de l'éventualité d'un Pearl Harbor cybernétique. Quelque chose de cet ordre semblait presque imminent dans les semaines qui ont précédé l'invasion de l'Ukraine par la Russie, mais, comme on le sait, cela ne s'est pas produit. Au début de la guerre, la campagne cybernétique de la Russie était loin d'avoir atteint son but. Les préparatifs de l'Ukraine à cet égard, après une décennie de collaboration avec les États-Unis, le Canada et de nombreux autres pays, ont contribué à l'empêcher. L'hiver dernier, la Russie a encore une fois échoué à mettre hors service les systèmes énergétiques de l'Ukraine, ce qu'elle avait pu faire à maintes reprises et assez facilement dans le passé. Au lieu de cela, depuis octobre 2022, la Russie a eu recours à la destruction physique massive plutôt qu'à la cyberperturbation des infrastructures énergétiques ukrainiennes.

Troisièmement, le conflit a amené des secteurs commerciaux entiers, généralement peu familiers de la guerre, sur la ligne de front du combat. Des entreprises technologiques comme Microsoft ont aidé l'Ukraine à se prémunir contre le piratage

engineering solutions and by openly identifying, attributing and tracking Russian attacks. At one point, Microsoft opened a 24-7 cybersecurity hotline dedicated to ridding Ukraine of Russian malware sitting on its networks. Other companies, like Starlink — a satellite internet constellation operated by SpaceX — became an integral aspect of Ukraine's war effort. Starlink internet has proven difficult to target, hack and disrupt. The capability has sharpened Ukrainian operations and targeting. It has ensured broadband connectivity between troops and decision makers, and it enabled Ukrainian innovations in drone warfare, a startup effort that has paired homegrown software and hobby drones with satellite internet. This latter innovation has rankled SpaceX, which limited certain services over Ukraine last month, providing us all with a stark lesson on the emerging nexus between commercial internet services, statecraft and war.

informatique en lui fournissant des services de sécurité et des solutions techniques et en identifiant, en attribuant et en suivant ouvertement les attaques russes. À un moment donné, Microsoft a ouvert une ligne d'assistance en cybersécurité 24 heures sur 24, sept jours sur sept, pour débarrasser l'Ukraine des maliciels russes sur ses réseaux. D'autres entreprises, comme Starlink, une constellation Internet par satellite exploitée par SpaceX, sont devenues un élément essentiel de l'effort de guerre de l'Ukraine. Starlink Internet s'est révélé difficile à cibler, à pirater et à perturber. Cette capacité a renforcé les opérations et le ciblage en Ukraine. Elle a assuré la connectivité à large bande entre les troupes et les décideurs et a permis à l'Ukraine d'innover dans la guerre des drones, grâce à un jumelage des logiciels locaux et des drones récréatifs à l'Internet par satellite. Cette dernière innovation a irrité SpaceX, qui a limité certains services au-dessus de l'Ukraine le mois dernier, nous donnant à tous une dure leçon sur le lien émergent entre les services Internet commerciaux, la gouvernance et la guerre.

The conflict illustrates with clarity that cyberwar now stretches from the device in your hand, to the satellite providing it with connectivity, to the apps informing operations, to the drones providing real-time intelligence, to the GoFundMe campaigns that supply military kit, to the ideas and to the communities celebrating each and every Ukrainian success.

Le conflit illustre clairement que la cyberguerre va désormais de l'appareil que vous avez en main au satellite qui lui fournit une connectivité en passant par les applications qui alimentent les opérations, les drones qui fournissent du renseignement en temps réel, les campagnes GoFundMe qui permettent de financer l'acquisition de matériel militaire, les idées, et les collectivités qui célèbrent chaque succès ukrainien.

Of course, take these findings with a grain of salt. I am using imperfect, open-source information to assess the murky world of cyber statecraft in which subterfuge and deception are often the name of the game.

Il faut, bien sûr, prendre ces résultats avec un grain de sel. J'utilise de l'information imparfaite et de source ouverte pour évaluer le monde trouble de la cybercriminalité, dans lequel les subterfuges et les supercheries sont souvent la règle.

In response to these emerging trends, let me turn briefly to a rather quick discussion of cyber deterrence. In theory, deterrence entails an absence of open conflict, but in practice it relies on a combination of threats, like the sting of retaliation, the hindrance of defence and denial and the reputational cost of delegitimization.

Face à ces nouvelles tendances, voyons brièvement ce qu'il en est de la cyberdissuasion. En théorie, la dissuasion suppose l'absence de conflit ouvert, mais, dans la pratique, elle repose à la fois sur des menaces, comme l'incitation aux représailles, sur l'entrave à la défense et le déni, et sur le coût de la délégitimisation de la réputation.

For Canadian cyber deterrence, two considerations stand out. First, cyber deterrence will rest on a whole-of-government application. It isn't exclusively about hard power or threats of punishment, nor must our punitive responses rest within cyberspace alone. Instead, cyber deterrence should rely on a range of capabilities that can harm challengers in both cyber and physical space. At times, DND and CSE will be called upon to take action, so Canada must ensure that both have the technical capability to do so. Besides them, RCMP and Justice also have a role to play with prosecutions, Global Affairs with economic sanctions, and Shared Services by denying services attack. Cyber deterrence also needs to be nimbly communicated. I don't think Canada has a deterrence posture; we have never had one. My

En matière de cyberdissuasion, deux éléments entrent notamment en ligne de compte au Canada. Premièrement, la cyberdissuasion reposera sur une application pangouvernementale. Il ne s'agit pas exclusivement de strict pouvoir coercitif, et nos mesures punitives ne doivent pas viser uniquement le cyberespace. La cyberdissuasion devrait plutôt s'appuyer sur un éventail de capacités susceptibles de nuire aux adversaires dans le cyberespace et dans l'espace physique. À l'occasion, le MDN et le CST seront appelés à intervenir, et le Canada doit donc s'assurer que les deux en ont la capacité technique. En outre, la GRC et le ministère de la Justice ont également un rôle à jouer dans les poursuites, Affaires mondiales dans les sanctions économiques et Services partagés dans la

second recommendation ultimately is that Canada needs to think about cyber deterrence, but also how to communicate it at best.

Thank you.

[*Translation*]

The Deputy Chair: Thank you very much for your presentation, Mr. Wilner. I now yield the floor to Mr. Christian Leuprecht.

Christian Leuprecht, Professor, Department of Political Science and Economics, Royal Military College of Canada, as an individual: Thank you for the invitation, Mr. Deputy Chair. I will speak in English, but please feel free to ask me questions in both official languages. My remarks will follow upon what you just heard.

[*English*]

Harvard University's Belfer Center Cyber Power Index ranks Canada in eighth place as a comprehensive global cyber power. The CPI characterizes Canada as a high-intent, low-capacity cyber power with notable strengths in cyberdefence, cyber norms development initiatives and surveillance. By contrast, Canada's intent and capability to conduct cyber-enabled foreign intelligence and offensive cyber operations places it in the middle of the CPI pack, lagging Russia, China, the Five Eyes partners, the Netherlands, Israel and so on. On the one hand, the CPI's evaluation of Canada reflects two decades of Canadian cybersecurity initiatives; on the other hand, the ranking shows that Canada has a strategic cyber deficit.

For 20 years, cyber diplomacy has largely failed to generate broad agreement on international norms to constrain malicious behaviour by state-based and state-tolerated actors in cyberspace. To deter and constrain bad behaviour, Western states need to engage, using active and offensive cyber measures. This is what the U.S. doctrine of persistent engagement has been enabling since 2018. However, no U.S. ally comes close to matching U.S. resources and capabilities.

In 2019, the passage of Bill C-59 expanded the role and impact Canada could have in cyberspace by authorizing CSE to conduct offensive cyber operations. The addition of these capabilities to CSE'S mandate was hailed as a major step in aligning Canada's cyber operations authorities with its Five Eyes allies. In theory, the combination of foreign intelligence, active protection contre les attaques visant les services. La cyberdissuasion doit également être communiquée habilement. Je ne pense pas que le Canada ait une position de dissuasion, et cela n'a jamais été le cas. Ma deuxième recommandation serait, en fait, que le Canada réfléchisse à la cyberdissuasion, mais aussi à la meilleure façon de la communiquer.

Merci.

[*Français*]

Le vice-président : Merci beaucoup de votre présentation, monsieur Wilner. Nous allons maintenant céder la parole à M. Christian Leuprecht.

Christian Leuprecht, professeur, Département de science politique et d'économique, Collège militaire royal du Canada, à titre personnel : Merci pour l'invitation, monsieur le vice-président. Je vais m'exprimer en anglais, mais n'hésitez pas à me poser des questions dans les deux langues officielles. Mon intervention est un bon prolongement aux propos que vous venez d'entendre.

[*Traduction*]

Le Belfer Center Cyber Power Index de l'Université Harvard classe le Canada au huitième rang des cyberpuissances mondiales. L'Index des cyberpuissances décrit le Canada comme une puissance à faible capacité et à forte intention, dotée de forces notables en matière de cyberdéfense, d'initiatives d'élaboration de normes cybernétiques et de surveillance. En revanche, l'intention et la capacité du Canada de mener des cyberopérations de renseignement étranger et des cyberopérations offensives le placent au milieu du peloton de tête de l'Index, devançant la Russie, la Chine, les partenaires du Groupe des cinq, les Pays-Bas, Israël, etc. D'une part, l'évaluation du Canada traduit deux décennies d'initiatives canadiennes en matière de cybersécurité et, d'autre part, le classement montre que le Canada a un cyberdéficit stratégique.

Pendant 20 ans, la cyberdiplomatie n'a pas réussi à dégager de large consensus sur les normes internationales visant à limiter les comportements malveillants des agents étatiques et des agents tolérés par les États dans le cyberespace. Pour décourager et limiter les mauvais comportements, les États occidentaux doivent s'engager et utiliser des cybermesures actives et offensives. C'est ce que la doctrine américaine de l'engagement durable permet depuis 2018. Cependant, aucun allié des États-Unis n'a de ressources et de capacités ayant une commune mesure avec celles des Américains.

En 2019, l'adoption du projet de loi C-59 a permis d'élargir le rôle et l'impact que le Canada pourrait avoir dans le cyberespace en autorisant le CST à mener des cyberopérations offensives. L'ajout de ces capacités au mandat du CST a été salué comme une étape importante dans l'harmonisation des autorités canadiennes en matière de cyberopérations avec leurs alliés du

cyber operations and defensive cyber operations mandates enables the full spectrum of cyber espionage, sabotage and subversion operations. Canada now has capacity but it lacks political will to demonstrate independent international leadership to reduce instability and uncertainty in cyberspace.

I propose a cyber doctrine of functional engagement to bolster tacitly accepted norms. Regularly employing cyber capabilities is the most effective way for Canada to reduce uncertainty in cyberspace and limit threats to its national interests. Due to Canada's resource constraints and limited foreign policy ambitions, functional engagement prescribes that Canada employs the full range of its cyber capabilities to establish and reinforce a limited set of clearly defined and communicated focal points to deter and constrain unacceptable behaviour in cyberspace.

Instead of continuously and globally employing cyber capabilities to change the balance of power in the international system, functional engagement calls for Canada to employ its cyber capabilities more narrowly in specific instances when a malicious cyber actor conducts activity that is antithetical to Canada's focal points. Those focal points of unacceptable behaviour could include malicious activities such as directly degrading Canada's sovereignty and the security of people, degrading or subverting international law and the integrity of international, electoral or democratic institutions, and undermining Canada's economic security, competitiveness and prosperity. The proposed cyber doctrine of functional engagement seeks to shape adversarial behaviour cumulatively by strengthening the tacitly accepted cyber norms within the limited resources and unique character of Canada's historical leadership on foreign policy niches as a traditional middle power.

[*Translation*]

Thank you.

The Deputy Chair: Thank you very much, Mr. Leuprecht. We will now proceed to questions. I remind the committee that we have until 6:10 p.m. for this panel. So each question, including answers, will be limited to four minutes. We ask that you be brief and identify the person to whom you wish to direct your question. We will begin with Senator Boisvenu.

Senator Boisvenu: Welcome to our witnesses and thank you for your very informative testimony.

Groupe des cinq. En théorie, la combinaison du renseignement étranger, des cyberopérations actives et des cyberopérations défensives couvre l'éventail complet des opérations de cyberespionnage, de sabotage et de subversion. Le Canada a maintenant la capacité nécessaire, mais il n'a pas la volonté politique d'assumer un leadership international indépendant pour réduire l'instabilité et l'incertitude dans le cyberespace.

Je propose une doctrine cybernétique d'engagement fonctionnel pour consolider les normes tacitement acceptées. L'utilisation régulière de cybercapacités est la façon la plus efficace pour le Canada de réduire l'incertitude dans le cyberespace et de limiter les menaces visant ses intérêts nationaux. Compte tenu de nos ressources restreintes et de nos ambitions limitées en matière de politique étrangère, l'engagement fonctionnel supposerait que le Canada utilise toute la gamme de ses cybercapacités pour établir et consolider une série limitée de centres névralgiques clairement définis et communiqués, afin de décourager et de limiter les comportements inacceptables dans le cyberespace.

Au lieu d'utiliser continuellement et à l'échelle mondiale des cybercapacités pour modifier l'équilibre global des pouvoirs dans le système international, l'engagement fonctionnel demande au Canada d'employer ses cybercapacités de manière plus étroite, dans des cas précis, lorsqu'un cyberacteur malveillant mène une activité antithétique aux points focaux du Canada. Ces points focaux de comportements inacceptables pourraient inclure des activités malveillantes qui portent directement atteinte à la souveraineté du Canada et à la sécurité des personnes, qui dégradent ou subvertissent le droit international et l'intégrité des institutions internationales, électorales ou démocratiques, et qui sapent la sécurité économique, la compétitivité et la prospérité du Canada. La cyberdoctrine d'engagement fonctionnel proposée vise à façonner le comportement contradictoire de manière cumulative en renforçant les normes cybernétiques tacitement acceptées dans le cadre des ressources limitées et du caractère unique du leadership historique du Canada sur les créneaux de la politique étrangère en tant que puissance moyenne traditionnelle.

[*Français*]

Je vous remercie.

Le vice-président : Merci beaucoup, monsieur Leuprecht. Nous allons maintenant passer aux questions. Je rappelle aux membres du comité que nous avons jusqu'à 18 h 10 pour ce groupe de témoins. Chaque question, y compris les réponses, sera donc limitée à quatre minutes. Nous vous demandons d'être brefs et d'identifier la personne à laquelle vous voulez adresser votre question. Nous allons commencer avec le sénateur Boisvenu.

Le sénateur Boisvenu : Bienvenue à nos invités et merci pour vos témoignages très enrichissants.

My question is for Mr. Leuprecht. Your description of the cybersecurity situation in Canada is worrisome.

I would like to hear your thoughts on the strategy Canada should take immediately in view of the future redeployment in the North, in the Arctic, in order to reach the same level of technology as the Americans. We have just returned from a visit to NORAD, in Colorado Springs, which showed us how far out of step Canada is with the agreement concluded for North America. That gives us an idea of the discrepancy we are facing as regards cybersecurity management.

What are your thoughts on harmonizing the cybersecurity strategy with the massive investments that have to be made in the Arctic?

Mr. Leuprecht: That is an interesting question. I sent you my latest book, *Polar Cousins: Comparing Antarctic and Arctic Geostrategic Futures*, which examines in detail the threatening activities that Russia and China are conducting in both polar regions.

As you pointed out, cybersecurity and kinetic approaches have to be combined because the current threats in the Arctic and Antarctic and the resulting instability will have a huge impact on overall global stability. So neglecting the Arctic and not investing in that region will have a major impact on Canada's interests elsewhere in the global system.

Canada therefore has strategic weaknesses relating to kinetics and cybersecurity. As you indicated, the recent AUKUS security pact is not simply an alliance involving nuclear submarines; it is also a technological alliance between our closest partners. Canada chose not to be part of the most important alliance in the world for sharing advanced technology. As for National Defence, it has used constraints and dissuasion against hostile states.

Senator Boisvenu: Was it Canada that decided not to participate or was it not invited?

Mr. Leuprecht: I would say it is a two-way street, but Canada has failed to invest in national security, intelligence and defence for a number of years. As a result, Canada is increasingly excluded from the conversations, dialogues and partnerships among our closest allies. Canada is increasingly marginalized and that is a problem, because these partners provide tremendous added value for our national interests. So we are less and less able to protect our national interests because we are being marginalized by our closest partners.

Ma question s'adresse à M. Leuprecht. Ce que vous faites comme description du Canada en matière de cybersécurité est inquiétant.

J'aimerais avoir votre point de vue sur la stratégie que le Canada devrait employer immédiatement en vue du redéploiement qui va se faire dans le Nord du Canada, dans l'Arctique, dans le but d'être au même niveau technologique que les Américains. Nous arrivons d'une visite du NORAD, à Colorado Springs, qui nous a montré à quel point le Canada était décalé à l'extérieur de cette entente conclue pour l'Amérique du Nord. Cela nous donne une idée du décalage que nous avons sur le plan de la gestion de la cybersécurité.

Quel serait votre point de vue sur une harmonisation entre la stratégie en matière de cybersécurité et les investissements massifs qui doivent être faits dans l'Arctique?

M. Leuprecht : C'est une question intéressante. Je vais vous faire parvenir mon dernier livre, *Polar Cousins : Comparing Antarctic and Arctic Geostrategic Futures*, qui parle en détail des activités menaçantes menées par la Russie et la Chine dans les deux régions polaires.

Comme vous l'avez identifié, il faut une combinaison des approches de cybersécurité et des approches cinétiques, car les menaces qui existent dans l'Arctique et l'Antarctique et l'instabilité qui s'ensuivra auront des conséquences très importantes pour toute la stabilité globale. Donc, le fait de ne pas porter attention à l'Arctique et de ne pas investir dans cette région aurait des conséquences très importantes pour les intérêts du Canada ailleurs dans le système global.

Il y a donc des manques par rapport au déficit stratégique du Canada dans les domaines de la cinétique et de la cybersécurité. Comme vous l'avez bien dit, le récent pacte de sécurité AUKUS n'est pas seulement une alliance ayant trait aux sous-marins à propulsion nucléaire; c'est aussi une alliance technologique conclue entre nos plus proches partenaires. Le Canada a choisi de ne pas faire partie de la plus importante alliance d'échange de technologies avancées au monde. Quant à la Défense nationale, elle a imposé des contraintes et de la dissuasion aux États hostiles.

Le sénateur Boisvenu : Est-ce le Canada qui a décidé de ne pas participer, ou est-ce qu'il n'a pas été invité à participer?

M. Leuprecht : Je dirais que c'est une route dans les deux sens, mais le non-investissement du Canada dans les domaines de la sécurité nationale, du renseignement et de la défense se poursuit depuis plusieurs années. Par conséquent, le Canada est de plus en plus exclu des conversations, dialogues et partenariats de nos plus proches alliés. Le Canada se trouve de plus en plus marginalisé et c'est problématique, parce que ces partenaires représentent une très importante plus-value pour nos intérêts nationaux. Donc, on est de moins en moins en mesure d'assurer

Senator Boisvenu: Thank you very much, that is very interesting.

[*English*]

Senator Boehm: I would like to thank our witnesses. I have questions for all three.

Ms. Csenskey, my first question is for you. You recently co-authored an article entitled "Post-quantum cryptographic assemblages and the governance of the quantum threat." We know that gasoline-powered vehicles, because of their electronics, have been vulnerable for some time, but it's the first time I have seen anything on how electric vehicles are moving into that vulnerability category as well. In other committees in the Senate, we have looked at the benefits of electric vehicles and the need to set up charging stations, et cetera. You specifically mentioned the threat of quantum computers basically being able to outwit systems that would be built into electric vehicles, particularly with respect to brakes. Could you elucidate on that point, whether we or industry will be ready to deal with that or whether you are aware of any specific groups that would stoop to those lows in terms of exercising malware into that domain?

Ms. Csenkey: Thank you so much for that question.

I very much appreciate your bringing up that paper. As you mentioned, it's a co-authored paper in an academic journal. My co-author and I looked at how different cooperating states are trying to understand what the quantum threat is and what the capabilities of quantum computers are — both very generally, but in specific contexts and instances. As a technology, quantum computers can have a wide range of capabilities and things we can do with them. There can be great things that we can do with them — they are excellent as powerful computers processing large amounts of data — but they can also be used for not-so-good things.

Basically, in our paper we were looking at how cooperating states understand the quantum threat, and what do these intersection points of understanding or misunderstanding mean for future defence and security cooperation? We found that there was some discrepancy among different cooperating allies in, first of all, understanding the quantum threat and cooperating for solutions. We found that there were a number of pathways, both of understanding and misunderstanding.

Le sénateur Boisvenu : Merci beaucoup; c'est très intéressant.

[*Traduction*]

Le sénateur Boehm : Je remercie nos témoins. J'ai des questions pour les trois.

Madame Csenskey, ma première question s'adresse à vous. Vous avez récemment corédigé un article intitulé « Post-quantum cryptographic assemblages and the governance of the quantum threat ». Nous savons que les véhicules à essence sont vulnérables depuis un certain temps en raison de leur électronique, mais c'est la première fois que je vois quoi que ce soit sur la façon dont les véhicules électriques entrent également dans cette catégorie de vulnérabilité. Dans d'autres comités du Sénat, nous avons examiné les avantages des véhicules électriques et la nécessité d'installer des bornes de recharge, etc. Vous avez parlé plus précisément de la menace que représentent les ordinateurs quantiques capables de déjouer les systèmes intégrés dans les véhicules électriques, particulièrement en ce qui concerne les freins. Pourriez-vous nous éclairer sur ce point, et nous dire si nous serons, nous ou l'industrie, prêts à faire face à cette situation, ou si vous connaissez des groupes particuliers qui s'abaisseraient à de telles bassesses en utilisant des logiciels malveillants dans ce domaine?

Mme Csenkey : Merci beaucoup pour cette question.

Je vous suis très reconnaissante de mentionner cet article. Comme vous l'avez dit, il s'agit d'un article publié en collaboration dans une revue universitaire. Ma coautrice et moi-même avons examiné la façon dont différents États coopérants tentent de comprendre la menace quantique et les capacités des ordinateurs quantiques — de façon très générale, mais dans des contextes et des cas précis. En tant que technologie, les ordinateurs quantiques peuvent avoir un large éventail de capacités et de possibilités. Nous pouvons faire des choses formidables grâce à eux. Ce sont d'excellents ordinateurs qui traitent de grandes quantités de données, mais ils peuvent aussi être utilisés pour des choses moins bonnes.

Essentiellement, dans notre article, nous nous sommes penchés sur la façon dont les États coopérants comprennent la menace quantique, et sur ce que ces points d'intersection de compréhension ou d'incompréhension signifient pour la coopération future en matière de défense et de sécurité. Nous avons constaté qu'il y avait des divergences entre les différents alliés coopérants, tout d'abord en ce qui concerne la compréhension de la menace quantique, et aussi la coopération pour trouver des solutions. Nous avons constaté qu'il existait un certain nombre de voies, à la fois de compréhension et d'incompréhension.

One of them was cooperation and partnership on infrastructure. Some of that was understanding how the quantum threat can impact infrastructure and how different states, through their various departments, can work together through various associations to protect against this threat and protect their internal government infrastructure, as well as critical infrastructure, against quantum threat and quantum threat actors.

As one of those pieces of infrastructure, as you mentioned, we could talk about electric vehicles and the whole infrastructure that includes electric vehicles. It's not just the physical vehicle, but it's also the computers that are those vehicles. It's also the data collected, where that data is stored and all the different technologies that have to be connected to make this work. It also includes the physical infrastructure of our roads and charging stations and individual people who will be using this type of technology as part of these larger intersecting infrastructures.

Senator Boehm: I'm sorry to interrupt you, but this would also apply to defence equipment. As we're learning more from the war in Ukraine and want to modernize and maybe use more electric and other vehicles and systems, is there a danger that the quantum computing aspect could impact or, shall we say, outwit algorithms that might already be in existence?

Ms. Csenkey: Thank you for that question.

That's something that I will be looking into in more detail. I just received a grant from the Department of National Defence through their Mobilizing Insights in Defence and Security Target Engagement Grants to look at this specific issue.

Senator Cardozo: I have two questions. I'll pose them both to you, and each of you can take whichever one you like.

We talk a lot about cyber-threats being international. Do you think there are domestic cyber-threats? Are there non-state actors, bad actors within Canada, who are now beginning to get the attention of the security forces and who may be threats to our cybersecurity system?

The other is a longer-term system. I think of globalization and trade. About a decade ago, it seemed to be gone forever. Then about five years ago, we suddenly said no, we're not going to go global, or there was a move away from globalization. Is there any world in which we will pull back from our cyber system, the internet? The online world being global, the World Wide Web, is there ever a system where we would pull back parts of it for

L'une d'elles était la coopération et le partenariat en matière d'infrastructure. Il s'agissait en partie de comprendre comment la menace quantique peut avoir une incidence sur l'infrastructure et comment différents États, par l'entremise de leurs divers ministères, peuvent travailler ensemble par l'entremise de diverses associations pour se protéger contre cette menace et protéger leurs infrastructures gouvernementales internes, ainsi que les infrastructures essentielles, contre les menaces quantiques et les auteurs de menaces quantiques.

Comme vous l'avez mentionné, nous pourrions parler des véhicules électriques et de l'ensemble de l'infrastructure dont ils font partie. Il ne s'agit pas seulement des véhicules, mais aussi des ordinateurs qui les équipent. Il y a également les données recueillies, l'endroit où elles sont stockées et toutes les différentes technologies qui doivent être connectées pour que cela fonctionne. Cela comprend aussi l'infrastructure physique de nos routes et de nos bornes de recharge, ainsi que les personnes qui utiliseront ce type de technologie dans le cadre de ces grandes infrastructures qui se croisent.

Le sénateur Boehm : Je m'excuse de vous interrompre, mais cela s'appliquerait également au matériel de défense. Au fur et à mesure que nous tirons des leçons de la guerre en Ukraine et que nous voulons moderniser, et peut-être utiliser davantage de véhicules et de systèmes électriques et autres, y a-t-il un risque que l'aspect informatique quantique ait un impact ou, dirons-nous, qu'il déjoue les algorithmes qui pourraient déjà exister?

Mme Csenkey : Merci pour cette question.

C'est quelque chose que je vais examiner plus en détail. Je viens tout juste de recevoir une subvention du ministère de la Défense nationale dans le cadre du Programme de subventions de coopération ciblées de la Mobilisation des idées nouvelles en matière de défense et de sécurité, pour examiner cette question précise.

Le sénateur Cardozo : J'ai deux questions. Je vais les poser toutes les deux, et chacun d'entre vous pourra choisir celle qui lui convient.

Nous parlons beaucoup des cybermenaces internationales. Pensez-vous qu'il y a des cybermenaces nationales? Y a-t-il des acteurs non étatiques, de mauvais acteurs au Canada, qui commencent à attirer l'attention des forces de sécurité et qui pourraient représenter une menace pour notre système de cybersécurité?

L'autre est un système à plus long terme. Je pense à la mondialisation et au commerce. Il y a une dizaine d'années, il semblait que cela allait durer éternellement. Puis, il y a environ cinq ans, nous avons soudainement déclaré que nous n'allions pas nous mondialiser, ou nous nous sommes éloignés de la mondialisation. Est-il envisageable que nous nous retirions de notre cybersystème, d'Internet? Le monde en ligne étant

security reasons because we just have no control over the security of the system at some point?

Mr. Wilner: To your first question, there are domestic actors that are poised and that are conducting attacks. Many of them are criminals. Some of them are organized. Some of them are small. I think the focus of this discussion and the focus of our energies has been on state-driven cyber activity. I think that's the tip of the spear, frankly. We know that the online marketplace is being undone by cybercriminals, and many of them — or some of them, certainly — are active within this border. The same would go for some extremist groups, terrorists, far-right extremists and so forth. We need to be looking both internally and externally.

In terms of your second question, the splinternet is coming. We have this world of divided internet access, depending on your nationality, effectively. We know that Russia and China are creating islands of their own. You can imagine a future in which, for a number of reasons, you have maybe not a Canadian internet island but one that is shared and partners with traditional allies and partners. I think that's especially likely.

Mr. Leuprecht: On the domestic versus international threats, the key, of course, is that there are state-based actors — in particular, Russia and China — that have capabilities that no one can match. The SolarWinds infiltration is probably the best example to that effect. It's estimated that it took about 18 months and probably a thousand people for Russia to build that particular exploit. Russia and China have capabilities that pose a genuine existential threat in the way they can be deployed against our systems and in a way that I think non-state actors and domestic actors simply cannot provide. At the same time, only about 1 to 1.5% of those risks emanate from state-based actors, but those risks have a potentially high impact against which only governments can effectively deter and dissuade.

Ms. Csenkey: Picking up on your question about dealing with globalization and understanding this connectedness of technologies and people and services and ideas via the internet, and if we are approaching a moment where maybe these things would be less connected and more secluded, and I don't think so.

We are seeing more devices, more technology and more people coming online and connected. We have seen this especially during the pandemic, and now, as a result of that, many services are available online. Many people have different connected devices in their home. We can think of that as the internet of things, the internet of devices, but also the internet of

mondial, le World Wide Web, aurons-nous un jour un système dont nous retirerons des parties pour des raisons de sécurité parce que nous n'aurons tout simplement aucun contrôle sur la sécurité du système à un moment donné?

M. Wilner : Pour répondre à votre première question, il y a des acteurs nationaux qui sont prêts et qui mènent des attaques. Bon nombre d'entre eux sont des criminels. Certains d'entre eux sont organisés. Certains sont de petite taille. Je pense que nous avons surtout centré la discussion et nos efforts sur les activités cybernétiques menées par les États. En toute franchise, je pense que c'est la pointe de l'iceberg. Nous savons que le marché en ligne est en train d'être détruit par des cybercriminels, et bon nombre d'entre eux — ou du moins certains d'entre eux — sont actifs dans notre pays. Il en va de même pour certains groupes extrémistes, terroristes, extrémistes d'extrême droite et autres. Nous devons être attentifs à la fois à l'intérieur et à l'extérieur de nos frontières.

Pour ce qui est de votre deuxième question, le Splinternet est en train d'arriver. Nous vivons dans un monde où l'accès à Internet est divisé, en fonction de la nationalité de chacun. Nous savons que la Russie et la Chine sont en train de créer leurs propres îlots. Vous pouvez imaginer un avenir où, pour un certain nombre de raisons, nous n'aurons peut-être pas un îlot Internet canadien, mais un îlot partagé avec des alliés et des partenaires traditionnels. Cela me semble fort probable.

M. Leuprecht : En ce qui concerne les menaces nationales et internationales, l'élément clé, bien sûr, c'est qu'il y a des acteurs étatiques — en particulier la Russie et la Chine — qui ont des capacités que personne ne peut égaler. L'infiltration de SolarWinds en est probablement le meilleur exemple. On estime qu'il a fallu environ 18 mois, et probablement un millier de personnes à la Russie pour réaliser cet exploit. La Russie et la Chine ont des capacités qui représentent une véritable menace existentielle dans la manière dont elles peuvent être déployées contre nos systèmes et d'une façon que, selon moi, les acteurs non étatiques et nationaux ne peuvent tout simplement pas fournir. En même temps, seulement environ 1 % à 1,5 % de ces risques émanent d'acteurs étatiques, mais ces risques ont un impact potentiellement élevé que seuls les gouvernements peuvent contrer et dissuader efficacement.

Mme Csenkey : Pour revenir à votre question sur la mondialisation et la compréhension du lien entre les technologies, les gens, les services et les idées par Internet, et quant à savoir s'il arrivera bientôt que ces choses soient peut-être moins connectées et plus isolées, je ne le crois pas.

Nous voyons de plus en plus d'appareils, de technologies et de gens qui se connectent en ligne. On l'a vu surtout pendant la pandémie, et maintenant, de nombreux services sont disponibles en ligne. De nombreuses personnes ont différents appareils connectés à leur domicile. On peut considérer cela comme l'Internet des objets, l'Internet des appareils, mais aussi

services and of people too. It's not only thinking about how we're connected globally through the results of globalization, but also that there are so many different products that need to connect to the internet to work, and in so many different sectors, too — not just in our home, but in hospitals or in the transportation sector.

I don't think there is a time where we can say that we're not going to be as connected or that there will be fewer things and people connected. I think we have seen that there has been more engagement in the online space and more critical services being offered and accessible through these spaces. I think that is an opportunity, but it also comes with risks and potential threats. Especially when those critical systems and critical services are online, that is something that we need to understand and protect.

Senator M. Deacon: Thank you for being here today.

Ms. Csenkey, I'm a very big fan of the Balsillie School, and I'll start by asking you a question. I'm thrilled to speak to students there. You started off in your opening remarks on the importance of reliable power sources for our cybersecurity systems. You made reference to old legacy power sources and technology and part of these chains. As I was sitting here thinking about that, it made me recall the power outage we had in eastern North America that blacked out large swaths of Canada. That is coming up to 20 years ago, surprisingly, but it also highlighted to us how vulnerable our power grid is. I am wondering if we have done anything, or from your perspective, enough to reinforce this, or are we continuing to put off this essential and necessary work because it's expensive and disruptive?

Ms. Csenkey: Thank you so much for that question.

It's definitely an important issue, especially when we're thinking about connecting more devices or the example that we brought up today of electric vehicles. Those things require electricity in order to function, and we can see how important it is to just have electricity to function in our daily lives. We have also seen that recently in Ottawa as well when there was a power outage due to another storm.

I think we need to be making sure that the systems already up and running are able to be securely transitioned to digital networks. When you have these legacy systems that perhaps don't necessarily have the security that we need today connecting with devices, connecting with other services or making those internet connections with other infrastructures, we need to make sure they are speaking together, but they are speaking together securely and safely.

l'Internet des services et des gens. Il ne s'agit pas seulement de réfléchir à la façon dont nous sommes connectés à l'échelle mondiale en raison de la mondialisation, mais aussi au fait qu'il y a tellement de produits différents qui doivent se connecter à Internet pour fonctionner, et cela dans tellement de secteurs différents aussi, pas seulement dans nos maisons, mais dans les hôpitaux ou dans le secteur des transports.

Je ne pense pas que l'on puisse dire qu'à un moment donné, nous ne serons plus aussi connectés ou qu'il y aura moins d'objets et de personnes connectés. Je crois que nous avons constaté une plus grande participation dans l'espace en ligne et une augmentation de l'offre de services essentiels accessibles par l'entremise de cet espace. Je pense que c'est une opportunité, mais cela comporte aussi des risques et des menaces potentielles. Surtout lorsque les systèmes et services essentiels sont en ligne, c'est quelque chose que nous devons comprendre et protéger.

La sénatrice M. Deacon : Merci d'être ici aujourd'hui.

Madame Csenkey, je tiens la Balsillie School en haute estime, et je vais commencer par vous poser une question. J'ai toujours un grand plaisir à parler aux étudiants de cet établissement. Dans votre déclaration préliminaire, vous avez parlé de l'importance d'avoir des sources d'énergie fiables pour nos systèmes de cybersécurité. Vous avez fait allusion aux vieilles sources d'énergie et technologies et aux maillons de ces chaînes. En y réfléchissant, je me suis souvenue de la panne que nous avons connue dans l'Est de l'Amérique du Nord et qui a privé d'électricité une grande partie du Canada. Cela fera bientôt 20 ans, étonnamment, mais cela nous a aussi montré à quel point notre réseau électrique est vulnérable. Je me demande si nous avons fait quelque chose, ou si, de votre point de vue, nous avons fait suffisamment pour renforcer le réseau, ou si nous continuons de reporter ces travaux essentiels et nécessaires parce qu'ils sont coûteux et perturbateurs?

Mme Csenkey : Merci beaucoup pour cette question.

C'est certainement une question importante, surtout lorsque nous pensons à connecter davantage d'appareils, ou à l'exemple des véhicules électriques dont nous avons parlé aujourd'hui. Ces objets ont besoin d'électricité pour fonctionner, et nous pouvons voir à quel point il est important d'avoir de l'électricité pour fonctionner dans notre vie quotidienne. Nous l'avons aussi vu récemment à Ottawa, lorsqu'il y a eu une panne d'électricité en raison d'une autre tempête.

Je pense que nous devons veiller à ce que les systèmes déjà en service puissent faire la transition en toute sécurité vers les réseaux numériques. Lorsque vous avez des anciens systèmes qui n'ont peut-être pas la sécurité dont nous avons besoin aujourd'hui et qui se connectent à des appareils, à d'autres services ou à d'autres infrastructures par Internet, nous devons nous assurer qu'ils communiquent ensemble, mais qu'ils le font en toute sécurité.

We can always do more. When we're talking about this in the context of cybersecurity, it isn't just one and done. It's something that we always have to revisit. We always have to be adaptable to that. We need to make sure that we're not just setting a standard or setting a framework and hoping it works for the next 5, 10 or 15 years.

Senator M. Deacon: Let's leave that and fast forward to something else that you have mentioned and which has come up earlier today. We touched on quantum corrupting already, and most recently through our assessment to the CSE, which was just before, as mentioned. Quantum computing and the potential to disrupt the field of cyberdefence is a pretty big deal, specifically around the matters of encryption. My staff and I recently met with Professor Greg Dick from the Perimeter Institute just across the street from you. He left us with the impression that Canada is or is becoming a global leader in quantum computing, with a great number of bright young minds working on this. As you have spoken on quantum computing at great length already, I am wondering if Canada is doing enough to build homegrown talent and knowledge in this field that clearly is here now and ever so much around the corner.

Ms. Csenkey: Thank you so much for that question.

It's another very important issue. I think Canada has the expertise base. We have many different regional hubs of experts, both in academia and in industry, who are working on developing and understanding these technologies.

With the recent release of the National Quantum Strategy, as well as the S&T strategy, it is really providing the space and framework to have more engagement with these centres and researchers to really cultivate that relationship between industry, academia and with the government in various interested government departments and government actors. Fostering that triple helix relationship between all of these parties is really important. That's really how we can, as a country, make sure that we're investing in the right types of technologies and in secure applications of those technologies, as well as thinking ahead and making sure that we have the continued expertise base to continue working on these technologies and continue making new advancements. That includes bringing in people who perhaps might not have engaged in this type of work. I'm thinking of women and other underrepresented groups being engaged in STEM and these types of fields.

Senator M. Deacon: Thank you.

Senator Richards: Thank you very much to everybody here for their expertise.

Nous pouvons toujours faire plus. Lorsque nous parlons de cela dans le contexte de la cybersécurité, nous ne pouvons pas régler les problèmes une fois pour toutes. C'est quelque chose que nous devons toujours revoir. Nous devons nous adapter constamment. Nous devons nous assurer de ne pas nous contenter d'établir une norme ou une stratégie en espérant que cela fonctionnera pour les 5, 10 ou 15 prochaines années.

La sénatrice M. Deacon : Laissons cela de côté et passons à un autre sujet dont vous avez fait mention, et qui a été soulevé plus tôt aujourd'hui. Nous avons déjà abordé la question de la corruption quantique, et plus récemment, dans le cadre de notre évaluation du CST, qui a eu lieu juste avant, comme on l'a mentionné. L'informatique quantique et la possibilité de perturber le domaine de la cyberdéfense sont des éléments très importants, surtout en ce qui concerne le chiffrement. Mon personnel et moi-même avons récemment rencontré Greg Dick, professeur à l'Institut Périmètre, juste en face de chez vous. Il nous a donné l'impression que le Canada est, ou est en train de devenir un chef de file mondial dans le domaine de l'informatique quantique et qu'un grand nombre de jeunes gens brillants travaillent dans ce domaine. Comme vous avez déjà longuement parlé de l'informatique quantique, je me demande si le Canada fait suffisamment d'efforts pour développer les talents et les connaissances dans ce domaine qui est clairement présent chez nous aujourd'hui et qui le sera bientôt davantage.

Mme Csenkey : Merci beaucoup pour cette question.

C'est un autre enjeu très important. Je pense que le Canada a l'expertise nécessaire. Nous avons de nombreux centres régionaux d'experts, tant dans le milieu universitaire que dans l'industrie, qui travaillent au développement et à la compréhension de ces technologies.

La publication récente de la Stratégie quantique nationale, ainsi que de la Stratégie S & T, fournit vraiment un espace et un cadre pour s'engager davantage avec ces centres et ces chercheurs afin de vraiment cultiver une relation entre l'industrie, le milieu universitaire et le gouvernement dans divers ministères et acteurs gouvernementaux intéressés. Il est vraiment important de favoriser cette relation à triple hélice entre toutes ces parties. C'est vraiment de cette façon que nous pouvons, en tant que pays, nous assurer d'investir dans les bons types de technologies et dans les applications sécurisées de ces technologies, tout en pensant à l'avenir et en veillant à disposer de l'expertise nécessaire pour continuer à travailler sur ces technologies et à faire de nouvelles avancées. Cela comprend le recrutement de personnes qui ne se sont peut-être jamais engagées dans ce type de travail. Je pense aux femmes et à d'autres groupes sous-représentés qui s'intéressent aux STIM et à ce genre de domaines.

La sénatrice M. Deacon : Merci.

Le sénateur Richards : Merci beaucoup à tous les témoins de leur expertise.

I'm going to Mr. Leuprecht a question. It's a question that I don't think can be answered, but that's the problem. Why do you think Canada lacks the will to shape its own independent policies in the North or anywhere else? I mentioned in an article I wrote last week that if the U.S. had a reliable ally among the former colonies, it was not Canada any longer but was Australia, which in my mind is extremely unfortunate given the times we are now in and the bad actors on our shores. Could you comment on that, please?

Mr. Leuprecht: That is a fantastic question.

First, we still have a very linear and kinetic thinking, especially when it comes to issues such as cyber, national security or defence in general. It's very outdated and outmoded. People simply can't or don't want to wrap their head around issues of contemporary international security. They are complex, they are difficult and, ultimately, they call for significant changes in investments.

Second, much of this conversation is controversial as a policy, and it's controversial in terms of the investment required. In that context, governments, and I think politicians of certain stripes, would rather avoid it. At the same time, I think there is a sense that it also distracts from other policy agendas that governments prefer to drive, so let's not draw too much attention to it.

Third, I think we really lack a sense of strategy in this country, both domestic and international. We always criticize the United States, but for better or worse, people in the United States have a very clear vision for their country. We might not agree with some of those visions, but they have a clear vision. Show me a politician in this country that has a clear vision for this country for where we want or need to be 10 or 20 years from now. What do we need today to preserve the security, the prosperity and the democracy that we so cherish?

There is an opportunity here for us to think hard. I think this comes out of a certain — I want to be charitable, but say, on the one hand, intellectual laziness. We have hitched our wagon to the United States for decades, like many allies, for that matter, and it's just easier to draft behind the United States. Of course, the United States, both in interests and ideology is diverging from both Canada's and other key allies' national interests and priorities.

Having genuinely independent policies — in particular foreign policy, but also more generally defence and security — could be extremely divisive in a country such as Canada. I would remind you, senator, as you appreciate, the single-largest national unity crisis in this country was as a result of defence policy — of course, conscription. Governments realize this is going to be

Je vais poser une question à M. Leuprecht. C'est une question à laquelle je ne pense pas qu'on puisse répondre, mais c'est bien là le problème. Pourquoi pensez-vous que le Canada n'a pas la volonté d'élaborer ses propres politiques indépendantes dans le Nord ou ailleurs? J'ai mentionné dans un article que j'ai écrit la semaine dernière que si les États-Unis avaient un allié fiable parmi les anciennes colonies, ce n'était plus le Canada, mais l'Australie, ce que je trouve extrêmement regrettable compte tenu de la conjoncture actuelle et des mauvais acteurs sur nos côtes. Pourriez-vous nous dire ce que vous en pensez?

M. Leuprecht : C'est une excellente question.

Premièrement, nous avons toujours une pensée très linéaire et cinétique, surtout lorsqu'il s'agit de questions comme la cybersécurité, la sécurité nationale ou la défense en général. C'est très dépassé et obsolète. Les gens ne peuvent ou ne veulent tout simplement pas se pencher sur les questions de sécurité internationale contemporaines. Elles sont complexes, elles sont difficiles et, au bout du compte, elles exigent des changements importants dans les investissements.

Deuxièmement, une grande partie de cette conversation est controversée en tant que politique, et elle est controversée en ce qui concerne l'investissement requis. Dans ce contexte, les gouvernements et, je crois, les politiciens de certaines allégeances préfèrent l'éviter. En même temps, je pense qu'on a l'impression que cela détourne l'attention des autres programmes politiques que les gouvernements préfèrent mettre en œuvre, alors n'insistons pas trop sur ces questions.

Troisièmement, je pense que nous manquons vraiment de stratégie au Canada, au niveau tant national qu'international. Nous critiquons toujours les États-Unis, mais pour le meilleur ou pour le pire, les Américains ont une vision très claire de leur pays. Nous ne sommes peut-être pas d'accord avec certains aspects de cette vision, mais elle est claire. Montrez-moi un membre de la classe politique canadienne qui a une vision claire de ce que nous voulons ou devons faire dans 10 ou 20 ans. De quoi avons-nous besoin aujourd'hui pour préserver la sécurité, la prospérité et la démocratie qui nous sont si chères?

Nous avons ici l'occasion de réfléchir sérieusement. Je pense que cela découle — je veux être charitable —, mais disons, d'une certaine paresse intellectuelle. Nous nous sommes accrochés aux États-Unis pendant des décennies, comme beaucoup de nos alliés, d'ailleurs, et il est tout simplement plus facile de suivre les États-Unis. Bien entendu, les intérêts et l'idéologie des États-Unis s'écartent des priorités et des intérêts nationaux du Canada et d'autres alliés clés.

Le fait d'avoir des politiques véritablement indépendantes — surtout en matière de politique étrangère, mais aussi, de façon plus générale, pour la défense et la sécurité — pourrait être une très grande source de division dans un pays comme le Canada. Je vous rappelle, sénateur, comme vous le savez, que la plus importante crise de l'unité nationale au pays a été causée par la

very difficult, so they would just rather steer clear. That means we reduce our ability to shape the international security environment because increasingly we are become an unreliable and unpredictable ally.

Senator Richards: I said something the same in my article. Thank you very much.

Senator Dasko: I would like to probe the topic of Russia's strengths and weaknesses a little bit more. Professor Wilner, you said earlier that the Russians' specialty is disinformation. You also said they have moved into the destructive mode but that their capabilities have proven to be flat. However, Professor Leuprecht a few minutes ago talked about the strengths of Russia and the strength they have in cyber activity, cyberwarfare, the resources and their particular strengths. Actually, your comments about Russia's flat capabilities remind me of what we heard about the Russian military after they invaded Ukraine. We heard that, in fact, they were poorly trained and poorly resourced, so a similar kind of theme as to what you just said.

Given these perspectives, I'm not sure if we disagree with each other or if we could just probe a little bit more the strengths of Russia in cyberwarfare, and the weaknesses as well. I would like us to probe it just a little bit more so that I can understand that better. Obviously, with their activity in Ukraine and in Canada, it's of great interest to Canadians to understand this.

Mr. Wilner: Thank you for your comments.

Christian and I work together quite a bit, so we see eye to eye on many things. I would agree probably on this point as well.

I think what has happened is Russia's focus historically has been using cyber for disinformation, but its focus has shifted obviously because of the war in Ukraine. It was meant to try to soften the ground with cyber operations in advance of its operation last February. That didn't go too well for Russia. I think some commentators, including myself, were a bit surprised at the lacklustre cyber showing, if you will, of Russia.

I think part of the reason they weren't successful is that Ukraine wasn't sitting still for the last 10 years. They have been beefing up their cyber capabilities, as I suggested, with corporate entities, with allies, including Canada and the United States, and they anticipated far worse. They were then able to respond, both from an infrastructure protection process and a communications perspective, effectively to Russia.

politique de défense, par la conscription, bien sûr. Les gouvernements se rendent compte que cela va être très difficile, alors ils préfèrent simplement éviter les problèmes. Cela signifie que nous réduisons notre capacité de façonner l'environnement de la sécurité internationale parce que nous devenons de plus en plus un allié peu fiable et imprévisible.

Le sénateur Richards : J'ai dit la même chose dans mon article. Merci beaucoup.

La sénatrice Dasko : J'aimerais approfondir un peu plus le sujet des forces et des faiblesses de la Russie. Monsieur Wilner, vous avez dit plus tôt que la spécialité des Russes était la désinformation. Vous avez également dit qu'ils sont passés au mode destructeur, mais que leurs capacités se sont avérées limitées. Cependant, il y a quelques minutes, M. Leuprecht a parlé des atouts de la Russie et de ses forces en matière de cyberactivité, de cyberguerre, de ressources et de forces particulières. En fait, vos commentaires sur les capacités limitées de la Russie me rappellent ce que nous avons entendu au sujet des soldats russes après leur invasion de l'Ukraine. On nous a dit qu'en fait, ils étaient mal formés et mal dotés en ressources, ce qui revient à ce que vous venez de dire.

Compte tenu de ces points de vue, je ne sais pas si nous sommes en désaccord les uns avec les autres ou si nous pourrions simplement examiner un peu plus les forces de la Russie en matière de cyberguerre, ainsi que ses faiblesses. J'aimerais que nous nous penchions un peu plus sur la question afin que je puisse mieux comprendre. De toute évidence, compte tenu des activités de la Russie en Ukraine et au Canada, il est très intéressant pour les Canadiens de comprendre cela.

M. Wilner : Je vous remercie de vos commentaires.

Mon collègue et moi travaillons beaucoup ensemble, alors nous sommes d'accord sur bien des choses. Je suis probablement d'accord sur ce point également.

Ce qui s'est passé, je pense, c'est que la Russie s'est toujours concentrée sur l'utilisation de la cybernétique à des fins de désinformation, mais son orientation a manifestement changé en raison de la guerre en Ukraine. L'objectif était d'essayer d'assouplir le terrain avec des cyberopérations en prévision de son opération de février dernier. Cela ne s'est pas très bien passé pour la Russie. Je pense que certains commentateurs, y compris moi-même, ont été un peu surpris de sa piètre performance en matière de cybernétique.

Je pense qu'une des raisons pour lesquelles elle n'a pas réussi, c'est que l'Ukraine n'est pas restée les bras croisés pendant les 10 dernières années. Elle a renforcé ses capacités cybernétiques, comme je l'ai dit, avec des entreprises, des alliés, dont le Canada et les États-Unis, et elle s'attendait à ce que la situation soit bien pire. Elle a ensuite été en mesure de répondre efficacement à la Russie, tant du point de vue du processus de protection des infrastructures que des communications.

Now, doesn't mean that Russia doesn't invest heavily, as Christian suggested. They do. They are still a shark in the cyber realm. And yet, I think the lesson from Ukraine is appropriately planning and investing in cyberdefences can undo some of that investment that they are putting in offence.

Mr. Leuprecht: Dovetailing on what Alex just said, indeed, Soviet active measures are well known. They were deployed, including in this country. This is well documented. Russia is building on a strength that it has honed for decades.

At the same time, what we see in Ukraine if you look at some of the reports, such as the open-source reports by Microsoft, for instance, you see some of the CSE warnings. We do know Russia has had some success, especially combining cyber operations and kinetic operations. It is not entirely that this is the dog that didn't bark. We have also been very effective in helping Ukraine with hunt forward teams and other capabilities to ensure that Ukraine has the support it needs, both on its own and with support, against larger Russian efforts to destabilize in particular civilian but also defence cyber infrastructure. As Alex says, this has been as a result of foresight, of real capabilities that have imposed real constraints, but also real deterrents on Russia's ability to deploy some of its capabilities.

But certainly in light of CSE warnings, Russia's capabilities are not to be underestimated. I have often compared our own government infrastructure to the minivan that I drive, which is over 12 years old. It runs okay, but it is certainly not the best opportunity to drive. There is a lot of heavy lifting that needs to be done to make sure that we get our networks to the point where we have the insurance pieces that we need against hostile activity.

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

Ms. Csenkey, I want to come back to some statements you made earlier. As you know, both Canada and the United States are involved in this renewal of NORAD, and both countries have committed a huge amount of resources. There is a sense that, with the president coming here later this week, there is a need to accelerate the time frame for the implication of NORAD and a renewal. Much has been learned in the many decades now since the NORAD relationship has existed.

Recognizing that 40% of our territories are in the North, it's very challenging despite developments and ongoing efforts to link our communities in the North to those in the South. You have made a point in regard to the different levels of infrastructure we have and, more importantly, the links with each

Cela ne veut pas dire que la Russie n'investit pas beaucoup, comme l'a laissé entendre M. Leuprecht. Elle le fait. Elle est encore un requin dans le cyberespace. Pourtant, je pense que la leçon à tirer de l'Ukraine, c'est que la planification et l'investissement appropriés dans la cyberdéfense peuvent annuler une partie de l'investissement consacré à l'offensive.

M. Leuprecht : Compte tenu de ce que M. Wilner vient de dire, les mesures actives soviétiques sont bien connues. Elles ont été déployées, y compris au Canada. C'est bien documenté. La Russie s'appuie sur une force qu'elle a perfectionnée pendant des décennies.

En même temps, ce que nous voyons en Ukraine, si vous examinez certains des rapports, comme les rapports de source ouverte de Microsoft, par exemple, vous verrez certains des avertissements du CST. Nous savons que la Russie a connu un certain succès, surtout en combinant cyberopérations et opérations cinétiques. Ce ne sont pas vraiment les preuves qui manquent. Nous avons également été très efficaces pour aider l'Ukraine grâce à des équipes de cybermission et d'autres capacités afin de lui fournir le soutien nécessaire pour contrer, par elle-même ou avec de l'aide, les efforts plus vastes de la Russie visant à déstabiliser, en particulier l'infrastructure cybernétique civile, mais aussi celle de défense. Comme l'a dit mon collègue, c'est le résultat de la prévoyance, de capacités réelles qui ont imposé des contraintes réelles, mais aussi de vrais moyens de dissuasion contre la capacité de la Russie à déployer certaines de ses forces.

Néanmoins, à la lumière des avertissements du CST, il ne faut pas sous-estimer les capacités de la Russie. J'ai souvent comparé notre propre infrastructure gouvernementale à ma fourgonnette, qui a plus de 12 ans. Elle roule assez bien, mais ce n'est certainement pas le véhicule idéal. Il y a beaucoup de travail à faire pour nous assurer que nos réseaux sont suffisamment bien protégés contre les activités hostiles.

Le sénateur Yussuff : Je remercie les témoins de leur présence.

Madame Csenkey, j'aimerais revenir sur certaines déclarations que vous avez faites plus tôt. Comme vous le savez, le Canada et les États-Unis participent au renouvellement du NORAD, et les deux pays ont engagé d'énormes ressources. On a l'impression, avec la venue du président plus tard cette semaine, qu'il faut accélérer le calendrier des répercussions du NORAD et de son renouvellement. Nous avons beaucoup appris au cours des nombreuses décennies qui se sont écoulées depuis que le NORAD existe.

Compte tenu du fait que 40 % de nos territoires se trouvent dans le Nord, il est très difficile, malgré les progrès et les efforts continus, de relier nos collectivités du Nord à celles du Sud. Vous avez parlé des différents niveaux d'infrastructure que nous avons, et plus important encore, des liens qui nous unissent. Je

other. I recognize you are talking about quantum disruption that could come. Is it also in itself not a blessing, the fact that it is not linked? It may be an opportunity for us to learn that it can be disrupted. At the same time, in the context of NORAD renewal, what would you suggest that we can learn from this experience? Also at the same time, both Canada and the United States are very much aware that our major source of disruption is going to come from two countries which are extreme allies against us in the war in Ukraine, China and Russia and their friendship. Both are posing a tremendous threat to our Northern borders. Is there anything you would like to say in regard to the NORAD renewal that's about to happen? More importantly, what would you offer in terms of advice that we can benefit from?

reconnais que vous parlez des perturbations quantiques qui pourraient survenir. Le fait que nos collectivités ne soient pas reliées n'est-il pas aussi une bénédiction? C'est peut-être l'occasion pour nous d'apprendre que les liens peuvent être perturbés. En même temps, dans le contexte du renouvellement du NORAD, que pensez-vous que nous puissions apprendre de cette expérience? Parallèlement, le Canada et les États-Unis savent très bien que notre principale source de perturbation viendra de deux pays, la Chine et la Russie, qui sont des alliés extrêmes contre nous dans la guerre en Ukraine, et de leur amitié. Les deux représentent une menace énorme pour nos frontières septentrionales. Y a-t-il quelque chose que vous aimeriez dire au sujet du renouvellement du NORAD qui est sur le point d'avoir lieu? Plus important encore, quels conseils pourriez-vous nous donner?

Ms. Csenkey: Thank you so much for that question.

NORAD modernization and renewal have come up again and again. When it comes to talking about modernization, it's important to understand that modernization also needs to include modernization of organizations, of the infrastructure that we're talking about and of devices and services and how those are connected.

When I think about modernization in the context of NORAD, the systems have to be compatible. They have to be interoperable, especially if we're thinking from a defence perspective. One of the examples that I brought up was the cloud computing for command and control, so thinking about bringing technologies and developing technologies to spaces where maybe they haven't necessarily gone before and making them work in place, in a location, but also making sure that they work with our allies and that they are talking to different technologies, and talking securely so there isn't the space and opportunities for malicious cyber-threat actors to disrupt those secure communications and come in and exploit those threat vectors. When I think modernization, I think we need to have the interoperability of systems when we're updating systems. We need to make sure those systems are compatible but also understanding that there is a physical place to them with an existing operating environment. If we want to update certain systems in the context of NORAD modernization, if we're thinking about it in more remote locations, maybe in the North, in harsher operating or climate environments, how are those systems going to physically function in those spaces?

The other example that I brought up was we have the example of cloud computing for command and control systems, but then how is it powered? Will we be relying upon the electrical infrastructure that is there, or are we going to be bringing in portable high-performance micro-grids to make sure those systems work? If we are bringing in those systems, how are we

Mme Csenkey : Merci beaucoup pour cette question.

La modernisation et le renouvellement du NORAD ont été évoqués à maintes reprises. Lorsqu'il est question de modernisation, il est important de comprendre que cela doit également inclure la modernisation des organisations, de l'infrastructure dont nous parlons, des appareils et des services et de la façon dont ils sont connectés.

Quand je pense à la modernisation dans le contexte du NORAD, les systèmes doivent être compatibles. Ils doivent être interopérables, surtout du point de vue de la défense. L'un des exemples que j'ai cités était l'informatique en nuage pour le commandement et le contrôle. Il s'agit donc d'apporter et de développer des technologies dans des espaces où elles n'ont pas été nécessairement utilisées auparavant et de les faire fonctionner sur place, dans un certain endroit. Mais il faut aussi s'assurer qu'elles fonctionnent avec nos alliés et qu'elles communiquent avec différentes technologies de manière sécurisée afin qu'il n'y ait pas d'espace et d'opportunités pour les acteurs malveillants de la cybermenace de perturber ces communications sécurisées et d'exploiter ces vecteurs de menace. Lorsque je pense à la modernisation, je pense que nous devons nous assurer de l'interopérabilité des systèmes lorsque nous les mettons à jour. Nous devons nous assurer que ces systèmes sont compatibles, mais nous devons aussi comprendre qu'ils ont une place physique dans un environnement opérationnel existant. Si nous voulons mettre à jour certains systèmes dans le contexte de la modernisation du NORAD, si nous envisageons de le faire dans des endroits plus éloignés, peut-être dans le Nord, dans des environnements opérationnels ou climatiques plus rigoureux, comment ces systèmes vont-ils fonctionner physiquement dans ces espaces?

L'autre exemple que j'ai évoqué est celui de l'informatique en nuage pour les systèmes de commandement et de contrôle, mais comment est-elle alimentée? Allons-nous compter sur l'infrastructure électrique existante, ou allons-nous recourir à des micro-réseaux portables à haut rendement pour nous assurer que ces systèmes fonctionnent? Si nous mettons en place ces

making sure those systems are securely communicating with our allies? How are we working with the U.S. to protect our digital borders in addition to our physical borders in these different operating environments?

There are two things: We need to make sure that it's compatible and interoperable, but that it can also withstand disruptions in both physical and digital environments.

[*Translation*]

The Deputy Chair: Thank you, Ms. Csenkey. Before we begin the second round of questions, I have a question for Mr. Leuprecht. The threats of cybersecurity attacks are multi-faceted and the attackers' objectives vary from country to country. Are we more vulnerable to having secrets stolen and attacks that could compromise the ongoing operations of our institutions, such as power stations and banks?

Mr. Leuprecht: There are two different worlds in this regard in Canada right now.

There is an old law that requires organizations to report to government every time there is a cybersecurity incident at a company.

The problem is that there are no clear conditions or scales right now. Consider a bank, for example, if the entire financial sector were attacked or threatened in a way that exceeded that bank's ability to defend itself. Under what conditions could that bank appeal to the CSE or use other avenues to get help? This relates not only to defence, but potentially also to the deployment of active and offensive measures to neutralize the threat to the company or to certain critical infrastructure in the country. There is a lack of dialogue and cooperation at the operational level between the government and critical infrastructure for the defence of our systems.

The Deputy Chair: Thank you very much. We will now begin the second round, with Senator Boehm.

[*English*]

Senator Boehm: My questions will be for Professors Leuprecht and Wilner.

First, I'm not comfortable with the blanket notion that there is intellectual laziness in the policy development in this country, no matter who is in power. I don't like expressions that we are an unreliable or unpredictable ally. I think we're proving quite the contrary right now in Ukraine.

systèmes, comment nous assurons-nous qu'ils communiquent en toute sécurité avec nos alliés? Comment travaillons-nous avec les États-Unis pour protéger nos frontières numériques en plus de nos frontières physiques dans ces différents environnements opérationnels?

Il y a deux choses à considérer : nous devons nous assurer de la compatibilité et de l'interopérabilité des systèmes, mais aussi de leur capacité à résister aux perturbations dans les environnements physiques et numériques.

[*Français*]

Le vice-président : Merci, madame Csenkey. Avant de passer au second tour, j'ai une question pour M. Leuprecht. Les menaces de cyberattaques ont de multiples volets et les objectifs des attaquants peuvent varier selon les pays. Sommes-nous plus vulnérables de nous faire voler des secrets et d'être l'objet de saccages qui pourraient compromettre les opérations courantes de nos institutions, comme les centrales électriques ou les banques?

M. Leuprecht : Il y a deux mondes particuliers sur cette question au Canada actuellement.

Il y a une ancienne loi qui oblige les organisations à fournir un rapport au gouvernement chaque fois qu'il y a un incident lié à la cybersécurité dans une entreprise.

Le problème, c'est qu'il n'y a pas de conditions ou d'échelle claires actuellement. Prenons l'exemple d'une banque, où tout le secteur financier ferait l'objet d'une attaque ou d'une menace surpassant la capacité de cette banque à se défendre elle-même. Quelles seraient les conditions pour que cette banque puisse faire appel au CST ou à d'autres moyens pour lui venir en aide? Cela concerne non seulement la défense, mais aussi, potentiellement, le déploiement de mesures actives et offensives, afin de neutraliser la menace posée envers l'entreprise ou certaines infrastructures critiques au pays. Il y a un décalage de dialogues et un décalage opérationnel de collaboration entre le gouvernement et l'infrastructure critique sur le plan de la défense de nos systèmes.

Le vice-président : Merci beaucoup. Nous allons passer au second tour avec le sénateur Boehm.

[*Traduction*]

Le sénateur Boehm : Mes questions s'adressent aux professeurs Leuprecht et Wilner.

Tout d'abord, j'ai peine à croire que tous nos gouvernements au pouvoir, quel que soit leur parti, font preuve de paresse intellectuelle en élaborant les politiques du pays. Je n'aime pas entendre dire que notre pays est un allié peu fiable et imprévisible. Il me semble que les mesures que nous prenons dans le cas de l'Ukraine prouvent le contraire.

Professor Leuprecht, you talked about your cyber doctrine of functional engagement. In a realistic perspective, how would you see that going forward? Is it something that we as legislators should think about in terms of domestic legislation and push for the government to introduce something? On the other hand, is it something that could be handled in an international organization and get others to join in? I would like you to think about that.

Professor Wilner, in the last part of your presentation, you talked about a national cyber deterrence posture. What will that require in terms of political will, or will it be set off by some galvanic event we can't predict, after which we are reacting again and pushing forward?

I would be interested in both of your comments, even though we have only about two minutes remaining.

Mr. Leuprecht: I will keep it to 60 seconds.

On your comments with regard to policy development and function, there are few votes to be gotten in foreign policy in this country — 88 might be the sole exception — so I think it's just simply not where governments and politicians necessarily focus most of their energies, usually.

Functional engagement is a matter of determining the key areas where we find behaviour unacceptable. I made a few proposals in my opening statement. It is to get together with allies and lay out clear red lines for adversaries, with the United States as well but where we are also allies, as middle powers, and demonstrate that we will act in concert when you cross those lines and that we have the authorities and capabilities in place, and that politicians will act. The problem we have in Canada is similar to the problem of many European countries have, where we have the capabilities and the authorizations is placed in legislation but we don't have the political will to follow through. It is less a matter of legislation than it is of drawing those red lines and what adversaries can expect —

Senator Boehm: Thank you, Professor Leuprecht. That's a great answer to that question.

Mr. Wilner: Canada has never had to create its own deterrence posture because we've been part of the two greatest alliances in the world, NORAD and NATO, and they provide us with deterrence clout. Cyberspace is sufficiently different such that NORAD and NATO won't realistically accomplish everything we need it to do. That's why I am suggesting a cyber deterrence posture that starts with intent and resolve to respond when attacked; to draw out those red lines we have been discussing; to create credibility, which I think we have; and then

Monsieur Leuprecht, vous nous avez présenté votre doctrine d'engagement fonctionnel en matière de cybersécurité. Quelle application concrète proposez-vous? Devrions-nous, dans notre rôle de législateurs, envisager de promulguer une loi nationale afin d'inciter le gouvernement à proposer des solutions? D'un autre côté, serait-il possible de confier cela à une organisation internationale afin d'inviter d'autres nations à y participer? Je voudrais que vous pensiez à cette question.

Monsieur Wilner, dans la dernière partie de votre exposé, vous avez parlé d'une stratégie nationale de cyberdissuasion. Quelle volonté politique faudra-t-il pour cela? Pensez-vous qu'au contraire, un événement galvanique totalement imprévisible nous forcera à élaborer cette stratégie?

Il ne nous reste que deux minutes, mais vos réponses m'intéressent beaucoup.

M. Leuprecht : Je ne dépasserai pas 60 secondes.

Pour répondre à vos commentaires sur le fonctionnement de l'élaboration de politiques, le Canada ne peut espérer marquer beaucoup de points en politique étrangère, sauf peut-être avec la résolution 88, ce qui explique que nos gouvernements et nos politiciens s'investissent peu à cet égard.

L'engagement fonctionnel consiste à cerner les principaux domaines où nous constatons des comportements inacceptables. J'ai présenté quelques suggestions dans ma déclaration préliminaire. Il s'agit de nous unir avec nos alliés pour fixer des limites claires à nos adversaires. Nous le ferions bien sûr de concert avec les États-Unis, mais aussi avec d'autres puissances moyennes alliées. Nous affirmerons ainsi que si nos adversaires dépassent ces limites de tolérance, nous interviendrons de concert avec nos alliés, ce qui nous donnera le pouvoir et la capacité d'agir. Nous affirmerons que nos politiciens sont prêts à agir. Le problème qui paralyse le Canada est semblable à celui de nombreux pays européens. Nos lois nous accordent les capacités et les autorisations d'agir, mais notre volonté politique est faible. Le problème ne réside pas dans notre législation. Nous devons fixer des limites pour que nos adversaires sachent à quoi s'attendre...

Le sénateur Boehm : Merci, monsieur Leuprecht. Votre réponse est excellente.

M. Wilner : Le Canada n'a jamais dû créer sa propre posture de dissuasion, parce qu'il fait partie des deux plus grandes alliances au monde, le NORAD et l'OTAN, ce qui lui confère un pouvoir de dissuasion. Comme le cyberespace est très différent, le NORAD et l'OTAN ne peuvent pas intervenir de la bonne façon. C'est pourquoi je propose une posture de cyberdissuasion reposant sur notre intention et notre détermination d'intervenir en cas d'attaque, de fixer des limites de tolérance. Je suis convaincu que nous avons su établir notre crédibilité. Nous

to communicate the threats to our adversaries. Communication is critical to deterrence.

A posture means standing up to all three of those things. It means political leadership, but it's also a question of smart military and strategic thinking, some from DND, Public Safety and CSE. We can start, grassroots up, but at some point, it needs to be a political decision.

[*Translation*]

The Deputy Chair: Before we conclude, I have a question for Mr. Wilner. In fighting cybercriminals, are we condemned to always only being on the defensive, or might there one day be arrests and charges against cybercriminals?

[*English*]

Mr. Wilner: Cybercrime is pervasive. Part of what Canada needs to do — and I think we are doing it — is to create the tools and mechanisms for stopping crime when it is happening and to intersect criminals when we are able to catch them. We are certainly capable when it is done domestically, but it also has to happen in partnership with our allies. Fighting crime in cyberspace is like fighting crime anywhere. There are smart lessons we can use from how we do it in physical space. It's a great question. I don't have a fulsome answer for you, but it's a work-in-progress.

[*Translation*]

The Deputy Chair: That concludes this group of witnesses. Thank you all for being here. Your ideas and knowledge are greatly appreciated. We will suspend briefly and return at 6:20 p.m. for our third and final panel.

I would remind committee members that we now have our third witness panel. We are still examining cyberthreats to Canada's defence infrastructure.

Once again, we have some very interesting witnesses. I would like to welcome Brandon Valeriano, distinguished senior fellow, Marine Corps University, and senior advisor, Cyberspace Solarium Commission 2.0; and Alexis Rapin, research fellow, Raoul-Dandurand Chair of Strategic and Diplomatic Studies, Université du Québec à Montréal. Finally, we welcome, by video conference, Quentin E. Hodgson, senior international defence researcher, RAND Corporation. Welcome and thank you for being here.

devons lancer ces avertissements à nos adversaires. La communication est essentielle pour que la dissuasion soit efficace.

Notre posture doit souligner ces trois éléments. Elle doit attester de notre leadership politique, mais aussi s'appuyer sur une réflexion intelligente du point de vue militaire et stratégique, tant au ministère de la Défense nationale et à Sécurité publique Canada qu'au Centre de la sécurité des télécommunications. Elle doit partir de la base, mais la décision doit être politique.

[*Français*]

Le vice-président : Avant de conclure, j'aurais une question pour M. Wilner. Dans la lutte contre les cybercriminels, est-on condamné à être toujours et seulement sur la défensive, ou pourra-t-on assister un jour à des arrestations et à des mises en accusation de cybercriminels?

[*Traduction*]

M. Wilner : La cybercriminalité est omniprésente. Le Canada doit, entre autres choses, créer des outils et des mécanismes pour stopper la criminalité dès qu'elle se manifeste et pour arrêter les criminels lorsque c'est possible. Il est évident que nous savons le faire à l'échelle nationale, mais nous devons aussi le faire en partenariat avec nos alliés. La lutte contre la criminalité dans le cyberespace est semblable à celle que nous menons partout ailleurs. Nous pouvons tirer d'excellentes leçons de notre lutte contre la criminalité dans l'espace physique. Votre question est excellente. Je n'ai pas de réponse complète à vous donner, mais nous poursuivons cette réflexion.

[*Français*]

Le vice-président : Cela nous amène à la fin de ce groupe de témoins. Je vous remercie tous de votre présence. Vos idées et vos connaissances sont très appréciées. Nous allons suspendre brièvement la séance; nous reviendrons à 18 h 20 pour notre troisième et dernier groupe.

Je rappelle aux membres du comité que nous en sommes à notre troisième groupe de témoins. Nous étudions toujours les cybermenaces à l'endroit de l'infrastructure de défense du Canada.

Nous avons, encore une fois, des témoins très intéressants. Je souhaite la bienvenue à M. Brandon Valeriano, agrégé supérieur émérite, Marine Corps University, et conseiller principal, Cyberspace Solarium Commission 2.0, et à M. Alexis Rapin, chercheur en résidence à la Chaire Raoul-Dandurand en études stratégiques et diplomatiques de l'Université du Québec à Montréal. Enfin, nous accueillons par vidéoconférence M. Quentin E. Hodgson, chercheur principal en défense internationale, RAND Corporation. Bienvenue et merci de votre présence.

You will each have five minutes for your opening remarks, and then the committee members will have some questions. We will begin with Mr. Valeriano. Please go ahead.

[*English*]

Brandon Valeriano, Distinguished Senior Fellow, Marine Corps University and Senior Advisor, Cyberspace Solarium Commission 2.0, as an individual: Thank you. I'm glad to be here, and I hope we can have an interesting session.

To set the stage, cybersecurity and malicious cyber operations represent transformative national and domestic security threats. From weaknesses in systemically critical infrastructure to the vulnerabilities emanating from information campaigns seeking to reshape the hearts and minds of the defender, these threats are pervasive and all-encompassing. However, many purporting a revolution in military affairs brought on by cyber power and other emerging technologies are grossly wrong and misconstrue the threat in dangerous ways. Cyber tools are helpful for some goals, like dismantling confidence in the state or harassing dissidents, but they are poor tools of war and coercion.

For many, the Russo-Ukrainian war was expected to fulfill the age-old warning of a cyberwar. Some contended that this would be a dramatic cyber shock and awe campaign, with others suggesting this would be the first time that states with real cyber capabilities put it all on the line. Yet, these sweeping predictions have not materialized. Instead, the war has evolved into something entirely different than was predicted by most pundits. While there was a dramatic uptick in cyber operations during the conflict, there is no difference in the style of attacks, the targets or the effectiveness of the operations, based on data we've collected on this war. The numbers are stark. There is an increase in operations to 47 incidents in 2022 compared to 28 between 2014 and 2020. What is interesting is that the severity of these incidents actually declined and the targets did not shift to government or military targets. They continued to target the private civilian critical infrastructure.

The overall conclusion we have to take from this is that some of the dramatic outcomes we've seen predicted have dramatically failed. The question, then, is why are we seeing these outcomes? Many will purport to tell you the story of why Russia has failed in its cyber operations, but many will be wrong because these are multi-causal social events and a combination of factors has led to this outcome. We can dissect them during the question-and-

Vous aurez chacun cinq minutes pour faire vos remarques préliminaires, qui seront suivies de questions de la part des membres du comité. Nous commençons avec M. Valeriano. La parole est à vous.

[*Traduction*]

Brandon Valeriano, agrégé supérieur émérite, Marine Corps University, et conseiller principal, Cyberspace Solarium Commission 2.0, à titre personnel : Merci. Je suis heureux d'être ici et j'espère que nous produirons une séance intéressante.

Disons tout d'abord que la cybersécurité et les cyberopérations malveillantes sont des menaces qui transforment la sécurité nationale d'un pays. Elles visent parfois les faiblesses d'infrastructures systémiques critiques et, d'autres fois, des vulnérabilités issues de campagnes d'information qui visent à remodeler le cœur et l'esprit du pays défenseur. Ces menaces sont omniprésentes et touchent tous les aspects du pays. Cependant, bon nombre de ceux qui prétendent que la cyberpuissance et d'autres technologies émergentes ont déclenché une révolution des affaires militaires se trompent lourdement. Cette mauvaise interprétation est dangereuse. Les cyberoutils sont utiles dans certains cas, comme pour miner la confiance des gens envers l'État ou pour harceler des dissidents, mais ce sont de piètres outils de guerre et de coercition.

Bien des gens prédisaient que la guerre russo-ukrainienne répondrait au sempiternel avertissement de l'arrivée d'une cyberguerre. Certains ont soutenu qu'elle produirait une campagne cybernétique spectaculaire, alors que d'autres prédisaient que pour la première fois, les États dotés de véritables cybercapacités les mettraient toutes en jeu. Pourtant, ces prédictions radicales ne se sont pas concrétisées. La guerre s'est déroulée de manière entièrement différente de ce que la plupart des experts avaient prédit. Bien qu'elle ait produit une hausse spectaculaire des cyberopérations, les données recueillies sur cette guerre n'indiquent rien de nouveau dans le style des attaques, les cibles et l'efficacité des opérations. Les chiffres sont frappants. Les opérations ont provoqué 47 incidents en 2022 alors qu'on n'en avait compté que 28 entre 2014 et 2020. Nous avons cependant constaté avec surprise que la gravité de ces incidents a diminué et que ces opérations ne se sont pas tournées vers des cibles gouvernementales ou militaires. Elles ont continué à cibler des infrastructures civiles essentielles privées.

Nous pouvons donc en conclure que les résultats spectaculaires que nous avions prédits ont échoué lamentablement. Pour quelle raison? De nombreuses personnes prétendront expliquer pourquoi les cyberopérations de la Russie ont échoué, mais bon nombre d'entre elles auront tort, parce que ces opérations provenaient d'événements sociaux à multiples causes. Cet échec découle de nombreux facteurs. Nous pourrons

answer period, but the basic point remains that cyber operations have yet to fulfill their stated purpose of battlefield effects.

It is important to remember that the fantasies about the evolution of warfare enabled by cyber operations are purely that — they are fantasies disconnected from reality. Cyber effects are imagined in popular culture, but the reality is much different. Cyber operations and modern technology will not sanitize war. The Russo-Ukrainian war has been a devastating return to old-fashioned war of human waves, tank attacks and trench warfare.

The question is, "Now what?" Evolution under the Biden administration and its National Cybersecurity Strategy has been rather slow but also likely very transformative. The recently released strategy seeks to impose costs economically but does not mention the imposition of costs in or through cyberspace. Military and offensive actions are now downplayed. There is an effort to shift the burden to software and hardware producers to protect the user rather than depending on the state to protect all targets.

For Canada, there are many lessons to be learned. The promise of military dominance in cyberspace has been a dead end and is best avoided. Working to establish strong defensive organizations that can protect critical infrastructure and organize the state for defence is the first step to thwarting the impact of dramatic cyber operations. Taking a lead in the West to protect civil society is warranted and critical. The influence of zero-click malware that can be purchased like a weapon must be moderated and eliminated. The international rules-based order is making progress in establishing norms for cyberspace, but implementation has been disjointed and regulations are lacking. Canada can take the lead here and push for a more realistic vision of cybersecurity internationally.

Overall, a state that cannot keep the lights on, the schools open and the hospitals running is a state with limited power. Preparing for the defence by identifying critical infrastructure targets, organizing for the defence, including having plans for the continuation of the government, and establishing resiliency in both the private and public sectors are critical. Don't be swayed by the dramatic proclamations of futurists; rather, shore up the clear weaknesses evident in society. Organization, developing a workforce, establishing plans to share data between the public and private sector and coordinating the collection and analysis of data are the true roles of the state in the context of cybersecurity. These roles are less dramatic than promised but nonetheless important. Understanding that cybersecurity is truly about secrecy, defence and organization is the first step towards properly countering the threats that emanate from cyberspace.

Thank you.

les disséquer pendant la période de questions, mais essentiellement, les cyberopérations sont loin d'avoir démontré leur efficacité sur le champ de bataille.

Soulignons que l'idée selon laquelle la guerre évoluera dans le domaine des cyberopérations n'est qu'un fantasme très éloigné de la réalité. Il est très attrayant dans l'imagination populaire, mais la réalité est bien différente. Les cyberopérations et la technologie moderne n'assainiront pas la guerre. La guerre russo-ukrainienne a marqué un retour dévastateur au théâtre habituel du déferlement de soldats, d'attaques par chars d'assaut et de la guerre des tranchées.

Alors où en sommes-nous maintenant? L'évolution sous l'administration Biden et sa stratégie nationale en cybersécurité a été plutôt lente, mais transformatrice. La version récente de cette stratégie impose des coûts économiques, mais elle ne mentionne pas de coûts provenant du cyberespace. On y minimise maintenant les opérations militaires d'offensive. On s'efforce de transmettre le fardeau aux producteurs de logiciels et de matériel pour protéger les utilisateurs au lieu de compter sur l'État pour protéger toutes les cibles.

Le Canada a beaucoup de leçons à tirer de cela. La promesse d'une domination militaire dans le cyberespace est sans issue. Il faut absolument l'éviter. Pour contrer les répercussions de cyberopérations spectaculaires, il faut avant tout établir de solides organisations défensives pour protéger les infrastructures essentielles et organiser la défense. Il est crucial que l'Occident se place en tête de file pour protéger la société civile. Il est crucial d'atténuer et d'éliminer l'influence des maliciels à clic nul que l'on peut acheter comme on achète des armes. L'ordre international fondé sur des règles établit des normes pour le cyberespace, mais leur mise en œuvre a été incohérente, et l'on manque de règlements. Le Canada peut jouer un rôle de chef de file à cet égard et promouvoir une vision plus réaliste de la cybersécurité à l'échelle internationale.

En fait, un État incapable de protéger son électricité, ses écoles et le fonctionnement de ses hôpitaux est un État très faible. Il est essentiel que nous protégions nos infrastructures essentielles, que nous organisions notre défense. Nous devons établir des plans pour assurer le maintien du gouvernement et pour renforcer la résilience des secteurs privé et public. Ne vous laissez pas influencer par les proclamations dramatiques des futuristes, mais consolidez plutôt les faiblesses évidentes de notre société. Dans le contexte de la cybersécurité, l'État a pour véritables rôles d'organiser, de développer un effectif, d'établir des plans de partage de données entre les secteurs public et privé ainsi que de coordonner la collecte et l'analyse des données. Ces rôles ne semblent pas spectaculaires, mais ils sont critiques. Pour contrer efficacement les menaces venant du cyberespace, il faut reconnaître que la cybersécurité repose avant tout sur le secret, la défense et l'organisation.

Merci.

[*Translation*]

The Deputy Chair: Thank you, Mr. Valeriano. I now invite Mr. Rapin to make his presentation.

[*English*]

Alexis Rapin, Research Fellow, Raoul-Dandurand Chair of Strategic and Diplomatic Studies, Université du Québec à Montréal, as an individual: Mr. Chair, members of the committee, good evening and thank you for the opportunity to be here today.

My research focuses on issues related to cyber strategy, interstate rivalries in cyberspace and more generally on the impacts of information technology on military affairs and international security.

Since 2019, our research team has maintained a database dedicated to publicly record geopolitical cyber incidents targeting Canada, whether it be its government entities, its companies, its research institutions or its civil society. As of today, throughout our open source research, we have registered a total of 96 geopolitical cyber incidents in Canada since 2010. Among those, at least eight past incidents can be considered as having been directed at defence-related IT infrastructure. These include, for instance, a cyber intrusion at Defence Research and Development Canada in 2011; a Chinese cyber espionage campaign targeting naval technology research institutions in 2019; or, more recently, a ransomware attack against Black & McDonald, a major Canadian defence contractor, in early February. These examples demonstrate that cybersecurity issues related to Canada's defence infrastructure are not futuristic, hypothetical, distant threats for Canada. They are already with us today and, in fact, have been for several years, as some of these incidents illustrate.

These incidents also demonstrate that cyber-threats against Canada's defence infrastructure may take various forms and target various types of entities, not just the federal government. If we consider the defence industrial base as well as the military research and development community as integral parts of the defence infrastructure, we can observe that cyber-threats are not necessarily the same for everyone and that our defence supply chain is only as strong as its weakest links.

In this context, the fast-growing threat of ransomware attacks against Canadian entities, for instance, represents a major challenge for the protection of defence infrastructure. While ransomware attacks are mostly conducted by profit-motivated criminal actors, they may nevertheless entail national security

[*Français*]

Le vice-président : Merci, monsieur Valeriano. J'invite maintenant M. Rapin à faire sa présentation.

[*Traduction*]

Alexis Rapin, chercheur en résidence, Chaire Raoul-Dandurand en études stratégiques et diplomatiques, Université du Québec à Montréal, à titre personnel : Monsieur le président, mesdames et messieurs les membres du comité, bonsoir et merci de m'avoir offert cette occasion de comparaître devant vous aujourd'hui.

Mes recherches portent sur des questions liées à la cyberstratégie, aux rivalités entre États dans le cyberespace et, de façon plus générale, aux répercussions de la technologie de l'information sur les affaires militaires et sur la sécurité internationale.

Depuis 2019, notre équipe de recherche tient une base de données consacrée à l'enregistrement public des cyberincidents géopolitiques ciblant le Canada, tant ses entités gouvernementales que ses entreprises, ses établissements de recherche et sa société civile. À l'heure actuelle, dans le cadre de notre recherche à source ouverte, nous avons enregistré 96 cyberincidents géopolitiques au Canada depuis 2010. Au moins huit de ces incidents peuvent être considérés comme ayant ciblé l'infrastructure de TI liée à la défense. Il s'agit, par exemple, d'une cyberintrusion à Recherche et développement pour la défense Canada en 2011; d'une campagne de cyberespionnage menée par la Chine contre des établissements de recherche en technologie navale en 2019; et, plus récemment, au début février, d'une attaque par rançongiciel contre l'entreprise Black & McDonald, un important entrepreneur canadien en défense. Ces exemples démontrent que les problèmes de cybersécurité liés à l'infrastructure de défense du Canada ne sont pas des menaces futuristes, hypothétiques et lointaines. Nous y faisons face déjà aujourd'hui et, en fait, depuis bien des années, comme certains de ces incidents le démontrent.

Ces incidents indiquent également que les cybermenaces contre l'infrastructure de défense du Canada peuvent prendre diverses formes et cibler divers types d'entités autres que celles du gouvernement fédéral. En tenant compte de la base industrielle de défense et de la communauté de recherche et développement militaires dans l'infrastructure de la défense, nous observons que les cybermenaces visent différentes cibles et que la chaîne d'approvisionnement de notre défense n'est pas plus solide que son maillon le plus faible.

Dans ce contexte, la menace croissante d'attaques par rançongiciel contre des entités canadiennes, par exemple, pose un défi majeur à la protection de l'infrastructure de défense. Bien que les attaques par rançongiciel soient principalement le fait d'acteurs criminels motivés par le profit, elles perturbent souvent

issues. For instance, criminal hacker groups that have compromised strategically important companies may try to covertly sell the data they've stolen to third parties such as foreign powers. This is especially plausible with regard to Russian ransomware gangs, who are strongly suspected of maintaining ties with the Russian intelligence community. In the last 12 months, we have recorded three instances of major Canadian defence contractors being targeted by ransomware attacks. At least one of these — against the aerospace company CMC Electronics — was conducted by a Russian-based group whose relations with the Russian state are not fully understood.

It is also important to mention that we are beginning to see state-sponsored cyber actors using ransomware attacks as cover for clandestine intelligence collection. In recent months, Iranian actors, for instance, have apparently tried to disguise cyber espionage campaigns as criminal cyberattacks in order to confound incident responders and maintain plausible deniability for their actions.

[*Translation*]

Other types of cyberattacks conducted directly by state actors could target Canada's defence infrastructures. It is conceivable and even probable that hostile powers are seeking to infiltrate Canadian systems to map them and evaluate our defences with a view to potential confrontations in the future. Similarly, it is also possible that they will attempt to discretely pre-position malware that could be activated on short notice.

In 2019, for instance, Russian government hackers attempted to explore the digital networks of certain American and Canadian power infrastructures. Such cases show that critical Canadian infrastructures will from now on be actively scrutinized by hostile foreign actors and that much greater vigilance is therefore required.

While national security issues, including cybersecurity, are of growing concern to the Canadian public at this time, it is important that cybersecurity threats are discussed more openly, more vigorously, and with fewer silos from now on.

I think we have an excellent opportunity for that with the group you have gathered here today. I look forward to your questions. Thank you.

The Deputy Chair: Thank you for your presentation, Mr. Rapin.

notre sécurité nationale. Par exemple, des groupes de pirates qui compromettent d'importantes entreprises stratégiques peuvent tenter de vendre secrètement les données qu'ils ont volées à des tiers, comme à des puissances étrangères. Nous le constatons particulièrement dans le cas d'auteurs de rançongiciels russes, qui sont fortement soupçonnés de maintenir des liens avec la communauté du renseignement de leur pays. Au cours de ces 12 derniers mois, nous avons enregistré trois cas où de grands entrepreneurs canadiens de la défense ont été la cible d'attaques par rançongiciel. Au moins un de ces actes, qui a été perpétré contre la société aérospatiale CMC Électronique, venait d'un groupe basé en Russie dont nous ne comprenons pas encore bien la relation avec l'État russe.

Soulignons aussi que des cyberacteurs parrainés par leur gouvernement commencent à utiliser des rançongiciels pour recueillir des renseignements de façon clandestine. Au cours de ces derniers mois, des cyberacteurs iraniens, par exemple, ont apparemment tenté de déguiser des campagnes de cyberespionnage en cyberattaques criminelles afin de confondre les intervenants responsables d'y réagir et de pouvoir nier de façon plausible être les auteurs de ces attaques.

[*Français*]

D'autres types de cyberattaques menées directement par des acteurs étatiques pourraient chercher à viser les infrastructures de défense du Canada. Il est concevable, voire même probable, que des puissances adverses cherchent à infiltrer des systèmes canadiens afin de les cartographier et d'en évaluer les défenses, en vue de potentielles confrontations futures. Dans cette même optique, il est également possible qu'ils cherchent à y prépositionner discrètement des logiciels malveillants, capables d'être activés dans un bref délai.

En 2019, par exemple, des pirates informatiques étatiques russes ont cherché à explorer les réseaux informatiques de certaines infrastructures électriques américaines et canadiennes. De tels cas démontrent que les infrastructures critiques canadiennes sont d'ores et déjà activement scrutées par des acteurs étatiques adverses et doivent donc faire l'objet d'une très grande vigilance.

Alors que les enjeux de sécurité nationale, y compris dans le domaine de la cybersécurité, attirent une attention croissante dans le débat public canadien actuellement, il est important que les menaces en matière de cybersécurité soient désormais discutées plus ouvertement, plus vigoureusement et de manière moins cloisonnée.

L'audience que vous avez convoquée aujourd'hui est, à mon avis, une excellente occasion de le faire. Je me réjouis de répondre à vos questions. Merci.

Le vice-président : Merci beaucoup de votre présentation, monsieur Rapin.

Now for our last witness today, Quentin Hodgson. Mr. Hodgson, you may begin your presentation.

[*English*]

Quentin E. Hodgson, Senior International Defense Researcher, RAND Corporation, as an individual: Thank you for the opportunity to present and talk to you today on this very important topic. I'm a senior international defence researcher for the RAND Corporation, a nonprofit, non-partisan public-policy research organization.

I will not touch too much on the nature of the threat; you have just been given two presentations that have given slightly different takes on the nature of the threat. I will simply note that this idea of cyber-threats to critical infrastructure is not new. If you think back to the U.S. President's Commission on Critical Infrastructure Protection in 1997, it's one of the first times at a national level in the United States, at least, that the concept of cyberattacks against critical infrastructure was raised. Even though that committee said that there was not an impending expectation of a cyberattack, they did find there was widespread capability to exploit infrastructure vulnerabilities.

Since that time, we have seen that not just information communication technologies — the business systems that people rely upon every day, including what we're using right now to conduct this hearing — are subject to exploitation. Increasingly, operational technology, the hardware and software that controls physical processes, is also subject to threats — from the manufacturing sector, to electricity generation and distribution, to water treatment plants. Those are just a few examples.

Dr. Valeriano talked about the nature of what is going on in the Russia-Ukraine conflict. It is an interesting case study of how an adversary could employ cyber capabilities in the context of military operations. There has been a considerable amount of debate about the extent to which Russia has deployed cyber operations, how effective they have been and to what extent we are not getting the whole picture, at least in the public space.

It's important to note that the Russian cyber operations have continued to target many of the same critical infrastructure entities that Russia has always targeted, particularly in Ukraine: government institutions, the media and telecommunications, including, as we know from last February, a very widely reported cyberattack on the satellite communications system provided by Viasat. At the same time, the Ukrainian government noted that the attack on the Viasat system and the end points that were supporting that system had very little effect on military communications.

Nous passons maintenant à notre dernier témoin aujourd'hui, soit M. Quentin Hodgson. Monsieur Hodgson, je vous invite à faire votre présentation.

[*Traduction*]

Quentin E. Hodgson, chercheur principal en défense internationale, RAND Corporation, à titre personnel : Je vous remercie de me donner l'occasion de vous parler aujourd'hui de ce sujet très important. Je suis chercheur principal en défense internationale pour la RAND Corporation, qui se voue à la recherche à but non lucratif et non partisane en politiques publiques.

Je ne m'arrêterai pas trop sur la nature de la menace, car nous venons d'entendre, à ce sujet, deux exposés qui présentent des points de vue légèrement différents. Je tiens simplement à souligner que l'idée des cybermenaces contre les infrastructures essentielles n'est pas nouvelle. Si vous vous souvenez, en 1997, la commission que le président des États-Unis avait chargée d'enquêter sur la protection des infrastructures essentielles a été la première à soulever cette notion de cyberattaques contre les infrastructures essentielles, du moins aux États-Unis. Bien qu'affirmant qu'ils ne s'attendaient pas à ce que le pays subisse une cyberattaque, ses membres ont souligné qu'ils constataient d'amples capacités d'exploiter les vulnérabilités de ses infrastructures.

Depuis, les technologies de communication électroniques, que les gens utilisent quotidiennement et grâce auxquelles nous tenons aujourd'hui cette audience, sont couramment exploitées. De plus, les acteurs de cyberattaques s'en prennent maintenant au matériel et aux logiciels qui contrôlent les processus physiques de fabrication, de génération et de distribution de l'électricité, de traitement de l'eau, et je ne mentionne là que quelques exemples.

M. Valeriano a parlé de la nature du conflit entre la Russie et l'Ukraine. C'est une étude de cas intéressante sur la façon dont un adversaire pourrait utiliser des cybercapacités dans le contexte d'opérations militaires. Il y a eu beaucoup de débats sur la mesure dans laquelle la Russie a déployé des cyberopérations, sur leur efficacité et sur le manque d'un tableau global de tout cela, du moins dans l'espace public.

Il importe de noter que les cyberopérations russes ont continué de cibler bon nombre des mêmes infrastructures essentielles que la Russie a toujours ciblées, en particulier en Ukraine, soit les institutions gouvernementales, les médias et les télécommunications, y compris, comme nous le savons depuis février dernier, une cyberattaque contre le système de communication par satellite fourni par Viasat que les médias ont amplement évoquée. En même temps, le gouvernement ukrainien a fait valoir que l'attaque contre le système Viasat et les points d'entrée qui le soutenaient n'a eu que très peu d'effet sur les communications militaires.

The Russian invasion of Ukraine is an ongoing conflict. It is one from which we should take a note of caution about how much it really will tell us about the future role that cyber operations might play in future conflicts, but that doesn't mean we shouldn't be concerned about the potential threat that cyber can play in future crises or emerging conflicts, particularly with near-peer state adversaries such as Russia and China. There are many ways in which they may desire to affect our critical infrastructure and understand what we are planning, how we plan to deploy and how we plan to support military operations and engage in national security episodes. This is an important area where we should be focusing, even if we're not clear exactly on what the future of cyber conflict may end up being.

What can we do to address these threats? Governments have developed an array of tools and relationships to try to address cyber-threats. A lot of work has been done to try to agree on norms of behaviour in cyberspace, which has met with mixed success, to say the least. Leaders such as President Biden have sought to signal that cyberattacks of critical infrastructure will not be tolerated. There is also a vibrant and growing private sector that is providing cybersecurity services to critical infrastructure entities, including ones that conduct vulnerability assessments and penetration testing, referred to as "hunt operations," to actively identify malicious cyber activity as well as provide incident response. We have seen the development of better and more actionable cyber-threat intelligence-sharing from the government through bodies such as information-sharing analysis organizations. Companies that run a lot of the critical infrastructure we rely upon are more acutely aware of the nature of the threat and how it can potentially affect their operations.

The United States government, as well as others, has often pursued a more voluntary approach to adopting cybersecurity standards rather than imposing regulations. That is increasingly being seen as an insufficient approach to the problem, so more recently in the United States, at least, we have seen some efforts to use existing regulatory and hortatory powers of government, such as the Environmental Protection Agency issuing guidance to the states regarding including cybersecurity as an element of sanitary surveys, which I will note was in the news today as being challenged by the critical infrastructure owner-operators. Also, there is the Transportation Security Administration's work to revise cybersecurity requirements for oil and gas pipelines because of the Colonial Pipeline incident.

L'invasion russe de l'Ukraine est un conflit qui demeure vivant. Il faut donc faire preuve de prudence à l'heure d'en vouloir tirer des conclusions sur le rôle que les cyberopérations pourraient jouer à l'avenir, sans pour autant baisser la garde face à la menace qu'elles peuvent poser dans des crises futures ou des conflits émergents, en particulier avec des adversaires d'États pour ainsi dire comparables à la Russie et à la Chine. Il y a de nombreuses façons dont ils peuvent vouloir influer sur nos infrastructures essentielles et savoir quels sont les forces et les engins militaires que nous prévoyons déployer, et quelle sera notre participation à des incidents touchant la sécurité nationale. C'est un domaine important que nous ne devons pas perdre de vue, même si nous ne savons pas exactement quel sera l'avenir des cyberconflits.

Que pouvons-nous faire pour contrer ces menaces? Les gouvernements ont élaboré toute une gamme d'outils et tissé des relations pour tenter de contrer les cybermenaces. Tout le travail qui a été fait pour essayer de s'entendre sur les normes de comportement dans le cyberespace n'a eu qu'un succès mitigé, c'est le moins qu'on puisse dire. Des dirigeants comme le président Biden ont voulu signaler que les cyberattaques d'infrastructures essentielles ne seront pas tolérées. Il existe également un secteur privé dynamique et en croissance qui fournit des services de cybersécurité aux entités chargées des infrastructures essentielles, notamment en effectuant des évaluations de la vulnérabilité et des tests d'intrusion, dits « opérations de chasse », en cernant activement les activités cybernétiques malveillantes et en intervenant en cas d'incident. Nous avons constaté que le gouvernement est mieux équipé pour un échange plus efficace et viable de renseignements sur les cybermenaces grâce à ces organismes qui s'occupent d'analyser les renseignements échangés. Les entreprises qui gèrent une bonne partie des infrastructures essentielles dont nous dépendons sont plus conscientes de la nature de la menace et des répercussions qu'elle pourrait avoir sur leurs activités.

Le gouvernement des États-Unis, comme d'autres, a eu tendance à faire appel à l'adoption de normes de cybersécurité de manière volontaire plutôt que réglementée, ce qui est de plus en plus considéré comme une approche insuffisante. Plus récemment, aux États-Unis, du moins, nous avons vu certains efforts visant à utiliser un mélange des pouvoirs de réglementation et d'incitation dont dispose le gouvernement. Par exemple, l'Environmental Protection Agency a publié des lignes directrices à l'intention des États concernant l'inclusion de la cybersécurité dans les enquêtes sanitaires, ce qui, je le souligne, a fait les manchettes aujourd'hui parce que la mesure a été contestée par les propriétaires-exploitants des infrastructures essentielles. Il y a aussi le travail de la Transportation Security Administration visant à réviser les exigences en matière de cybersécurité pour les oléoducs et les gazoducs en raison de l'incident du pipeline Colonial.

I'll conclude by noting that attacks on critical infrastructure are not simple things. I agree with Dr. Valeriano that we can often be misled by what we see in the popular culture. These are extremely difficult and complex operations to undertake, so we should take a note of caution and yet also be aware of the threat.

Thank you. I look forward to your questions.

[*Translation*]

The Deputy Chair: Thank you for your presentation, Mr. Hodgson. We will now move on to questions from senators.

I would remind you that, as with previous panels, your time is limited to four minutes for both questions and answers. Let us begin with Senator Boisvenu.

Senator Boisvenu: Thank you to the witnesses, who were very interesting. Mr. Rapin, I am curious about something. How do you detect cyberattacks in your team?

Mr. Rapin: We rely entirely on public reports. We rely on what is reported in the media and in the reports of cybersecurity company, for instance, that have researched the incidents. We rely on statements by the federal government. So we gather information from open sources and try to be as exhaustive as possible, but we do not know any more than what is publicly reported.

Senator Boisvenu: So you do not look further into actors or system weaknesses? Your research does not dig any deeper?

Mr. Rapin: The incidents we identify can of course be used as case studies, and we also look into how the incident unfolded, its cause, what might have been done differently, and so forth. Our first step is to try to gather data as a basis for our examination.

Senator Boisvenu: You stated an opinion that did not surprise me. I was not surprised to hear you say we need discussions with fewer silos. Is that something you have noticed, that there are a lot of silos in the area of cybercrime in Canada? Those silos are often very reluctant to share information. We can see what has been happening in the past three weeks with regard to the Chinese communist government. There are bribes left and right, but no overall picture; is that how you see things in Canada?

Je terminerai en soulignant que les attaques contre les infrastructures essentielles ne sont pas simples. Je suis d'accord avec M. Valeriano pour dire que nous pouvons souvent être induits en erreur par ce que nous voyons dans la culture populaire. Il s'agit d'opérations extrêmement difficiles et complexes à entreprendre, alors il faut être prudent tout en étant conscient de la menace.

Merci. Je serai heureux de répondre à vos questions.

[*Français*]

Le vice-président : Merci beaucoup de votre présentation, monsieur Hodgson. Nous allons passer maintenant aux questions des sénateurs.

Je vous rappelle que, comme pour les groupes précédents, les questions, y compris les réponses, seront limitées à quatre minutes. Nous allons commencer avec le sénateur Boisvenu.

Le sénateur Boisvenu : Merci à nos témoins, qui étaient très intéressants. Monsieur Rapin, j'ai des questions liées à ma curiosité. Comment détectez-vous ces cyberattaques au sein de votre groupe de travail?

M. Rapin : On se base uniquement sur des rapports publics. On se base sur ce qui est relaté dans les médias et sur des rapports de compagnies de cybersécurité, par exemple, qui ont fait des recherches sur des incidents. On se base sur les déclarations du gouvernement fédéral. C'est, en quelque sorte, un travail de récolte de sources ouvertes où l'on essaie d'être aussi exhaustif que possible, mais on n'en sait pas plus que ce qui est divulgué publiquement.

Le sénateur Boisvenu : Vous n'approfondissez donc pas ce qui a trait aux auteurs ou aux faiblesses du système? Vous ne creusez pas plus loin la recherche?

M. Rapin : Évidemment, les incidents que l'on identifie peuvent nous servir à faire des études de cas, et on en fait aussi pour voir comment l'incident s'est déroulé, quelle est la cause de l'incident, ce qui aurait pu être fait différemment et ainsi de suite. La première étape de travail que l'on fait, c'est d'essayer de récolter des données sur lesquelles on peut baser nos réflexions.

Le sénateur Boisvenu : Vous avez émis une opinion qui ne m'a pas fait sursauter. Je n'étais pas surpris; vous dites que cela prend des discussions moins cloisonnées. Est-ce aussi un constat que vous faites, soit que, dans le domaine de la cybercriminalité au Canada, il y a beaucoup de silos? De plus, ces silos sont souvent très avares sur le plan du partage de l'information. On voit un peu ce qui se passe depuis trois semaines en ce qui concerne le gouvernement communiste chinois. Ce sont des bribes qui sortent à gauche et à droite et il y a comme l'absence d'un tout; est-ce votre vision des choses au Canada?

Mr. Rapin: I cannot really say that much about what is happening in the federal government since I don't work there and don't have sensitive information about what has changed or not. I can say for sure, though, that we researchers — and I would say the same thing for the Canadian public in general — , we do not sense a great deal of transparency about what has been done or not been done. That is one of the obstacles we face in assessing the solutions or potential solutions that could be considered. From our perspective, we do not really know what has already been done, what has not yet been done, and what could be done.

Senator Boisvenu: I would like to take part in the second round, Mr. Deputy Chair.

[*English*]

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

Mr. Valeriano, you made some very interesting points in regard to where our focus should be as opposed to being alarmist, but I think Canadians in general are concerned about things when they are happening as opposed to when they're not happening. Your point is in regard to advice for the government to deal with the things that are connected to people's lives so at least there is some confidence in that. In many of the things we have seen that have happened in this country, especially around cybersecurity, malware at hospitals and other institutions, it certainly gives us reasons for being alarmed. It seems the frequency is increasing. More importantly, they are very disruptive when they happen, as we saw with Rogers Communications most recently and some hospitals in that regard.

I would also try to get all the other witnesses to partake in this. I mean, it's not apples or oranges. It's a combination of both. It is being vigilant, but, at the same time, this is an evolving area of responsibility of both the national government and private companies. Given what we have seen and experienced in the country, and given what Mr. Rapin has said in regard to the most recent cyberattack on some specific defence companies, what would you suggest is Canada's effort in the evolution of this given we're a federation? The federal government is limited in regard to what it can do nationally, but it also has to work with the provinces and territories if we want to have a comprehensive strategy in dealing more specifically with some of the things that you outlined in your remarks.

Mr. Valeriano: In the United States, we often talk about a whole-of-nation approach. The reality is that we're not even developing whole-of-department approaches. We need to think broadly. We need to think collaboratively. Academics often speak of public-private collaboration in cyberspace. Working in policy these last 10 years, I can tell you that I have not seen

M. Rapin : Je peux moyennement me prononcer sur ce qui se passe à l'intérieur du gouvernement fédéral, car je n'y travaille pas et je n'ai pas d'informations privilégiées sur ce qui a changé ou non. Ce qui est certain, c'est que nous, en tant que chercheurs — et je dirais la même chose pour le public canadien en général —, n'avons pas le sentiment qu'il y a beaucoup de transparence sur ce qui est fait ou ce qui n'est pas fait. Pour nous, c'est l'un des obstacles que l'on rencontre pour poser un jugement sur les solutions ou les pistes de solutions qui pourraient être envisagées. Selon notre perspective, on ne sait pas très bien ce qui est déjà fait, ce qui n'est pas encore fait et ce qui pourrait être fait.

Le sénateur Boisvenu : J'aimerais m'inscrire pour la deuxième ronde, monsieur le vice-président.

[*Traduction*]

Le sénateur Yussuff : Je remercie les témoins de leur présence.

Monsieur Valeriano, vous avez soulevé des points très intéressants au sujet de ce qu'il ne faut pas perdre de vue au lieu de nous montrer alarmistes, mais je pense que les Canadiens en général s'inquiètent des faits lorsqu'ils se produisent plutôt que lorsqu'ils ne se produisent pas. Ce que vous voulez dire, c'est qu'il faut conseiller au gouvernement de s'occuper des choses qui ont un lien avec la vie des gens, pour qu'au moins on ait confiance en cela. Dans bien des cas, notamment en ce qui concerne la cybersécurité, les logiciels malveillants dans les hôpitaux et d'autres établissements, il va de soi que nous avons de quoi nous alarmer, et de plus en plus, à ce qu'il semble. Mais surtout, ils sont très perturbateurs lorsqu'ils se produisent, comme nous l'avons vu récemment avec Rogers Communications et certains hôpitaux.

J'aimerais aussi que tous les autres témoins participent. Ce n'est pas une question de pommes et de poires, mais d'un mélange des deux. Il s'agit de faire preuve de vigilance, mais en même temps, c'est un domaine de responsabilité en évolution du gouvernement national et des entreprises privées. Compte tenu de ce que nous avons vu et de ce que nous avons vécu au pays, et compte tenu de ce que M. Rapin a dit au sujet de la cyberattaque la plus récente contre certaines entreprises de la défense, quel effort le Canada devrait-il déployer à titre de fédération? Le gouvernement fédéral est limité quant à ce qu'il peut faire à l'échelle nationale, mais il doit aussi travailler avec les provinces et les territoires si nous voulons avoir une stratégie globale et aborder avec plus de précision certains aspects que vous avez relevés dans votre exposé.

M. Valeriano : Aux États-Unis, il est souvent question de notre approche pancanadienne. Or, en réalité, nous n'élaborons même pas des approches à l'échelle ministérielle. Nous devons penser de façon générale. Nous devons penser en collaboration. Les universitaires parlent souvent de collaboration entre les secteurs public et privé dans le cyberespace. Ayant travaillé dans

much collaboration. There is contact. There is working together. But there is no sharing of information. There is no sharing of threat data. In fact, the cyber intelligence community often sees this as a business. I'm very concerned, particularly in the United States, that in making this a business, they have sold so much data to so many different silos, as my co-presenter said, that we're not able to share and collaborate.

I think the first and the most important thing is understanding the need for data — that data can be the canary in the coal mine — and getting data up to the federal government and all the way down to the private sector will be a problem. In the United States, there are intense legal barriers. There was recently an incident reporting law that was passed, but that law will not be implemented for at least two years. We don't know how to implement these laws. We don't know how to analyze this data. We don't know how to share data.

I think solving the federal problem of how you share data, how you collaborate and how you share information is really the first step to getting the defence right. We, sadly, don't talk about this enough. I think it's a very critical problem, but you have to ask who holds the data, who is analyzing the data, who is sharing the data and then go from there.

[*Translation*]

Mr. Rapin: I will answer in French, if I may.

The Deputy Chair: You still have some time left.

[*English*]

Senator Yussuff: If he wants to offer any advice, yes.

[*Translation*]

The Deputy Chair: Mr. Rapin, would you like to say something?

Mr. Rapin: To answer your question, yes.

I think you have touched on something very important. A number of critical infrastructures are not operated by federal entities, but rather by entities at lower levels of government. In the past, in the United States, for instance, foreign cyber actors have investigated, if you will, infrastructure at the regional or local level, because they assumed that the entities operating them would have fewer resources, that they might not be as well defended and that they would have less expertise to protect them. That is the reality. Municipalities, for example, do not have the same resources to protect the cybersecurity of certain infrastructure.

le domaine des politiques au cours des 10 dernières années, je peux vous dire que je n'ai pas vu beaucoup de collaboration. Il y a un contact. On travaille ensemble. Mais il n'y a pas d'échange d'information. Pas d'échange de données sur les menaces. En fait, la communauté du cyberrenseignement a tendance à se voir comme une entreprise. Je suis très préoccupé, surtout aux États-Unis, par le fait qu'en faisant de ce secteur une entreprise, ils ont vendu tellement de données à tellement de silos différents, comme l'a dit mon collègue, que nous ne sommes pas en mesure de faire des échanges et de collaborer.

Je pense que la première chose, et la plus importante, c'est de comprendre le besoin de données — que les données peuvent être le canari dans la mine de charbon — et que leur transmission au gouvernement fédéral et jusqu'au secteur privé sera un problème. Aux États-Unis, les obstacles juridiques sont énormes. Ils ont encore tout récemment adopté une loi sur le signalement des incidents, mais elle n'entrera pas en vigueur avant au moins deux ans. Nous ne savons pas comment appliquer ces lois. Nous ne savons pas comment analyser ces données. Nous ne savons pas comment échanger les données.

Je pense que la solution du problème fédéral d'échange des données, de collaboration et de partage de l'information est vraiment la première étape pour bien se préparer à la défense. Malheureusement, nous n'en parlons pas assez. Le problème est très grave, mais il faut se demander qui détient les données, qui les analyse, qui les diffuse, pour ensuite procéder à partir de là.

[*Français*]

M. Rapin : Je vais répondre en français, si vous me le permettez.

Le vice-président : Vous avez encore du temps.

[*Traduction*]

Le sénateur Yussuff : S'il veut donner des conseils, oui.

[*Français*]

Le vice-président : Monsieur Rapin, voulez-vous faire un commentaire?

M. Rapin : Pour répondre à votre question, oui.

Je pense que vous avez touché un point très important. Plusieurs infrastructures critiques ne sont pas opérées par des entités fédérales, mais par des entités se trouvant à de plus bas échelons. Par le passé, aux États-Unis, par exemple, des acteurs cyberétrangers ont sondé, si l'on veut, des infrastructures plus régionales ou locales, parce qu'ils présumaient que les entités qui les opèrent auraient moins de ressources, que les infrastructures seraient peut-être moins bien défendues et qu'il y aurait moins d'expertise pour les protéger. C'est une réalité. Les municipalités, par exemple, n'ont pas les mêmes ressources pour assurer la cybersécurité de certaines infrastructures.

Consideration must be given at various levels to ensure very high security standards, and not just at the federal level. There is still a lot of complacency at the lower levels.

[*English*]

Senator M. Deacon: Mr. Hodgson, when you were speaking in your opening, you finished off with "Here are some of the things that are being done, and here are some of the things we can acknowledge as being done." I just want come back to you in that thinking. If you were to carry on with what you were saying about "Here are some of the things," and you comment on the U.S., what do you think are the misses right now that we need to react to first or act on first?

Mr. Hodgson: Thank you.

I agree that sharing of information is a key part of this. One of the things we have seen, though, is initially the sharing of information was seen as an unaltered good. Push as much information out there as can possibly be done. Of course, that just creates an overwhelming wave of information that people find very difficult to wade through. Some more recent action is taking place, where it's the U.S. government trying to share more actionable intelligence at levels that could be shared with entities, that's actually shown some improvement, and not just in terms of here is what the nature of the threat is, but here is what actually can be done to address it. I'm actually a little more optimistic that action has been taken to make that kind of information sharing better, but, of course, that's on things that we can see right now.

The other area that needs to be focused on and that I didn't touch on but is in my prepared remarks is on the resiliency aspect. How can we work to make sure that the critical infrastructure sectors are prepared for when things go wrong? They inevitably will. We have to be working on the contingency plans to make sure that we can fail gracefully as opposed to fail catastrophically.

Senator M. Deacon: If we move that from the sharing of information to action, jump in there literally on the field, you touched on the Russian actions in Ukraine. Absolutely, they have launched cyberattacks on critical infrastructure, as you said earlier, but they also relied on conventional weapons to do this as well. I am wondering, from your perspective, if we have learned anything from this conflict about how cyberwarfare will be employed in a conventional state-to-state conflict between two developed economies like that.

Mr. Hodgson: I think to a limited degree. Generally speaking, when it comes to a shooting war, the level of confidence that we might have in the employment of cyber capabilities to have an impact on critical infrastructure — to be honest, from the Russian perspective, I'm sure this is the same — is going to be

Il faut tenir une réflexion à différents niveaux pour s'assurer qu'il n'y a pas des normes très élevées seulement à l'échelle fédérale. On est encore très complaisant aux échelons inférieurs.

[*Traduction*]

La sénatrice M. Deacon : Monsieur Hodgson, dans votre déclaration préliminaire, vous avez conclu en mentionnant que certaines choses sont en train de se faire et qu'il en est d'autres que nous pouvons reconnaître comme étant faites. J'aimerais revenir à cette réflexion. Si vous poursuiviez dans cette veine en commentant la situation aux États-Unis, quelles sont, selon vous, les lacunes actuelles que nous devons aborder ou combler en premier?

M. Hodgson : Merci.

Je conviens que l'échange de renseignements est un élément clé. L'une des choses que nous avons constatées, cependant, c'est qu'au départ, cet échange est considéré comme un bien immuable. Diffusez le plus d'information possible. Bien sûr, cela crée une vague écrasante d'information où les gens ont beaucoup de mal à s'y retrouver. Des mesures plus récentes ont été prises, c'est-à-dire que le gouvernement des États-Unis essaie d'échanger des renseignements plus facilement exploitables à des niveaux où ils peuvent être confiés à des entités, ce qui a permis de constater une certaine amélioration, et pas seulement en ce qui a trait à la nature de la menace, mais voilà ce qui peut être fait pour régler le problème. En fait, je suis un peu plus optimiste quant aux mesures qui ont été prises pour améliorer ce genre d'échange de renseignements, mais, bien sûr, il s'agit de choses que nous pouvons voir en ce moment.

L'autre aspect sur lequel il faut se concentrer et que je n'ai pas abordé, mais que j'ai préparé, concerne la résilience. Comment pouvons-nous nous veiller à ce que les secteurs des infrastructures essentielles soient prêts lorsque ça ira mal? Et cela arrivera inévitablement. Nous devons travailler sur les plans d'urgence pour nous assurer que nous pouvons échouer la tête haute plutôt que de façon catastrophique.

La sénatrice M. Deacon : Si nous passons de l'échange d'information à l'action, en intervenant littéralement sur le terrain, vous avez parlé des actions de la Russie en Ukraine. Absolument, ils ont lancé des cyberattaques sur des infrastructures essentielles, comme vous l'avez dit plus tôt, mais ils comptaient également sur des armes conventionnelles pour le faire. Je me demande, de votre point de vue, si nous avons tiré des leçons de ce conflit sur la façon dont la cyberguerre sera utilisée dans un conflit conventionnel entre deux États développés comme ceux-là.

M. Hodgson : Je pense qu'elle le sera dans une certaine mesure. De façon générale, lorsqu'il s'agit d'une guerre frontale, le degré de confiance que nous pouvons avoir dans l'utilisation de cybercapacités pour avoir un impact sur les infrastructures essentielles — pour vous dire franchement, du point de vue de la

less than, quite frankly, using kinetic action. In those kinds of circumstances where the target, such as critical infrastructure like an electric power grid, is reachable by kinetic means, I think most governments that are engaged in conflict will rely more on that than they would rely on cyber capabilities. Cyber capabilities will be a sideshow. It will be an important way for these adversaries to try to sow confusion, to try to understand what we're planning and how we are planning to conduct things.

Also, if I were sitting in their shoes, they would probably want to focus more on the support infrastructure that is more amenable to these kinds of things, such as the logistic systems, the small- and medium-sized businesses that are providing key services to military operations in ways that are really important but we don't necessarily think about. It's sort of the equivalent of the ball-bearing plants in World War II. What are those key critical supplies? We saw it similarly within the COVID-19 pandemic with the development of vaccines and how adversaries were going after supply chains there as well.

Senator Cardozo: I would like to ask you a question that I asked the previous witnesses. Since two of you are from the U.S., I would be interested in your thoughts. We focus a lot on the cyber-threat coming from other countries such as China, Russia, North Korea and Iran — I don't know if anyone is thinking about the next batch of countries that will be a threat in the next few years — but we don't think much about cyber-threat coming from within. Are you thinking about bad actors within Canada and especially within North America, some of the forces that are getting pretty angry about how our countries are run and are reaching to new extremes in terms of how they respond to that? Do you have concerns about homegrown or North American-grown cyber-threats? I would like to hear all three of you on that, if I could.

Mr. Valeriano: Yes, sure. I was particularly delighted that the new Biden National Cybersecurity Strategy mentioned criminals as the fifth major actor and that it was not just Russia, China, North Korea and Iran. We need to stop, in this community, blaming everything on the Big Four. In fact, I think it's more important that we understand the relations of the target states and what they are doing to prepare and what they may not be doing to prepare to counter these threats.

Now, on the issue of homegrown threats and insider threats, these have always been pervasive, and they will never go away. In fact, they may be the most pernicious threat. But, really, I worry about the threat of what the state may do to the individual. What will happen in terms of repression, which we saw with Pegasus and what the Citizen Lab has uncovered? That's going to be the most important thing moving to the future. It's not so

Russie, je suis certain que c'est la même chose — sera manifestement inférieur à celui obtenu par l'action cinétique. Dans ce genre de situation où la cible, disons une infrastructure essentielle comme un réseau électrique, peut être atteinte par des moyens cinétiques, je pense que la plupart des gouvernements en guerre s'y fieront davantage qu'ils ne se fieraient aux cybercapacités. Les cybercapacités seront un accessoire. Ce sera un moyen important pour ces adversaires d'essayer de semer la confusion, d'essayer de comprendre ce que nous planifions et comment nous prévoyons mener les choses.

De plus, si j'étais à leur place, ils voudraient probablement se concentrer davantage sur l'infrastructure de soutien qui se prête davantage à ce genre de choses, comme les systèmes logistiques, les petites et moyennes entreprises qui fournissent des services essentiels aux opérations militaires, mais auxquelles nous ne pensons pas nécessairement. C'est un peu l'équivalent des usines de roulements à billes de la Seconde Guerre mondiale. Quelles sont ces fournitures essentielles? Nous avons vu la même chose pendant la pandémie de COVID-19 avec la mise au point de vaccins et la façon dont les adversaires s'attaquaient aux chaînes d'approvisionnement.

Le sénateur Cardozo : J'aimerais vous poser une question que j'ai posée aux témoins précédents. Puisque deux d'entre vous viennent des États-Unis, j'aimerais savoir ce que vous en pensez. Nous insistons énormément sur la cybermenace venant d'autres pays comme la Chine, la Russie, la Corée du Nord et l'Iran — je ne sais pas si quelqu'un pense à la prochaine série de pays qui constitueront une menace au cours des années à venir —, mais nous ne pensons que très peu à la cybermenace venant de l'intérieur. Pensez-vous aux acteurs malveillants au Canada et, surtout, en Amérique du Nord, à certaines forces qui sont très en colère au sujet de la façon dont nos pays sont gérés et qui cherchent à y réagir de façon plus extrémiste que jamais? Avez-vous des préoccupations au sujet des cybermenaces nationales ou nord-américaines? J'aimerais vous entendre tous les trois à ce sujet, si possible.

M. Valeriano : Oui, bien sûr. J'ai été particulièrement ravi de constater que la nouvelle stratégie nationale en cybersécurité de M. Biden mentionnait les criminels comme le cinquième acteur majeur et qu'il ne s'agissait pas seulement de la Russie, de la Chine, de la Corée du Nord et de l'Iran. Nous devons cesser, dans cette collectivité, de tout mettre sur le dos des quatre grands. En fait, je pense qu'il vaudrait mieux que nous comprenions les relations des États cibles et ce qu'ils font ou ne font pas pour se préparer à contrer ces menaces.

En ce qui concerne les menaces d'origine nationale et qui se produisent à l'interne, elles ont toujours été omniprésentes et ne disparaîtront jamais. En fait, c'est peut-être la menace la plus pernicieuse. Mais, vraiment, je m'inquiète quant à moi de la menace que l'État peut faire à la personne. Qu'adviendra-t-il sur le plan de la répression, comme nous l'avons vu avec Pegasus et ce que le Citizen Lab a découvert? Ce sera l'élément le plus

much what these right-wing extremists might do to the state but what may happen when other states target what they view as extremists operating within your state — dissidents and diaspora communities. These are the main targets moving forward, and this is what I'm really concerned about in the future.

[*Translation*]

Mr. Rapin: I have a methodology problem: I think our database is designed to focus on incidents coming from outside Canada. We do not automatically consider what might be initiated from within our borders. With regard to the information and disinformation featured in certain conspiracy theories that circulate a lot in Canada and that can be destabilizing factors, these narratives clearly come from our neighbours south of the border. These narratives are devised and democratized by political forces south of the border. The potential emulation and dissemination of "dangerous" narratives is of course something we should be thinking about.

[*English*]

Senator Cardozo: Mr. Hodgson, do you have thoughts on that?

Mr. Hodgson: It is also a challenge, the insider threat, as you mentioned. One of the key pieces of this, which we've talked about, is ransomware. You are seeing more and more of the commoditization of some of these basic tools that could be used to be very disruptive. I agree with Dr. Valeriano that we do also have to be concerned about trying to employ tools that become overly repressive or end up treating everyone like they're a potential perpetrator of cyber incidents.

One of the things we also discovered in the cybersecurity field is that the more onerous the controls we try to place on the user, the more they are going to try to find a way to circumvent them. They may not be malicious in what they are trying to do, but it can have some negative impacts.

We have seen ransomware — which, to be honest, at its root level is not a terribly sophisticated tool and is often exploiting very basic vulnerabilities, including human vulnerabilities like the fear of missing out, clicking a link and so forth — which can lead to pretty disruptive actions. There are technological but there are also educational as well as organizational things that need to be done to try to improve the cybersecurity posture. As I mentioned previously, how do you create better resilience in these organizations so that the one click doesn't lead to shutting down a hospital for a week?

important à l'avenir. Il ne s'agit pas tant de ce que ces extrémistes de droite peuvent faire à l'État que de ce qui peut arriver lorsque d'autres États ciblent ce qu'ils considèrent comme des extrémistes travaillant sur place — des dissidents et des communautés de la diaspora. Ce sont les principaux objectifs pour l'avenir, et c'est ce qui m'inquiète vraiment.

[*Français*]

M. Rapin : Je fais face à un problème méthodologique : notre base de données est pensée pour se concentrer sur les incidents provenant de l'extérieur. On n'a pas le réflexe d'examiner ce qui pourrait provenir du Canada. Ce qui est sûr, sur le terrain de l'information et de la désinformation qui est prévalent sur certaines théories du complot qui circulent beaucoup au Canada et qui peuvent être des facteurs déstabilisants, c'est que, bien souvent, ces discours proviennent de nos voisins du Sud. Ce sont des narratifs conçus et démocratisés par des forces politiques présentes chez nos voisins du Sud. Bien sûr, ce potentiel d'émulation et de dissémination des narratifs « dangereux » est une chose à laquelle on doit songer.

[*Traduction*]

Le sénateur Cardozo : Monsieur Hodgson, qu'en pensez-vous?

M. Hodgson : C'est aussi un défi, la menace interne, comme vous l'avez mentionné. L'un des éléments clés, dont nous avons parlé, est le rançongiciel. On assiste de plus en plus à la banalisation de certains de ces outils rudimentaires qui pourraient être très perturbateurs. Je suis d'accord avec M. Valeriano pour dire que nous devons bien réfléchir avant d'utiliser des outils qui deviennent trop répressifs ou qui finissent par traiter tout le monde comme d'éventuels auteurs de cyberincidents.

Un autre élément que nous avons également découvert dans le domaine de la cybersécurité, c'est que plus les contrôles que nous essayons d'imposer à l'utilisateur sont onéreux, plus on s'efforcera de trouver un moyen de les contourner. Ce ne sera pas forcément malveillant, mais il peut y avoir des répercussions négatives.

Nous avons vu des rançongiciels — qui, pour être honnête, à la base, ne sont pas un outil terriblement sophistiqué qui exploite souvent des vulnérabilités très fondamentales, y compris des vulnérabilités humaines comme la crainte de manquer l'occasion, le fait de cliquer sur un lien et ainsi de suite — qui peuvent mener à des actions assez perturbatrices. Il y a de la technologie, mais il y a aussi des mesures éducatives et organisationnelles qui doivent être prises pour essayer d'améliorer la situation en matière de cybersécurité. Comme je l'ai déjà dit, comment peut-on améliorer la résilience de ces organisations pour éviter qu'un simple clic mène à la fermeture d'un hôpital pendant toute une semaine?

Senator Cardozo: Thank you.

Senator Dasko: The concept of the development of norms has come up a couple of times from Mr. Valeriano and Mr. Hodgson. Both mentioned norms in their presentations, and others mentioned it earlier today. If the departments themselves cannot be organized, how can we develop norms? Who would be part of the development of norms? I'm wondering if you could comment on this. Is this something that is feasible? Is this the way to deal with some of the issues in this field? Who would the norms apply to? What would they involve? Is this development of norms something that takes the place of a regulatory framework or laws? Any of the witnesses can comment on the concept because it has come up a number of times.

Mr. Valeriano: It's an interesting and important question, and it animates a lot of research. We do have an extensive system of norms in the international community, but as I mentioned, there are not a lot of standards and regulations to enforce these norms. That's why standards and regulations go hand in hand with norms. That's why international law goes hand in hand with norms. For norms to work, we need strong entrepreneurs in the system. The norms that are being developed in the UN have been progressive, but there have also been extensive attempts to dismantle the development of these norms, particularly by Russia. For states like Canada, particularly right now with Singapore being in charge of the open-ended working group, these are the important moments to step up and to articulate what sorts of norms we want the rules-based order to operate under. But as to what these norms will be and how we will enforce them, these are the open-ended questions. The first step is developing a strong regime of rules, standards and regulations to move forward.

[*Translation*]

The Deputy Chair: Before we begin the second round, I have a question for Mr. Valeriano. I have already asked other witnesses this question. Given our proximity to the United States, could Canada serve as a computer base for cybercriminals targeting the United States?

[*English*]

Mr. Valeriano: Sure, I think anyone can. We are obviously seeing this extending very deeply into Latin America right now, so everyone needs to be prepared. Everyone can be a victim. Canada has a particular challenge not just from criminals but also from China. There are clear worries in this domestic space. There are things that you need to do in order to shore up your defences.

Le sénateur Cardozo : Merci.

La sénatrice Dasko : MM. Valeriano et Hodgson ont parlé à quelques reprises de l'élaboration de normes. Les deux ont parlé de normes dans leurs exposés, et d'autres l'ont mentionné plus tôt aujourd'hui. Si les ministères eux-mêmes ne peuvent s'organiser, comment pouvons-nous élaborer des normes? Qui participerait à l'élaboration des normes? J'aimerais savoir ce que vous en pensez. Est-ce faisable? Est-ce la façon de régler certains problèmes dans ce domaine? À qui les normes s'appliqueraient-elles? Qu'est-ce que cela impliquerait? L'élaboration de normes remplace-t-elle un cadre réglementaire ou des lois? N'importe lequel des témoins peut commenter le concept parce qu'il a été soulevé à plusieurs reprises.

M. Valeriano : C'est une question intéressante et importante qui suscite beaucoup de recherches. Nous avons un vaste système de normes dans la communauté internationale, mais comme je l'ai mentionné, il n'y a pas beaucoup de règles pratiques. C'est pourquoi les normes et les règlements vont de pair avec les règles pratiques et le droit international. Pour que les normes fonctionnent, nous avons besoin d'entrepreneurs bien établis dans le système. Les normes élaborées aux Nations unies sont progressistes, mais il y a aussi eu de nombreuses tentatives d'empêcher leur élaboration, en particulier par la Russie. Pour des États comme le Canada, particulièrement à l'heure actuelle, puisque Singapour est responsable du groupe de travail à composition non limitée, ce sont des moments importants pour intervenir et énoncer le genre de normes que nous voulons pour faire régner la primauté du droit. Quant à la nature de ces normes et à la façon dont nous les appliquerons, ce sont des questions ouvertes. La première étape consiste à élaborer un solide régime de normes et de règlements pour aller de l'avant.

[*Français*]

Le vice-président : Avant de passer au deuxième tour, j'ai une question pour M. Valeriano. J'ai déjà posé la question à d'autres témoins. À cause de notre proximité avec les États-Unis, est-ce que le Canada pourrait servir de base informatique pour des cybercriminels visant les Américains?

[*Traduction*]

M. Valeriano : Bien sûr, je pense que n'importe qui peut le faire. De toute évidence, la situation s'étend très profondément en Amérique latine en ce moment, alors tout le monde doit être prêt. Tout le monde peut être une victime. Le Canada fait face à un défi particulier, non seulement de la part des criminels, mais aussi de la part de la Chine. Il y a des inquiétudes évidentes dans cet espace national. Il y a des choses que vous devez faire pour renforcer vos défenses.

[*Translation*]

The Deputy Chair: Mr. Hodgson, I can imagine that our power stations, drinking water reservoirs and data banks could become key targets. If someone wants to disrupt activities in a country, as we saw in Ukraine, they attack the power stations. Do we have any information about the interests of other countries where cybercriminals might attack those infrastructures?

[*English*]

Mr. Hodgson: It's hard to understand the potential motivations. Going back to my point about the declaration or sort of deterrent value of statements, President Biden presented a statement to President Putin when they met in Geneva a while back about attacks on critical infrastructure not being tolerated. For a nation-state, even one such as Russia which is engaging in pretty horrendous acts in Ukraine, I think they understand that the stakes are much higher if they are going to be targeting critical infrastructure in a destructive manner. We have seen a lot of probing of networks, understanding what the networks look like and stealing of intellectual property. In some cases, it's unclear what the actual intents behind those are, and that's why it's been important to signal why we find those inappropriate.

To tie back to the previous question about norms, it's been really important that the international community has come together to express what it believes is inappropriate behaviour, such as happened with the Chinese exploitation of Microsoft Exchange server vulnerabilities in 2021. NATO, the European Union, the United States, Canada and the U.K. had all released statements to identify and point the finger at the people who perpetrated it. They pointed out that they thought it was not just inappropriate but indiscriminate, and that was really not acceptable behaviour. Will that stop it from happening? No, I don't think it will, but it does show that there's resolve. Norms are about how you act, not just about what you say.

[*Translation*]

Senator Boisvenu: My question is for Mr. Valeriano. Yesterday, the newspaper *La Presse* published an article about a thousand secrets, a thousand dangers, which also referenced the previous witness. That article indicates that the Chinese government's fundamental strategy is to gather information. In addition, China passed legislation in 2017 that requires Chinese citizens, wherever they might be in the world, to gather information for the Chinese government in order to improve its ability to penetrate computer systems or political systems.

[*Français*]

Le vice-président : Monsieur Hodgson, on peut penser que les centrales électriques, les réserves d'eau potable et nos banques de données peuvent devenir des cibles de choix. Si l'on veut perturber les activités d'un pays, comme on l'a vu en Ukraine, on s'attaque à des centrales électriques. Est-ce qu'on a des indices sur les intérêts d'autres pays où des cybercriminels pourraient s'attaquer à ces infrastructures?

[*Traduction*]

M. Hodgson : Il est difficile de comprendre les motivations possibles. Pour revenir à ce que je disais au sujet de la déclaration ou de la valeur soi-disant dissuasive des déclarations, lorsqu'ils se sont réunis à Genève il y a quelque temps, le président Biden a déclaré au président Poutine que des attaques contre les infrastructures essentielles ne seraient pas tolérées. Pour un État-nation, même un État comme la Russie qui se livre à des actes effroyables en Ukraine, je pense qu'il comprend que les enjeux deviennent beaucoup plus élevés s'il cherche à détruire des infrastructures essentielles. Nous avons vu beaucoup d'exploration des réseaux pour en comprendre l'intérêt et voler la propriété intellectuelle. Dans certains cas, il n'est pas clair quelles sont les intentions réelles derrière ces gestes, d'où l'importance de faire valoir pourquoi nous les trouvons inappropriés.

Pour revenir à la question précédente sur les normes, il est très important que la communauté internationale se réunisse pour exprimer ce qu'elle considère comme un comportement inapproprié, comme ce fut le cas avec l'exploitation chinoise des vulnérabilités du serveur Microsoft Exchange en 2021. L'OTAN, l'Union européenne, les États-Unis, le Canada et le Royaume-Uni ont tous publié des déclarations visant à recenser et à dénoncer les auteurs du crime. Ils ont fait remarquer qu'ils trouvaient que c'était non seulement inapproprié, mais aussi injustifié, un comportement vraiment inacceptable. Est-ce que cela va empêcher que ça se reproduise? Non, je ne le crois pas, mais cela montre qu'il y a une volonté. Les normes s'appliquent au geste, et pas seulement à la parole.

[*Français*]

Le sénateur Boisvenu : Ma question s'adresse à M. Valeriano. Hier, *La Presse* a fait paraître un article fondamental dont le titre était « Mille secrets, mille dangers », qui citait d'ailleurs le témoin précédent. Ce que l'article nous dit, c'est que la stratégie de base du gouvernement chinois, c'est la cueillette d'information. D'ailleurs, la Chine a adopté en 2017 une loi qui oblige les citoyens chinois, peu importe où ils sont dans le monde, à recueillir de l'information pour le gouvernement chinois, afin d'améliorer sa compétence pour ce qui est de percer des systèmes informatiques ou des systèmes politiques.

My colleague asked you this earlier: is Canada more vulnerable to this than the United States? Experts say that Canada is the weak link in cyber protection of North America because it can be easily penetrated. It is much easier than going to China to gather information.

For the United States, which has major systems for North American protection, among other things, this makes Canada the weak link. Is that of great concern to Americans?

[*English*]

Mr. Valeriano: I wouldn't say it's a concern; I believe it's a reality. I believe it's something that everyone's aware of. I think it's very true that China is trying to seek and collect as much data as possible. The challenge is also what they are going to do with that data. We have known for a long time that China has swept up OPM data. It has swept up Marriott passport data. It has swept up various airline data. To what end? I work with machine learning data all the time. I work with collected data by A.I. systems. I can tell you that it's very difficult to analyze and produce any actionable intelligence from this data. I wouldn't say we ignore this problem. I think we need to leverage data for our own ends. We need to use data proactively to defend the nation.

[*Translation*]

Senator Boisvenu: Knowing that it is much easier for Chinese spies to live in America, whether in Canada or the United States, and it is much more difficult for us to go to China to spy on the communist system which has pervasive control over its citizen, what strategy should be taken to address the threats from China and Russia, but especially China?

[*English*]

Mr. Valeriano: Yes. I think that's a realistic challenge right now. I know that we're not very good at adversary work and perceptions and that we worry very much about what they are attacking and not so much about what they are developing and how things are undertaken within their own state. I think it's a blind spot. It's a weakness. We think a lot about cyber intelligence, but we don't think about cyber intelligence to understand the behaviour of the opposition. I think the behavioural aspect of cybersecurity is one of the most important challenges that we have right now that I think a lot of people, particularly academics, are failing at.

Mon collègue vous a posé la question plus tôt : est-ce que le Canada est vulnérable sur ce point face aux États-Unis? Les experts disent que le maillon faible dans la protection cybernétique en Amérique du Nord, c'est le Canada, parce qu'il est facile d'y pénétrer. C'est beaucoup plus facile que d'aller en Chine pour y chercher de l'information.

Pour les États-Unis, qui ont des systèmes très importants sur le plan de la protection nord-américaine, entre autres, cette situation fait en sorte que le Canada est le maillon faible. Est-ce que cela préoccupe beaucoup les Américains?

[*Traduction*]

M. Valeriano : Je ne dirais pas que c'est une préoccupation; je crois que c'est une réalité. Je crois que tout le monde est au courant. Il est manifeste que la Chine essaie de recueillir le plus de données possible. Le défi, c'est ce qu'elle va faire avec ces données. Nous savons depuis longtemps que la Chine a balayé les données du bureau de gestion du personnel américain. Elle a balayé les données des passeports détenus par la chaîne Marriott. Elle a balayé diverses données des compagnies aériennes. Dans quel but? Je travaille constamment avec des données d'apprentissage automatique recueillies par des systèmes d'intelligence artificielle. Je peux vous dire qu'il est très difficile d'analyser et de produire des renseignements exploitables à partir de ces données. Nous sommes conscients de ce problème. Je pense que nous devons tirer parti des données à nos propres fins. Nous devons utiliser les données de façon proactive pour défendre la nation.

[*Français*]

Le sénateur Boisvenu : Comme on sait qu'il est beaucoup plus facile pour des espions chinois de résider en Amérique, que ce soit au Canada ou aux États-Unis, et qu'il est beaucoup plus difficile pour nous d'aller en Chine pour espionner ce système communiste qui exerce un contrôle omniprésent sur ses citoyens, quelle stratégie faut-il adopter par rapport à ces menaces que sont la Chine ou la Russie, mais surtout la Chine?

[*Traduction*]

M. Valeriano : Oui. Je pense que c'est un défi réaliste à l'heure actuelle. Je sais que nous ne sommes pas très bons pour ce qui est du travail et des perceptions des adversaires et que nous nous inquiétons beaucoup de ce qu'ils attaquent, mais pas tellement de ce qu'ils développent et de la façon dont les choses se font dans leur propre État. Je pense que c'est un angle mort. C'est une faiblesse. Nous pensons beaucoup au cyberrenseignement, mais pas pour comprendre le comportement de l'opposition. Je pense que l'aspect comportemental de la cybersécurité est l'un des défis majeurs que nous ayons à l'heure actuelle et que beaucoup de gens, surtout des universitaires, n'arrivent pas à relever.

Senator Yussuff: The public attitude towards cybersecurity is evolving. It's not new, but it is evolving in the sense of how people may view the seriousness of it. From my perspective, I think we have a long way to go. You made the point earlier about the sharing of information. If you don't know, you don't know. You can't really get the public to be incensed or angry about something that is going on if they don't know what's going on. Given most of the things that are happening in terms of the cyberattacks are also happening with private companies, some of it they share when our data is exposed, but if our data is not exposed, they don't tell us about it; there is that reality.

In the context, Mr. Valeriano, of the U.S. and the legislation that was passed about trying to collect this information and share it, how valuable do you think that would be in terms of changing public attitudes so governments and our elected people can become more ambitious in their effort to do more around cybersecurity and get the nation's efforts to be more robust in the same vein?

Mr. Valeriano: I think it would be critically important. We have a lot of folk sayings in cybersecurity, and the most pervasive is that if you haven't been hacked, you're about to be hacked. There is no evidence for that. There is no evidence for most of the statistics we have in cybersecurity. There is no real evidentiary basis for a lot of things that are said in cybersecurity.

Recently, the U.S. government said they want to develop some sort of colour-coded warning system for cyberattacks, much like we did during the Department of Homeland Security and terrorism era after 9/11. I'm not so sure that was effective. But in developing more actionable ways of demonstrating to the public that we have a problem, that there is a seismic shift and thinking about how we develop earthquake warnings in the United States, I think that that is something very important. Israel moved to a hotline system. Now, you're not going to get a lot of actionable data from a hotline system and by ordinary citizens reporting cyberattacks, but you will start to see patterns. We will start to see waves. I believe we haven't even begun to explore what we can do with data and notifying and engaging the public moving into the future.

Mr. Hodgson: One of the things that we're challenged by is that even when cyberattacks are reported, it doesn't seem to materially impact most people. When your identity is stolen and you have to go through the painful process of resurrecting your identity, to close accounts and reopen them, that's pretty powerful, but that's an individual level. Dr. Valeriano mentioned a couple of incidents. It's unclear, despite millions of records

Le sénateur Yussuff : L'attitude du public à l'égard de la cybersécurité évolue. Ce n'est pas nouveau, mais les gens s'aperçoivent de plus en plus de la gravité de la situation. À mon avis, nous avons encore beaucoup de chemin à faire. Vous avez parlé tout à l'heure de l'échange de renseignements. On ne peut pas savoir ce que l'on ne sait pas. On ne peut pas vraiment amener le public à se sentir outré ou en colère à l'égard de quelque chose qui se passe à son insu. Étant donné que la plupart des cyberattaques se produisent également au sein des entreprises privées, certaines d'entre elles nous le disent quand nos données sont compromises, mais si elles ne le sont pas, elles ne nous en parlent pas; c'est la réalité.

Dans le contexte, monsieur Valeriano, des États-Unis et de la loi qui a été adoptée pour essayer de recueillir ces renseignements et de les communiquer, dans quelle mesure cela servira-t-il selon vous à changer les attitudes du public afin que les gouvernements et nos représentants élus puissent redoubler leurs efforts en matière de cybersécurité et, par la même occasion, faire en sorte que les efforts du reste du pays soient plus robustes eux aussi?

M. Valeriano : Je pense que ce serait extrêmement important. Nous avons beaucoup d'expressions populaires sur la cybersécurité, et la plus répandue est que si vous n'avez pas été piraté, vous êtes sur le point de l'être. Rien ne le prouve. Il n'y a aucune preuve pour la plupart des statistiques dont nous disposons en matière de cybersécurité. Il n'y a pas le moindre fondement probant pour beaucoup de choses qui sont dites dans le domaine de la cybersécurité.

Récemment, le gouvernement des États-Unis a dit qu'il voulait mettre au point une sorte de système d'avertissement codé par couleur pour les cyberattaques, un peu comme nous l'avons fait à l'époque du département de la Sécurité intérieure et de l'ère du terrorisme qui a débuté le 11 septembre. Je ne suis pas sûr que cela ait été efficace. Mais en élaborant des façons plus concrètes de démontrer au public que nous avons un problème, qu'il y a un bouleversement sismique, et en réfléchissant aux avertisseurs de tremblement de terre que nous avons aux États-Unis, je pense que c'est quelque chose de très important. Israël est passé à un système de ligne directe. On n'obtiendra pas beaucoup de données exploitables d'un service d'assistance téléphonique et de citoyens ordinaires qui signalent des cyberattaques, mais on commencera à déceler des tendances. On commencera à voir des vagues. Je crois que nous n'avons même pas encore commencé à explorer ce que nous pouvons faire avec les données et à renseigner et mobiliser le public pour l'avenir.

M. Hodgson : Un des aspects qui nous posent problème, c'est que même lorsque des cyberattaques sont signalées, cela ne semble pas avoir d'incidence importante sur la plupart des gens. Lorsque votre identité est volée et que vous devez passer par le processus pénible de ressusciter votre identité, fermer des comptes et les rouvrir, c'est assez puissant, mais c'est ressenti au niveau individuel. M. Valeriano a mentionné quelques incidents.

having been impacted, what the real consequences of those cyberattacks have been. More recently, when you see ransomware, such as was executed against Colonial Pipeline, and what the result of that was, that has raised more awareness. Again, when you're not personally affected by it, it's very hard to motivate people to deal with it. Quite frankly, it can be extremely esoteric and technical for most people to understand what they should do.

I see you have a phone on your desk. How many people really understand exactly how that phone works? They don't, but they know how to use it. When they are told about the security vulnerabilities in it, I think for 99.44% of people, it really doesn't mean anything.

[*Translation*]

The Deputy Chair: Before we finish, I have a question for Mr. Rapin which I also asked the other witnesses earlier.

In fighting cybercriminals, are we condemned to always being on the defensive or can we hope one day to arrest and charge the cybercriminals?

Mr. Rapin: First, I am not sure it is true that Canada is only on the defensive since, if memory serves me, in late 2021, the Communications Security Establishment said it was conducting an offensive operation against a cybercriminal group. That is the first time we heard of such an event in Canada. So Canada is also taking proactive measures.

In terms of legal action, that is something the United States is doing increasingly. We are seeing more and more extremely public charges by the FBI, sometimes with photos of the persons identified or wanted. In late 2022, the U.S. convicted a first cybercriminal with links to Chinese intelligence who was arrested in Belgium, extradited to the U.S. and prosecuted. So we see that these things — This can work in one case but not in many others, but these efforts are sometimes successful. This is something Canada should consider doing more intensively, either of its own initiative or in cooperation with the United States to bring charges jointly. I think that is something that needs to be explored.

The Deputy Chair: That concludes our meeting. My sincere thanks to Mr. Valeriano, Mr. Rapin and Mr. Hodgson, and all of our witnesses today.

These discussions are extremely important and we appreciate your input. Thank you once again.

Même si des millions de dossiers ont été touchés, les conséquences réelles de ces cyberattaques ne sont pas claires. Plus récemment, lorsqu'on a constaté les résultats d'un rançongiciel comme celui qui a été lancé contre Colonial Pipeline, les gens se sont quelque peu sensibilisés. Cela dit, quand on n'est pas personnellement touché par le problème, il est très difficile de motiver les gens à s'y attaquer. Franchement, il peut être extrêmement ésotérique et technique pour la plupart des gens de comprendre ce qu'ils doivent faire.

Je vois que vous avez un téléphone sur votre bureau. Combien de personnes comprennent vraiment comment fonctionne ce téléphone? Ils ne le savent pas, mais ils savent comment l'utiliser. Lorsqu'on leur parle des vulnérabilités en matière de sécurité, je crois que ça ne veut rien dire pour 99,44 % des gens.

[*Français*]

Le vice-président : Avant de conclure la réunion, j'aurais une question pour M. Rapin que j'ai posée précédemment aux autres témoins.

Dans cette lutte aux cybercriminels, sommes-nous condamnés à être toujours sur la défensive, ou pouvons-nous espérer un jour faire des arrestations et mettre des cybercriminels en accusation?

M. Rapin : Premièrement, je ne sais pas à quel point on peut dire que le Canada est uniquement sur la défensive dans la mesure où, si ma mémoire est bonne, à la fin de 2021, le Centre de la sécurité des télécommunications a dit qu'il avait mené une opération offensive contre un groupe cybercriminel. C'est la première fois qu'on avait connaissance d'un tel événement au Canada. Il y a donc des actions proactives de la part du Canada.

Sur l'aspect judiciaire, c'est quelque chose que les États-Unis font de plus en plus. On voit de plus en plus d'inculpations extrêmement publiques de la part du FBI, avec parfois les photos des personnes identifiées et recherchées. À la fin de 2022, la justice américaine a condamné pour la première fois un pirate informatique lié au renseignement chinois qu'ils ont réussi à faire arrêter en Belgique, à extrader aux États-Unis et à traduire en justice. On voit donc que ce sont des choses qui... Cela peut fonctionner dans un cas par rapport à plusieurs autres, mais on voit que ces démarches peuvent parfois aboutir. C'est quelque chose que le Canada devrait envisager de faire un peu plus intensément, soit de sa propre initiative, soit en collaborant avec les États-Unis pour faire des inculpations conjointes. Je pense que ce sont des pistes qu'il faut explorer.

Le vice-président : Cela nous amène à la fin de notre réunion. Je tiens à remercier sincèrement MM. Valeriano, Rapin et Hodgson, ainsi que tous nos témoins aujourd'hui.

Ces discussions sont extrêmement importantes et nous vous sommes reconnaissants d'y avoir participé. Je vous remercie encore une fois.

Our next meeting will be next Monday, March 27, at the usual time of 4 p.m. (Eastern Time). Thank you and have a lovely evening.

(The meeting adjourned.)

Notre prochaine réunion aura lieu lundi prochain, le 27 mars, à l'heure habituelle, soit 16 heures (heure de l'Est). Je vous remercie et je vous souhaite une excellente soirée.

(La séance est levée.)