EVIDENCE

OTTAWA, Thursday, June 19, 2025

The Standing Senate Committee on National Finance met this day at 1:01 p.m. [ET] to study the Main Estimates for the fiscal year ending March 31, 2026, with the exception of Library of Parliament Vote 1 and to study the Supplementary Estimates (A) for the fiscal year ending March 31, 2026; and in camera for consideration of a draft report.

Senator Claude Carignan (*Chair*) in the chair.

[*Translation*]

The Chair: Honourable senators, good afternoon and welcome. Before we begin, I would like to ask all senators and other in-person participants to consult the cards on the table for guidelines to prevent audio feedback incidents.

Please make sure to keep your earpiece away from all microphones at all times.

Do not touch the microphone. It will be turned on and off by the console operator. Please avoid handling your earpiece while your microphone is on; you may either keep it on your ear or place it on the designated sticker. Thank you all for your cooperation.

[*English*]

I wish to welcome all senators as well as viewers across the country who are watching us on sencanada.ca. My name is Claude Carignan, a senator from Quebec. I am chair of this committee.

I now wish to ask my colleagues to introduce themselves.

[*Translation*]

Senator Forest: Welcome. Éric Forest from the Gulf division in Quebec.

[*English*]

Senator Pupatello: Hi. I'm Sandra Pupatello, an Ontario senator from Windsor.

[*Translation*]

Senator Galvez: Good afternoon. Rosa Galvez from Quebec.

TÉMOIGNAGES

OTTAWA, le jeudi 19 juin 2025

Le Comité sénatorial permanent des finances nationales se réunit aujourd'hui, à 13 h 1 (HE), pour étudier le Budget principal des dépenses pour l'exercice se terminant le 31 mars 2026, à l'exception du crédit 1 de la Bibliothèque du Parlement et pour étudier le Budget supplémentaire des dépenses (A) pour l'exercice se terminant le 31 mars 2026; et à huis clos, pour étudier une ébauche de rapport.

Le sénateur Claude Carignan (*président*) occupe le fauteuil.

[*Français*]

Le président : Honorables sénateurs et sénatrices, bonjour et bienvenue. Avant de commencer, je voudrais demander à tous les sénateurs et aux autres participants qui sont ici en personne de consulter les cartes sur la table pour connaître les lignes directrices visant à prévenir les incidents liés au retour de son.

Veuillez tenir votre oreillette éloignée de tous les microphones à tout moment.

Veuillez ne pas toucher au microphone. Il sera activé et désactivé par l'opérateur de console. Évitez de manipuler votre oreillette lorsque votre microphone est ouvert; vous pouvez la garder à l'oreille ou la déposer sur l'autocollant prévu à cet effet. Merci à tous de votre coopération.

[*Traduction*]

Je tiens à souhaiter la bienvenue à tous les sénateurs, ainsi qu'aux téléspectateurs de tout le pays qui nous regardent sur sencanada.ca. Je m'appelle Claude Carignan. Je suis un sénateur du Québec et je préside le comité.

J'invite maintenant mes collègues à se présenter.

[*Français*]

Le sénateur Forest : Bienvenue. Éric Forest, division du Golfe, au Québec.

[*Traduction*]

La sénatrice Pupatello : Bonjour. Je suis la sénatrice Sandra Pupatello, de Windsor, en Ontario.

[*Français*]

La sénatrice Galvez : Bon après-midi. Rosa Galvez, du Québec.

[*English*]

Senator Pate: Welcome. I live here on the unceded, unsurrendered and unreturned territory of the Algonquin Anishinaabeg.

[*Translation*]

Senator Gignac: Good afternoon. Clément Gignac from Quebec.

[*English*]

Senator MacAdam: Jane MacAdam, Prince Edward Island.

Senator Kingston: Joan Kingston, New Brunswick.

[*Translation*]

Senator Moreau: Pierre Moreau, Laurentides division, Quebec.

[*English*]

Senator Marshall: Elizabeth Marshall, Newfoundland and Labrador.

[*Translation*]

Senator Dalphond: Pierre Dalphond from Quebec.

The Chair: Honourable senators, today we will resume our study on the Main Estimates for the fiscal year ending March 31, 2026, and the Supplementary Estimates (A), 2025-26, which were referred to this committee on May 29, 2025, and June 11, 2025, respectively, by the Senate of Canada.

We are pleased to have with us witnesses from the Communications Security Establisment Canada. I imagine that many people will be listening to us today.

I would like to introduce Caroline Xavier, Chief; Julie Chassé, Chief Financial Officer; and Samantha McDonald, Assistant Deputy Minister of Strategic Policy, Planning and Partnerships.

Welcome and thank you for accepting our invitation to appear today. We will now hear opening remarks from Ms. Xavier. Ms. Xavier, the floor is yours.

Caroline Xavier, Chief, Communications Security Establishment Centre: Good afternoon, Mr. Chair and members of the committee. Thank you for the invitation to appear today to discuss the 2025-26 Main Estimates and Supplementary Estimates (A) 2025-26 on behalf of the

[*Traduction*]

La sénatrice Pate : Bienvenue. Je vis ici sur le territoire non cédé, non abandonné et non restitué du peuple algonquin anishinabe.

[*Français*]

Le sénateur Gignac : Bonjour. Clément Gignac, du Québec.

[*Traduction*]

La sénatrice MacAdam : Jane MacAdam, de l'Île-du-Prince-Édouard.

La sénatrice Kingston : Joan Kingston, du Nouveau-Brunswick.

[*Français*]

Le sénateur Moreau : Pierre Moreau, division des Laurentides, au Québec.

[*Traduction*]

La sénatrice Marshall : Elizabeth Marshall, de Terre-Neuve-et-Labrador.

[*Français*]

Le sénateur Dalphond : Pierre Dalphond, du Québec.

Le président : Honorables sénateurs et sénatrices, aujourd'hui nous continuons notre étude du Budget principal des dépenses pour l'exercice se terminant le 31 mars 2026 et du Budget supplémentaire des dépenses (A) de 2025-2026, qui ont été renvoyés à ce comité le 29 mai 2025 et le 11 juin 2025 respectivement par le Sénat du Canada.

Nous sommes heureux d'accueillir parmi nous des témoins du Centre de la sécurité des télécommunications Canada. J'imagine que beaucoup de monde nous écoutera aujourd'hui.

Je vous présente Mme Caroline Xavier, chef, Mme Julie Chassé, dirigeante principale des finances, et Mme Samantha McDonald, sous-ministre adjointe, Politiques stratégiques, planification et partenariats.

Bienvenue et merci d'avoir accepté notre invitation à comparaître aujourd'hui. Nous allons maintenant entendre les déclarations préliminaires de Mme Xavier. Madame Xavier, vous avez la parole.

Caroline Xavier, chef, Centre de la sécurité des télécommunications Canada : Bon après-midi, monsieur le président et mesdames et messieurs les membres du comité. Je vous remercie de nous avoir invitées à comparaître aujourd'hui pour discuter du Budget principal des dépenses et du Budget

Communications Security Establishment Canada, also known as CSE.

[*English*]

Today, I am joined by my colleagues, Samantha McDonald, Assistant Deputy Minister for Strategic Policy, Planning and Partnerships; as well as Julie Chassé, Chief Financial Officer.

Before we begin, I wish to acknowledge we are on the traditional unceded territory of the Algonquin Anishinaabe Nation. We acknowledge that this nation has been on this land since time immemorial. We recognize the important history of their stewardship of this land and understand their contributions to its present and future well-being.

For committee members less familiar with our agency, CSE is an important part of Canada's security and defence ecosystem. As a stand-alone agency, we report directly to the Minister of National Defence. Our role is to collect and report on foreign signals intelligence; provide cyber security, information assurance and secure communications for the Government of Canada; as well as provide cyber guidance and services to help protect systems of importance to the Government of Canada.

We disrupt foreign cyber operations and threats, and take action in cyberspace to defend systems of importance to the Government of Canada and to support Canadian international affairs, defence and security. We provide technical and operational assistance to federal law enforcement and security agencies, including to the Department of National Defence and the Canadian Armed Forces. We also lead the Canadian Centre for Cyber Security, the Cyber Centre, which offers cybersecurity advice to external stakeholders and the public. It is also the national lead and technical authority on cybersecurity.

[*Translation*]

CSE is a proud and valuable member of the Five Eyes, the world's longest-standing and closest intelligence-sharing alliance. The Five Eyes is a key element in Canada's intelligence and security landscape — a force multiplier for CSE and Canada — providing a forum to share intelligence, technology and insights to hone our understanding of threats, risk and adversaries, and strengthen our collective defences, helping to protect Canada's security and prosperity.

supplémentaire des dépenses (A) de 2025-2026 au nom du Centre de la sécurité des télécommunications Canada, aussi appelé le CST.

[*Traduction*]

Aujourd'hui, je suis accompagnée de ma collègue Samantha McDonald, sous-ministre adjointe responsable des Politiques, de la planification et des partenariats stratégiques, ainsi que Julie Chassé, notre dirigeante principale des finances.

Avant de commencer, je tiens à reconnaître que nous nous trouvons sur le territoire traditionnel non cédé du peuple algonquin anishinabe. Nous reconnaissons que cette nation vit sur ce territoire depuis des temps immémoriaux. Nous reconnaissons l'importance historique de leur intendance de ce territoire et sommes conscients de leurs contributions à son bien-être actuel et futur.

Pour les membres du comité qui connaissent un peu moins notre organisme, le CST est un élément important de l'écosystème de sécurité et de défense du Canada. En tant qu'organisme autonome, nous relevons directement du ministre de la Défense nationale. Notre rôle consiste à recueillir du renseignement électromagnétique étranger et produire des rapports connexes; assurer la cybersécurité, l'assurance de l'information et des communications sécurisées au gouvernement du Canada; offrir des conseils et des services en matière de cybersécurité pour aider à protéger les systèmes importants pour le gouvernement du Canada.

Notre rôle consiste également à contrer les cybermenaces étrangères et prendre des mesures dans le cyberespace pour défendre les systèmes d'importance pour le gouvernement du Canada et pour appuyer les affaires internationales, la défense et la sécurité du Canada; fournir de l'assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, y compris le ministère de la Défense nationale et les Forces armées canadiennes; diriger le Centre canadien pour la cybersécurité, qui offre des conseils en matière de cybersécurité aux parties prenantes externes et au public. Le CST est aussi le chef de file national et l'autorité technique en matière de cybersécurité.

[*Français*]

Le CST est un membre fier et estimé du Groupe des cinq, l'alliance d'échange de renseignements la plus ancienne et la plus étroite du monde. Le Groupe des cinq est un élément clé dans le domaine du renseignement et de la sécurité au Canada. Cette alliance décuple les forces du CST et du Canada en rendant possibles les échanges de renseignements, de technologies et de connaissances afin de mieux comprendre les menaces, les risques et nos adversaires, et de renforcer nos défenses collectives. Elle contribue ainsi à protéger la sécurité et la prospérité du Canada.

[*English*]

CSE's information advantage gained through our activities to support our mandate and our partnerships, provides Canada with a comprehensive understanding of the threat landscape. As a national security and intelligence organization, you can understand that we cannot publicly disclose all our information and intelligence. However, we use publications, such as our unclassified National Cyber Threat Assessment report, to share threat information to help raise Canada's cybersecurity bar so Canadians can live and work online safely and with confidence.

[*Translation*]

Canada is confronting an expanding and complex cyber threat landscape with a growing cast of malicious and unpredictable state and non-state cyber threat actors, from cybercriminals to hacktivists, that are targeting our critical infrastructure and endangering our national security. These cyber threat actors are evolving their tradecraft, adopting new technologies, and collaborating in an attempt to improve and amplify their malicious activities.

[*English*]

Canada's state adversaries are becoming more aggressive in cyberspace. State-sponsored cyber operations against Canada and our allies almost certainly extend beyond espionage. State-sponsored cyber-threat actors are almost certainly attempting to cause disruptive effects, such as denying service, deleting or leaking data and manipulating industrial control systems to support military objectives and/or information campaigns. We assess that our adversaries very likely consider civilian critical infrastructure to be a legitimate target for cyber sabotage in the event of a military conflict.

[*Translation*]

At the same time, cybercrime remains a persistent, widespread, and disruptive threat to individuals, organizations and all levels of government across Canada that is sustained by a thriving and resilient global cybercrime ecosystem.

[*English*]

In this year's Main Estimates, CSE sought a total of $1.22 billion. In addition, through the Supplementary Estimates (A), CSE sought $370.1 million for a total of $1.59 billion, all of which contribute toward reaching the 2% of GDP in defence expenditures this year.

[*Traduction*]

L'avantage du CST sur le plan de l'information, acquis dans le cadre de nos activités visant à appuyer notre mandat et nos partenariats, procure au Canada une compréhension globale du contexte des menaces. À titre d'organisme de sécurité nationale et de renseignement, vous pouvez comprendre que nous ne pouvons pas communiquer publiquement toute l'information et tout le renseignement que nous traitons. Cependant, nous utilisons des publications comme notre évaluation des cybermenaces nationales non classifiée pour présenter de l'information sur les menaces et ainsi aider à relever le niveau de la cybersécurité au Canada afin que la population canadienne puisse vivre et travailler en ligne en toute confiance et sécurité.

[*Français*]

Le Canada affronte un environnement de cybermenaces complexes et en pleine expansion comptant un éventail croissant d'auteurs de cybermenaces étatiques et non étatiques malveillants et imprévisibles, comme les cybercriminels et les activistes, qui ciblent ses infrastructures essentielles et compromettent sa sécurité nationale. Ces auteurs de cybermenaces développent leur métier, adoptent de nouvelles technologies et collaborent dans le but d'améliorer et d'intensifier leurs activités malveillantes.

[*Traduction*]

Les États adversaires du Canada deviennent plus agressifs dans le cyberespace. Les cyberopérations parrainées par des États visant le Canada et ses alliés ne se limitent certainement pas à l'espionnage. Les auteurs de cybermenace parrainés par des États tentent sans doute d'être perturbateurs, par exemple, en rendant un service inaccessible, en supprimant ou en divulguant des données et en manipulant des systèmes de contrôle industriels, afin de favoriser la réalisation d'objectifs militaires ou de campagnes d'information. Nous estimons que nos adversaires considèrent très probablement les infrastructures civiles essentielles comme une cible légitime de cybersabotage advenant un conflit militaire.

[*Français*]

Parallèlement, la cybercriminalité constitue toujours pour les particuliers, les organisations et tous les ordres de gouvernement au Canada une menace généralisée et perturbatrice appuyée par un écosystème mondial de cybercriminalité, prospère et résilient.

[*Traduction*]

Dans le Budget principal des dépenses de cette année, le CST a demandé un montant total de 1,22 milliard de dollars. En outre, dans le Budget supplémentaire des dépenses (A), le CST a cherché à obtenir 370,1 millions de dollars, pour un total de 1,59 milliard de dollars, qui font partie des investissements en

The Main Estimates include allocating $21 million to enhance foreign intelligence coverage of transnational organized crime and illegal drug supply chains, including combating fentanyl.

This funding was allocated to CSE to bolster the capacity to provide actionable intelligence to federal partners on foreign transnational criminal actors involved in the trafficking of fentanyl, other illicit drugs and their precursors to North America. This funding will also be used to bolster the cyberoperations aspect of its mandate to disrupt these illicit supply chains.

[*Translation*]

As announced last week by the Prime Minister, Canada will meet the NATO spending for investing 2% of GDP on defence this year. You will have heard from our colleagues at National Defence earlier this week that the Supplementary Estimates will provide both DND and CSE with investments for enhanced tools, capabilities and digital foundations, to support operations and help protect Government of Canada systems including our most top secret networks against the cyber threats I outlined earlier.

[*English*]

In support of defence, security and diplomatic goals, the $370.1 million sought through Supplementary Estimates (A) for CSE will strengthen and modernize our equipment and technology.

To continue toward a secure and sovereign Canada, investments in these digital foundations will expand our capabilities to keep Canada's most sensitive information, communications and operations protected, communicate securely with our allies and enable emerging capabilities such as artificial intelligence to be used in real time to support decision makers at the most classified level.

These investments will further allow us to expand our capabilities toward timely access to sensitive, mission-critical information, maximizing technological advancements that we know are being used by our adversaries. They will also increase the diversification of technology and equipment used by the Five Eyes, helping to build both the interoperability and resilience among allies.

défense du Canada et contribuent à l'atteinte de l'objectif de 2 % du PIB cette année.

Le Budget principal des dépenses comprend une affectation de 21 millions de dollars pour augmenter la couverture du renseignement étranger concernant le crime organisé transnational et les chaînes d'approvisionnement en drogues illégales, notamment la lutte contre le fentanyl.

Ces fonds ont été affectés au CST afin de renforcer sa capacité de fournir du renseignement exploitable aux partenaires fédéraux sur les auteurs étrangers de crime transnational participant au trafic de fentanyl, d'autres drogues illicites et de drogues précurseurs en Amérique du Nord. Ces fonds serviront également à renforcer le volet du mandat du CST touchant les cyberopérations dans le but de perturber ces chaînes d'approvisionnement en drogues illicites.

[*Français*]

Conformément à l'annonce du premier ministre la semaine dernière, le Canada atteindra cette année l'objectif fixé par l'OTAN de 2 % du PIB pour les dépenses en matière de défense. Plus tôt cette semaine, vous avez sans doute entendu de la part de nos collègues de la Défense nationale que le Budget supplémentaire des dépenses fournira au ministère de la Défense et au CST des investissements permettant d'améliorer leurs outils, leurs capacités et leurs fondations numériques, dans le but de soutenir les opérations et d'aider à protéger les systèmes du gouvernement du Canada, y compris nos réseaux les plus secrets, contre les cybermenaces que j'ai mentionnées plus tôt.

[*Traduction*]

Afin d'appuyer les objectifs en matière de défense, de sécurité et de diplomatie, les fonds de 370,1 millions de dollars demandés dans le Budget supplémentaire des dépenses (A) pour le CST serviront à renforcer et moderniser nos équipements et nos technologies.

Les investissements dans ces fondations numériques, qui visent à assurer la sécurité et la souveraineté du Canada, permettront d'étendre nos capacités afin d'assurer la protection continue des informations, communications et activités les plus sensibles du Canada, de communiquer en toute sécurité avec nos alliés, d'ouvrir la voie à des capacités émergentes, comme l'intelligence artificielle, et de les utiliser en temps réel pour appuyer les décideurs au niveau le plus classifié.

Ces investissements nous permettront d'accroître nos capacités et d'avoir accès en temps opportun à l'information sensible essentielle à la réalisation de notre mission, pour ainsi maximiser les avancées technologiques dont nos adversaires se servent, comme nous le savons. Ils permettront aussi d'augmenter la diversification des technologies et équipements utilisés par le Groupe des cinq, ce qui aidera à accroître la résilience et l'interopérabilité entre les alliés.

[*Translation*]

In conclusion, CSE continues to deliver its important mandate and investments detailed in these Estimates represent Canada's commitment towards a hardened and modernized Top Secret ecosystem, in support of Canada's defence security, diplomatic and economic goals.

[*English*]

The funding we are requesting through these Main Estimates is critical to the integral role that CSE and the Cyber Centre play in helping to protect Canada and Canadians against foreign threats, helping to ensure our nation's security, stability and prosperity now and into the future.

[*Translation*]

Once again, thank you for the invitation to appear before the committee today and my colleagues and I look forward to answering any questions you may have.

The Chair: We will begin the question period with Senator Marshall.

[*English*]

Senator Marshall: Thank you for being here today. I am especially interested in your request for the $370 million in Supplementary Estimates (A). Could you tell us what the money is for? I have read some media articles, and I understand that there has been a contractor selected for artificial intelligence, a systems firm, I imagine. Could you tell us about the contract with regard to how they were selected, how the price was obtained and whether it's a stand-alone contract or a multiyear contract? Will you give us background information there?

Ms. Xavier: Thank you, Mr. Chair, for the question.

As was stated, $370.1 million is being provided to us for this fiscal year with the intent to strengthen and modernize our equipment and technology.

In doing so, as you mentioned, an aspect of that will be linked to artificial intelligence but no contracts have been specifically signed related to this $370.1 million. The intent is that we will be able to, as I said, invest in a digital backbone that allows us to be able to ensure we are modernizing the one that already exists and leveraging, for the most part, existing standing offers.

[*Français*]

En conclusion, le CST continue de mener à bien son mandat très important, et les investissements détaillés dans ces budgets mettent en lumière l'engagement du Canada à l'égard d'un écosystème de niveau très secret renforcé et modernisé pour appuyer les objectifs en matière de défense, de sécurité, de diplomatie et d'économie.

[*Traduction*]

Le financement que nous cherchons à obtenir par l'intermédiaire du Budget principal des dépenses est essentiel au rôle vital que jouent le CST et le Centre pour la cybersécurité dans la protection du Canada et de la population canadienne contre les menaces étrangères, et dans les efforts visant à assurer la sécurité, la stabilité et la prospérité de notre pays, maintenant et à l'avenir.

[*Français*]

Encore une fois, je vous remercie de nous avoir donné l'occasion de témoigner devant le comité aujourd'hui. Mes collègues et moi serons heureuses de répondre maintenant à vos questions.

Le président : Nous allons commencer la période des questions avec la sénatrice Marshall.

[*Traduction*]

La sénatrice Marshall : Je vous remercie de votre présence aujourd'hui. Je m'intéresse en particulier aux 370 millions de dollars que vous demandez dans le Budget supplémentaire des dépenses (A). Pourriez-vous nous dire à quoi serviront ces fonds? J'ai lu divers articles dans les médias, et je crois comprendre qu'une entreprise a été choisie pour l'intelligence artificielle, une entreprise de systèmes, j'imagine. Pourriez-vous parler de ce contrat? Quel était le processus de sélection? Comment le montant a-t-il été établi? Est-ce un contrat autonome ou un contrat pluriannuel? Pouvez-vous nous donner des renseignements généraux à ce sujet?

Mme Xavier : Monsieur le président, je vous remercie de la question.

Comme nous l'avons indiqué, les 370,1 millions de dollars nous sont fournis pour l'exercice en cours et visent à renforcer et moderniser nos équipements et nos technologies.

Comme vous l'avez mentionné, ce sera en partie lié à l'intelligence artificielle, mais aucun contrat précis lié à ce montant de 370,1 millions de dollars n'a été signé. Comme je l'ai dit, l'objectif est d'investir dans une fondation numérique de façon à moderniser ce qui existe déjà et de tirer parti, surtout, des capacités existantes.

Senator Marshall: Is there no contract with a supplier? You are saying that the $370 million is sitting there. Have you designated what it is to be used for? The impression I had from reading the media is that there has been a contract with an AI firm.

Ms. Xavier: There are contracts that might be let, including with artificial intelligence firms. In particular, this funding will be used for several contracts not just with one artificial intelligent firm. It's important to note the majority of the funding allocated for CSE's use is within existing contracts, not only to sign with an artificial intelligence firm but also to do more in our top secret classified space, which is a space we already run for the Government of Canada.

We're expanding that and including the diversification of technology and equipment used in terms of being able to increase our interoperability domestically and internationally.

Senator Marshall: Is the $370 million going to one supplier, or is it broken down with regard to what it is going to be used for?

The sum of $370 million is a lot of money. Is there an itemized list of what the money is going to be used for, or is it a global amount?

Ms. Xavier: I will ask Samantha McDonald to add a few more details. Before I hand it over to Ms. McDonald, I will say that because we are an organization of national security, we do not itemize how we will spend the funds we receive in detail in public for reasons of national security.

Senator Marshall: I see.

Ms. Xavier: It will be a little difficult to give you the breakdown that you would —

Senator Marshall: But the numbers still —

Ms. Xavier: Correct. Ms. McDonald, is there anything you would like to add?

Samantha McDonald, Assistant Deputy Minister, Strategic Policy, Planning and Partnerships, Communications Security Establishment Canada: Maybe I can break down some of the pieces, but it will be at a high level.

Senator Marshall: It will be general, yes.

La sénatrice Marshall : N'y a-t-il pas un contrat avec un fournisseur? Vous dites que les 370 millions de dollars ne demandent qu'à être utilisés. Avez-vous déterminé à quoi serviront ces fonds? Ce que j'ai lu dans les médias me donnait l'impression qu'un contrat a été accordé à une entreprise du domaine de l'intelligence artificielle.

Mme Xavier : Des contrats pourraient être accordés, notamment avec des entreprises du domaine de l'intelligence artificielle. Plus particulièrement, ce financement servira pour divers contrats, pas seulement pour une seule entreprise d'intelligence artificielle. Il importe de souligner que la majorité des fonds alloués au CST sont liés à des contrats existants. Il ne s'agit pas seulement de signer un contrat avec une entreprise d'IA, mais aussi d'en faire plus dans notre écosystème de niveau secret, un espace que nous avons déjà dirigé pour le gouvernement du Canada.

Nous élargissons ces activités, et cela comprend la diversification des technologies et de l'équipement utilisé, de façon à accroître notre interopérabilité, au pays et à l'étranger.

La sénatrice Marshall : Les 370 millions de dollars vont-ils à un fournisseur unique, ou serviront-ils à diverses fins?

Trois cent soixante-dix millions de dollars, c'est une somme considérable. Avez-vous une ventilation détaillée de l'utilisation des fonds, ou seulement un montant global?

Mme Xavier : Je demanderais à Samantha McDonald de vous donner plus de détails, mais avant de lui céder la parole, permettez-moi de préciser qu'étant donné que nous sommes un organisme de sécurité nationale, nous ne pouvons pas, pour des raisons de sécurité nationale, divulguer publiquement des détails sur l'utilisation des fonds que nous recevons.

La sénatrice Marshall : Je vois.

Mme Xavier : Il sera plutôt difficile de vous donner la ventilation que vous aimeriez...

La sénatrice Marshall : Toutefois, les chiffres sont quand même...

Mme Xavier : C'est exact. Madame McDonald, aimeriez-vous ajouter quelque chose?

Samantha McDonald, sous-ministre adjointe, Politiques stratégiques, planification et partenariats, Centre de la sécurité des télécommunications Canada : Je pourrais peut-être donner une ventilation pour certains éléments, mais ce sera de manière très générale.

La sénatrice Marshall : Oui, exactement.

Ms. McDonald: As the chief has mentioned, some of the digital infrastructure that we use both in our organization and to interact with our colleagues at a top secret level across the Government of Canada requires us to always be looking at cybersecurity and the materials we use to do that in a protected and secure way.

Some of the funding will be used to continue to uplift that network in relation to the threats that we know and see as an organization and make sure that we are strengthening. As the chief has mentioned, some of that will be to ensure that network and our systems are ready to use.

Different types of emerging technologies are evolving. We know that AI has recently come online in a bigger way, and there are other technologies like that, so there may be contracts or different ways of doing that across the organization.

Then as the chief also mentioned, a part of our mandate is the information assurance part. This is the equipment we use both in Canada and across the Five Eyes, equipment and a process we use —

Senator Marshall: Is the $370 million for your organization alone, or are you linked up? You mentioned the Five Eyes. I know that Innovation, Science and Economic Development Canada is involved in artificial intelligence. Is this stand alone, or are you linked up with other governments or government departments? I just need a quick answer.

Ms. Xavier: We are linked up with other government departments. However, the $370.1 million is for Communications Security Establishment Canada's use.

Senator Marshall: Thank you.

[*Translation*]

Senator Forest: Thank you for being with us. We understand the very nature of your activities, so we will try to stick to more general facts.

Can you give us an overview of the evolution of CSE's workforce? Is it increasing or stable? Budgets are increasing now, but is there also an increase in staff?

Ms. Xavier, in an interview you gave, you confirmed that the shortage of cybersecurity experts is a widespread problem; in fact, the CBC article referred to it as a "personnel crisis." Has the situation improved since that interview?

Mme McDonald : Comme la cheffe l'a mentionné, certaines infrastructures numériques que nous utilisons à la fois dans l'organisation et pour communiquer avec nos collègues à un niveau très secret, dans l'ensemble du gouvernement du Canada, exigent une surveillance constante du point de vue de la cybersécurité et du matériel que nous utilisons pour mener nos activités de manière protégée et sécurisée.

Une partie du financement servira à l'amélioration continue de ce réseau pour contrer les menaces connues et observées par notre organisation, et à nous renforcer. Comme la cheffe l'a indiqué, une partie du travail sera de veiller à ce que ce réseau et nos systèmes soient prêts à utiliser.

Différents types de technologies émergentes évoluent. Nous savons que l'intelligence artificielle prend une place de plus en plus prépondérante, et il y a d'autres technologies semblables. Par conséquent, il pourrait y avoir des contrats ou diverses activités à cet égard au sein de l'organisation.

En outre, comme la cheffe l'a aussi mentionné, notre mandat comprend l'assurance de l'information. Il s'agit de l'équipement que nous utilisons tant au Canada qu'au sein du Groupe des cinq, l'équipement et un processus que nous utilisons...

La sénatrice Marshall : Les 370 millions de dollars sont-ils pour votre organisme seulement, ou avez-vous des liens quelconques? Vous avez parlé du Groupe des cinq. Je sais qu'Innovation, Sciences et Développement économique Canada a des activités liées au domaine de l'intelligence artificielle. Est-ce uniquement pour vous, ou avez-vous des liens avec d'autres gouvernements ou ministères du gouvernement? J'ai besoin d'une réponse rapide.

Mme Xavier : Nous avons des liens avec d'autres ministères. Cependant, les 370,1 millions de dollars sont réservés au Centre de la sécurité des télécommunications Canada.

La sénatrice Marshall : Je vous remercie.

[*Français*]

Le sénateur Forest : Merci de votre présence. On comprend la nature même de vos activités, donc on va essayer de rester dans des faits plus généraux.

Pouvez-vous nous donner un aperçu de l'évolution des effectifs du CST? Est-ce que l'effectif augmente ou est-il stable? Les budgets augmentent maintenant, mais est-ce que le personnel augmente?

Madame Xavier, dans une entrevue que vous avez accordée, vous avez confirmé que la pénurie d'experts en cybersécurité est un problème généralisé; d'ailleurs, l'article de Radio-Canada en parlait comme d'une « crise de personnel ». Est-ce que la situation s'est améliorée depuis cette entrevue?

Ms. Xavier: Thank you for the question. Yes, we have seen a significant increase in our workforce. I am happy to say that, over the past two years, we have hired more than 800 people. The agency now has over 3,800 employees. We have no difficulty attracting talent, and we are very proud of that. Our organization has an extraordinary mandate and, because of our mandate, there are things we can do that others outside our agency cannot. In general, we receive between 10,000 and 15,000 resumes per year from people expressing an interest in our organization.

I am also happy to say that our attrition is about 3% for the fiscal year. This figure is quite low compared to other institutions and agencies. We are also proud of the fact that we have been named employer of choice for 10 consecutive years in the National Capital Region and employer of choice for young professionals. I believe we are doing things right and can be proud of that.

Senator Forest: The problem is that you can't talk too much about it.

Ms. Xavier: If I may, I would add that we will be releasing our annual report next week, which will make as many details as possible public.

Senator Forest: Given the nature of your activities, one of the issues seems to be retention. Am I right?

Ms. Xavier: Of course, we never like to see people leave the agency. At the same time, it is good to have staff turnover, with people coming and going. As a technology agency, we like to stay at the forefront of new technologies. As I mentioned earlier, attrition for the agency is 3%, which is quite low, compared to 4% in the past. If we don't count people who leave the agency to retire, it's 2%. We are not doing badly. At the same time, we do experience staff losses, just like any other organization.

Senator Forest: According to Statistics Canada, losses attributable to cybercrime increased by 50% to $1.2 billion in 2023. We do not have the figures for 2024-25 yet. Can you explain your role with respect to other organizations, such as the RCMP, in the fight against cybercrime?

Ms. Xavier: As I said, the CSE is a technical leader and an authority on cybersecurity. That said, we cannot do everything on our own. We work very closely with colleagues in the security and intelligence community, including the RCMP. When it comes to cybersecurity, the RCMP focuses mainly on the criminal aspect and fraud. We focus on defence. We issue

Mme Xavier : Merci pour la question. En effet, nous avons vu une grosse augmentation des effectifs. Je suis contente de dire que, au-delà des deux dernières années, nous avons embauché plus de 800 personnes. L'agence compte maintenant plus de 3 800 employés. Nous n'avons aucune difficulté à attirer des talents et nous en sommes très fiers. Notre organisation a un mandat extraordinaire. Grâce à notre mandat, il y a des choses que nous pouvons faire que d'autres à l'extérieur de notre agence ne peuvent pas faire. En général, nous recevons entre 10 000 et 15 000 curriculum vitæ par année de la part de personnes qui expriment leur intérêt pour notre organisation.

Je suis contente aussi de dire que pour nous, l'attrition correspond à environ 3 % de l'année fiscale. Ce chiffre est plutôt bas en comparaison à d'autres institutions et agences. Nous sommes aussi fiers du fait que nous avons été nommés employeur par excellence pour une dixième année consécutive dans la région de la capitale nationale et employeur par excellence pour les jeunes professionnels. Je crois que nous faisons bien les choses et que nous pouvons en être fiers.

Le sénateur Forest : Le problème, c'est que vous ne pouvez pas trop en parler.

Mme Xavier : Si vous me le permettez, j'ajouterais que nous publierons la semaine prochaine notre rapport annuel, qui rendra publics le plus de détails possible.

Le sénateur Forest : Compte tenu de la nature de vos activités, un des enjeux semble être la rétention du personnel. Ai-je raison?

Mme Xavier : Bien sûr, on n'aime jamais voir les gens quitter l'agence. En même temps, il est bon d'avoir une rotation du personnel, avec les arrivées et les départs. Comme nous sommes une agence de technologie, nous aimons rester à l'avant-garde des nouvelles technologies. Comme je l'ai mentionné plus tôt, l'attrition pour l'agence représente 3 %, ce qui est plutôt bas, alors que le taux était de 4 % par le passé. Si on ne compte pas les personnes qui quittent l'agence pour prendre leur retraite, la proportion est de 2 %. On ne se débrouille pas mal. En même temps, nous subissons des pertes de personnel, comme toute autre organisation.

Le sénateur Forest : Selon Statistique Canada, les pertes attribuables à la cybercriminalité ont augmenté de 50 % pour atteindre 1,2 milliard de dollars en 2023. Nous n'avons pas encore les chiffres pour 2024-2025. Pouvez-vous nous expliquer votre rôle par rapport à d'autres organisations, par exemple la GRC, quant à la lutte contre la cybercriminalité?

Mme Xavier : Comme je le disais, le Centre de la sécurité des télécommunications est un chef de file du point de vue technique et qui a l'autorité au chapitre de la cybersécurité. Cela dit, nous ne pouvons pas tout faire seuls. Nous travaillons très étroitement avec des collègues de la communauté, de la sécurité et du renseignement, y compris la GRC. En matière de

notices, advice and alerts. We work to make Canada and its critical infrastructure more cyber resilient. In conjunction with other colleagues, we produce a number of domestic and international publications so that as many people as possible can see the advice we give. Our guidelines and mandates are very clear in terms of ensuring that everyone has the same starting point. The RCMP is a police force; we are not.

cybersécurité, la GRC se concentre surtout sur l'aspect criminel et sur la fraude. Nous nous concentrons sur la défense. Nous émettons des avis, des conseils et des alertes. Nous nous assurons d'améliorer la cyberrésilience du pays et des infrastructures essentielles. Avec d'autres collègues, nous produisons plusieurs publications d'ordre domestique et international pour permettre au plus grand nombre de personnes possible de voir les conseils que nous donnons. Nos lignes directrices et nos mandats sont très clairs pour ce qui est de faire en sorte que le point de départ soit le même pour tout le monde. La GRC est tout de même un service de police, alors que nous ne le sommes pas.

The Chair: If I may, I would like to comment on the same subject. If I understand correctly, when you talk about the attrition rate, you are talking about the number of people who leave the agency or the centre.

Le président : Si vous me le permettez, j'aimerais intervenir sur le même sujet. Si je comprends bien, lorsque vous parlez du taux d'attrition, vous parlez du taux de personnes qui quittent l'agence ou le centre.

Ms. Xavier: That is correct.

Mme Xavier : C'est exact.

The Chair: You say that the rate is 3%, including retirees and 2% otherwise. That rate is extremely low. Is it not too low? It will take 50 years before everyone leaves, but I would imagine that a career lasts 25 years. Since the CSE is in the technology sector, you want to have the best people in the field. It seems to me that the rate is too low.

Le président : Vous dites que le taux est de 3 %, y compris les personnes qui prennent leur retraite, et de 2 % pour les autres. Ce taux est extrêmement bas. N'est-il pas trop bas? Il faudra 50 ans avant que tout le monde parte. Or, j'imagine qu'une carrière dure 25 ans. Puisque le CST est dans le secteur technologique, vous souhaitez avoir les meilleurs en la matière. Il me semble que ce taux est trop bas.

Ms. Xavier: I understand the question and the thinking. That is why I say that it is not seen as a bad thing when someone leaves. The CSE even encourages development and encourages people to try something else and come back. It does that within the government and with the private sector. While the rate seems low, I do not want to give you the impression that the agency doesn't provide ongoing development and training, because we do, in cooperation with international partners and the private sector. We could not do what we do without them.

Mme Xavier : Je comprends bien la question et la réflexion. C'est pourquoi je dis qu'on ne le voit pas d'un mauvais œil quand une personne nous quitte. On encourage même le développement et on encourage les gens à essayer autre chose et à revenir. On le fait au sein du gouvernement et avec des entreprises privées. Bien que le taux semble bas, je ne veux pas vous donner l'impression qu'il n'y a pas de développement ou de formation constante qui se fait au sein de l'agence, en collaboration avec nos partenaires internationaux et le secteur privé. On ne pourrait pas faire ce qu'on fait sans être intégré avec eux.

The Chair: You understood my concerns well, even though I did not express them that clearly.

Le président : Vous avez bien compris mes inquiétudes, même si je ne les ai pas exprimées aussi clairement.

Ms. Xavier: It was a good question. Thank you.

Mme Xavier : C'était une bonne question, merci.

The Chair: I was concerned about the consequences of a low rate.

Le président : Je m'inquiétais des conséquences d'un taux aussi bas.

Senator Gignac: Welcome, witnesses. I looked through your annual report, and it's very informative. I understand that you can't go into too much detail for security reasons. I paused on one part in particular. Two years ago, some of my colleagues and I had the opportunity to visit the military and civilian infrastructure in the Canadian Arctic. We went to Inuvik, where there is a radar station that is unable to detect the missiles that Russia is using against Kyiv.

Le sénateur Gignac : Bienvenue aux témoins. J'ai parcouru votre rapport annuel. Je le trouve très intéressant. Je comprends qu'on ne peut pas aller trop en détail pour des raisons de sécurité. Je me suis arrêté sur un article en particulier. Avec certains de mes collègues, il y a deux ans, j'ai eu la chance de visiter les infrastructures militaires et civiles dans l'Arctique canadien. Nous sommes allés notamment à Inuvik, où il y a une station de radar qui est incapable de détecter les missiles que la Russie utilise contre Kiev.

Could you talk about that a bit more? You were involved in the decision to modernize the radar station. I think it is Australia that is going to help us do that work. What can you tell us about that? According to media reports, the cost of carrying out the modernization, or at least identifying threats, is estimated at $6 billion.

Ms. Xavier: Thank you for the question. I am not a radar expert. Our agency works very closely with our counterparts and colleagues in the Canadian Forces on radar-related matters. Our expertise is in ensuring that data captured by radar remain secure. We are experts in signals intelligence and data security. We make sure that the data are also available in real time to those who need them. We provide the digital foundations, not the radar itself. I would not want to give you details on a topic I am not an expert on.

Senator Gignac: You mentioned a cyberincident that happened in 2022. You even came to the conclusion that you had to provide the Northwest Territories with equipment. That is no longer about an agency or a federal department; that is about providing equipment at the provincial and territorial level. Could you talk a bit about your relationships with the provinces? What is true for one will be true for the others. It could be Quebec or any other province. What are your relationships, and how can you properly provide equipment to all regions in Canada and ensure that they are on par with the federal government?

Ms. Xavier: I appreciate the question very much. We have an excellent relationship with the provinces and territories. We meet with them at least once a year, in addition to all the regular conversations we have with them. We invite the provinces and territories to talk to us and provide us with higher-level briefings so that they fully understand what the threats are.

As you said regarding the Northwest Territories, we were able to deploy our sensors to get a better idea of the threats that exist in the North, given the incident the Northwest Territories experienced. For us to do that work with the provinces and territories, they have to be open to those exchanges. We cannot impose anything on them. They have to ask us for help. We work with them so that they understand what the threats are and how to increase cyber resilience in each province and territory.

We maintain close ties with them, thanks to the work we do together and our ability to notify them of threats quickly, given our mandate. They are happy with our relationship, and the same is true for Indigenous communities. We even translated our publications into other languages to ensure that they understand

Pouvez-vous nous en parler un peu plus? Vous avez été impliqués dans cette décision de moderniser la station de radar. Je crois que c'est l'Australie qui va nous aider à faire ce travail. Que pouvez-vous nous dire à ce sujet? Selon les médias, on parle de 6 milliards de dollars pour faire cette modernisation ou, à tout le moins, pour identifier les menaces.

Mme Xavier : Merci pour la question. Je ne suis pas une experte des radars. Notre agence travaille très étroitement avec nos homologues et nos collègues des Forces canadiennes pour ce qui est des radars. Notre expertise est de nous assurer que les données capturées par les radars resteront sécuritaires. Nous sommes experts dans le domaine électromagnétique et la sécurité des données. Nous nous assurons que les données sont aussi disponibles pour ceux qui en ont besoin en temps réel. Nous fournirons les fondations numériques et non le radar en soi. Je ne voudrais pas vous donner des détails sur un sujet dont je ne suis pas experte.

Le sénateur Gignac : Vous avez mentionné un cyberincident qui s'est produit en 2022. Vous en êtes même venus à la conclusion que vous deviez équiper les Territoires du Nord-Ouest. On ne parle plus d'une agence ni d'un ministère fédéral, mais de fournir de l'équipement à l'échelle provinciale et territoriale. Pouvez-vous nous parler un peu de vos relations avec les provinces? Si c'est vrai pour l'un, c'est vrai pour l'autre. Il peut s'agir du Québec ou d'autres provinces. Quelles sont vos relations, et comment pouvez-vous bien doter toutes les régions au Canada et faire en sorte qu'elles soient au même niveau que le fédéral?

Mme Xavier : J'apprécie énormément la question. Notre relation avec les provinces et territoires est excellente. Nous les rencontrons au minimum une fois par année, en plus de toutes les conversations régulières que nous avons avec eux. Nous invitons les provinces et les territoires à nous parler et à nous fournir des breffages à des niveaux plus élevés pour qu'ils comprennent bien quelles sont les menaces.

Comme vous l'avez dit, dans le cas des Territoires du Nord-Ouest, nous avons pu déployer nos capteurs pour avoir une meilleure idée des menaces qui existent dans le Nord, vu l'incident qu'ils ont vécu. Pour que nous puissions faire ce travail avec les provinces et territoires, ils doivent être ouverts à ces échanges. Nous ne pouvons pas nous imposer. Ils doivent nous inviter à leur donner un coup de main. Nous travaillons avec eux pour qu'ils comprennent quelles sont les menaces et quelles sont les manières d'augmenter la cyberrésilience dans chaque province et territoire.

Grâce au travail que nous faisons avec eux et à la rapidité avec laquelle nous leur faisons part des menaces, étant donné notre mandat, nous gardons des liens étroits. Ils sont contents de notre relation et il en va de même pour ce qui est des communautés autochtones. Nous avons même traduit nos publications dans

the threats. Whenever possible, we work closely with local communities to raise awareness of cyber-threats.

We also work with our counterparts in the Canadian Security Intelligence Service, or CSIS, who are more involved in Canada's national security. That cooperation enables us to work together to increase resilience in all areas of national security in all provinces, especially those in the North.

Senator Gignac: Okay.

[*English*]

Senator Pupatello: Can I understand exactly the area that you cover, because I understand that you are involved in surveillance where it is cyber-related. So electronic messaging, is that a good way to encapsulate the area you cover and protect?

Ms. Xavier: The way we like to describe ourselves is we call ourselves the "foreign intelligence collection agency." Our space is very much focused in the foreign space. We are not allowed to target our apparatus toward Canadians or any individuals in Canada, so an important point to make there.

The other thing, we are code makers and code breakers. Basically, we do our part to go and find intelligence linked to the priorities that have been put in place by the Government of Canada via cabinet. They are the ones who decide what the priorities are and what the intelligence that matters to them for decision making is.

The collection of that foreign intelligence is very focused on those priorities, and in doing so, we do that in the foreign space.

In addition to that, we then are the information's assurance team. So in trying to ensure that any information that the Government of Canada is collecting, for example, or any data we would want to remain in Canada is protected and shielded from cybersecurity.

Senator Pupatello: Can I ask you, from a hard-asset perspective, by way of example, in the north Baltic Sea area between England and France or Scandinavian countries, a ship managed to get in there and cut all of the fibre-optic cables. That seems to me to be fairly easy to do. These pirates got in there and caused all kinds of trouble, and of course, all this data was then either stolen or communication cut.

Do we have exposure like that anywhere around our country where there is a hard asset that could easily be damaged in that fashion?

d'autres langues pour faire en sorte qu'elles comprennent les menaces. Nous travaillons étroitement avec les communautés locales, dans la mesure du possible, pour qu'il y ait une meilleure sensibilisation à la cybermenace.

On travaille aussi avec nos homologues du Service canadien du renseignement de sécurité, qui travaillent davantage au chapitre de la sécurité intérieure du pays. Cette collaboration nous permet de travailler en collaboration pour faire en sorte d'ajouter de la résilience dans tous les domaines de la sécurité nationale et dans toutes les provinces, y compris et surtout celles du Nord.

Le sénateur Gignac : D'accord.

[*Traduction*]

La sénatrice Pupatello : J'aimerais savoir avec exactitude quel est votre champ d'activité. Je crois comprendre que votre rôle est lié à la surveillance du cyberespace. Donc, on parle de messages électroniques. Est-ce une bonne description du secteur que vous couvrez et protégez?

Mme Xavier : Nous nous décrivons nous-mêmes comme un « organisme de collecte de renseignements étrangers ». Nos activités sont fortement concentrées dans le contexte étranger. Il nous est interdit de cibler nos activités sur des Canadiens ou toute personne au Canada. Il est important de le souligner.

En outre, nous sommes des spécialistes du codage et du décodage. Essentiellement, notre rôle consiste à chercher du renseignement, en fonction de la liste des priorités établie par le gouvernement du Canada par l'intermédiaire du Cabinet. Ce sont eux qui déterminent les priorités et les renseignements importants pour eux pour la prise de décisions.

La collecte de renseignements étrangers est très axée sur ces priorités, et ces activités se font dans l'espace étranger.

De plus, nous sommes l'équipe de l'assurance de l'information. Notre rôle est donc de veiller à ce que les renseignements collectés par le gouvernement du Canada, par exemple, ou toute donnée que nous voulons conserver au Canada, soient protégés contre les incidents de cybersécurité.

La sénatrice Pupatello : Permettez-moi de poser une question au sujet des infrastructures matérielles. À titre d'exemple, un navire est parvenu à se rendre en mer Baltique, au nord, entre l'Angleterre et la France ou les pays scandinaves, pour couper tous les câbles à fibre optique. Cela me semble assez facile à faire. Ces pirates sont allés là-bas et ont causé bien des problèmes, évidemment, comme des vols de données ou l'interruption des communications.

Y a-t-il des endroits, où que ce soit au pays, où il serait facile de saboter des infrastructures matérielles de cette façon?

Ms. Xavier: Mr. Chair, that question would be better directed at the Canadian Armed Forces and our Department of National Defence. Our domain is truly in the collection of data. Where my role would come in this example that was presented is potentially in the collection of foreign intelligence that would have identified that X adversary may have cut that. I would pass that information on to the necessary other partners to potentially act accordingly.

The other space that we are often able to be called in for, especially by a request for assistance. If, for example, the RCMP needed our assistance from a technical perspective, they could seek to ask us for our assistance. We would be operating under their mandate.

The other role we play and the other part of our mandate is what we call foreign cyber operations. In cyberspace, again, if I have sufficient intelligence or awareness, again linked to intelligence priorities, working with my colleagues at Global Affairs Canada, I might choose to do an active cyber operation linked to the priorities of national interest as well as economic interest to disrupt, perhaps, something that I'm seeing, again, in the cyberspace that potentially could be something that is targeted toward Canada or its allies. So it's mainly in the cyberspace that I operate, not in the physical, tangible space, if that's helpful.

Senator Pupatello: Based on that space you operate in, after an event has occurred, you would know that is a weak link.

Ms. Xavier: It's fair to say it is possible that I might see it after, but it's also possible I might see it before. Part of what we do when we are doing foreign intelligence collection is possibly looking for warnings in advance, so not only after. I might be able to warn somebody.

We do this, for example, in the cyberdefence perspective. We actually contact organizations where we give them what we call a pre-notification saying "X company, we have good indications to identify that you have a cyber possible incident that is happening" because we have seen it either in the foreign intelligence space or through a defence sensor that is letting us know that there is something — an anomaly — going on there. We have been able to prevent over 300 Canadian companies from being attacked by ransomware as a result of it.

Senator Pupatello: That's good to know. Is that in that report coming up?

Ms. Xavier: It will be in the report. It was in last year's, and it will be in this year's as well.

Mme Xavier : Monsieur le président, cette question devrait plutôt être posée aux Forces armées canadiennes et au ministère de la Défense nationale. Notre domaine de compétence est vraiment la collecte de données. Mon rôle, dans l'exemple qui a été donné, consisterait à collecter des renseignements étrangers permettant de déterminer l'identité de l'adversaire qui est l'auteur probable de ce sabotage. Je transmettrais ces renseignements aux autres partenaires concernés afin qu'ils puissent, possiblement, prendre des mesures en conséquence.

Une autre situation pour laquelle on fait souvent appel à nous, c'est dans le cas d'une demande d'aide, par exemple une demande d'aide de la GRC pour une question technique. À ce moment-là, nous fonctionnerions dans le cadre de leur mandat.

L'autre rôle que nous jouons — et qui est l'autre partie de notre mandat —, c'est ce que nous appelons les cyberopérations étrangères. Dans le cyberespace, encore une fois, si j'ai suffisamment de renseignements ou de connaissances sur un incident quelconque, toujours par rapport aux priorités en matière de renseignement, je pourrais choisir de mener, en collaboration avec mes collègues d'Affaires mondiales Canada, une cyberopération active qui serait liée à la liste des priorités d'intérêt national ou économique afin de perturber une activité dans le cyberespace ciblant le Canada ou ses alliés. Mes activités se passent essentiellement dans le cyberespace et non dans le monde physique et concret, si cela peut vous aider.

La sénatrice Pupatello : Étant donné le milieu dans lequel vous évoluez, si un incident se produit, vous savez qu'il s'agit d'un maillon faible.

Mme Xavier : Il est possible que je le constate après coup, certes, mais il est aussi possible que je le constate avant. Dans la collecte de renseignements étrangers, notre travail consiste probablement, en partie, à chercher des indices avant qu'un incident se produise, donc pas seulement après, de sorte que je pourrais alerter quelqu'un.

C'est ce que nous faisons, par exemple, du point de vue de la cyberdéfense. Il nous arrive de communiquer avec des organismes pour leur donner ce que l'on appelle un préavis, en disant : « Nous avons de bonnes raisons de croire que vous faites l'objet d'une cyberattaque », parce que nous avons constaté, durant une opération de renseignement étranger ou grâce à un mécanisme de détection de défense, qu'il se passe quelque chose, une anomalie. Ces opérations nous ont permis de prévenir des attaques par rançongiciel contre plus de 300 entreprises canadiennes.

La sénatrice Pupatello : C'est bon à savoir. Cela figure-t-il dans le rapport à venir?

Mme Xavier : Ce sera dans le rapport. C'était dans celui de l'année dernière, et ce sera dans celui de cette année aussi.

Senator Pupatello: Just one more quick question. Is there anything you collect as far as data or work you do in prevention that is of use in a briefing to MPs, ministers or senators? Do you do those types of regular briefings besides the annual report?

Ms. Xavier: We do. And absolutely, a great deal of the information that we learn, both from our intelligence mandate as well as our cyber defence mandate, is extremely helpful in the publication that we put out, as well as for the briefings we have given to MPs, senators, politicians, anybody who will listen to us —

Senator Pupatello: Do you do that on request or do you hold quarterly briefings?

Ms. Xavier: We do it in a variety of ways. For example, leading up to the general election, we did those on a regular basis, because we wanted to make sure that various individuals were quite aware of what could be coming. But we also do them on request. But that's also why we do the publications, because we try to do it using our social media channels as well as another feature. During the month of October, which is Cyber Security Awareness Month, we go out and do a proactive splash campaign to be able to reach various generations of people so that they are interested in cyber resilience.

[*Translation*]

Senator Moreau: I would like to note that Canada has entrusted its cybersecurity to women; that means we are safe. Congratulations on that. Thank you for being with us.

I fully understand the top-secret nature of your activities. When it comes to public finances, who knows what you are doing with the money entrusted to you, apart from your Chief Financial Officer, Julie Chassé? Who do you ultimately report to, or is the idea to have complete independence in discretion and the use of funds?

Ms. Xavier: As I said in my opening remarks, we report directly to the defence minister, and I'm accountable to him. We are also supported by an extensive system of review bodies, including the National Security and Intelligence Committee of Parliamentarians, or NSICOP, the National Security and Intelligence Review Agency, and the Intelligence Commissioner, who scrutinizes everything we do, especially when we request special authorization from the minister. Everything we do needs to be authorized by the minister and reviewed by the commissioner. We are audited by the Auditor General of Canada, but we also have our own internal auditor. My Chief

La sénatrice Pupatello : J'ai une dernière petite question. Dans les renseignements que vous collectez ou dans votre travail de prévention, y a-t-il, des éléments qui pourraient être utiles pour une séance d'information à l'intention des députés, des ministres ou des sénateurs? Outre votre rapport annuel, offrez-vous des séances d'information régulières de ce genre?

Mme Xavier : Oui. Bien entendu, bon nombre des renseignements dont nous prenons connaissance, tant dans le cadre de notre mandat de renseignement que dans celui de cyberdéfense, sont extrêmement utiles pour nos publications, mais aussi dans nos séances d'information à l'intention des députés, des sénateurs, des politiciens, de tous ceux qui sont prêts à nous écouter...

La sénatrice Pupatello : Offrez-vous ces séances d'information sur demande? En organisez-vous chaque trimestre?

Mme Xavier : Nous faisons différentes choses. Par exemple, avant les élections générales, nous avons tenu ces séances régulièrement, car nous voulions nous assurer que tout le monde était bien conscient de ce qui pouvait arriver. Mais nous pouvons également les organiser lorsque l'on en fait la demande. C'est aussi la raison pour laquelle nous publions des rapports. Nous essayons de renseigner les gens par l'entremise de nos réseaux sociaux et d'autres moyens. Durant le mois d'octobre, qui est le Mois de la sensibilisation à la cybersécurité, nous menons une campagne intensive et proactive afin de rejoindre différentes générations de Canadiens et de les intéresser à la cyberrésilience.

[*Français*]

Le sénateur Moreau : Je constate que le Canada a confié sa cybersécurité à des femmes; nous sommes donc en sécurité. Félicitations pour cela. Merci d'être avec nous.

Je comprends très bien la nature des activités que vous faites et qui sont à un niveau top secret. Sur le plan des finances publiques, outre votre collègue Julie Chassé, dirigeante principale des finances, qui sait ce que vous faites avec l'argent qui vous est confié? À qui vous rapportez-vous, ultimement? À l'inverse, le principe est-il plutôt d'avoir une totale autonomie dans la discrétion et l'utilisation des fonds?

Mme Xavier : Comme je l'ai dit dans mes remarques d'ouverture, on se rapporte directement au ministre de la Défense, devant qui je suis responsable. De plus, nous avons un important système de surveillance qui nous soutient, qui comprend le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR), l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, ainsi qu'un commissaire au renseignement qui doit examiner tout ce que l'on fait, surtout lorsqu'on demande une autorisation spéciale de notre ministre. Tout ce que l'on fait doit donc être autorisé par notre ministre et revu par ce commissaire. Des

Financial Officer ensures that expenditures are reported to the Comptroller General of Canada.

In other words, we are accountable to several authorities and need to act in accordance with the law.

Senator Moreau: I understand that this information may not be public, but does the Auditor General, for example, have access to all the funds you are allocated? Unlike some police forces, your organization doesn't have a slush fund. Is that correct?

Ms. Xavier: I'm not sure I understand what you mean by "slush fund."

Senator Moreau: I mean a fund that no one can examine. The overall amount is known, but there is no way of finding out what it will be used for.

Ms. Xavier: The fund's overall amount is publicly known. I will now defer to my colleague.

Julie Chassé, Chief Financial Officer, Communications Security Establishment Canada: We have no slush fund. Anyone from the Office of the Auditor General of Canada with the proper security clearance has access to our information.

Senator Moreau: That person can ask any question about all the amounts spent?

Ms. Chassé: Exactly. We also have an internal audit committee, including external members, that has access to all information.

Senator Moreau: Great.

Governments in general have a very bad reputation when it comes to IT services. Examples around here include the federal Phoenix pay system and SAAQclic in Quebec. You are in the business of gathering sensitive information. How do you ensure that the systems available to you are reliable? I have some related sub-questions.

What do you do to make sure that the security-related data you collect remains confidential to avoid situations like Wikileaks?

What do you do about people who leave the CSEC? Senator Carignan said that very few people leave. Do you have to kill them to make sure the information they collect when working for you is kept secret?

How do you ensure the security chain for the information gathered?

vérifications sont également faites par la vérificatrice générale du Canada, mais nous avons notre propre vérificateur à l'interne, et ma dirigeante principale des finances s'assure que les dépenses sont rapportées à la contrôleure générale du Canada.

C'est donc dire que nous devons rendre des comptes à plusieurs instances et faire les choses conformément à la loi.

Le sénateur Moreau : Je comprends que cette information puisse ne pas être publique, mais est-ce que la vérificatrice générale, par exemple, a accès à l'ensemble des fonds qui vous sont confiés? Contrairement à certains corps policiers qui ont des fonds secrets, votre organisation n'en dispose pas. Est-ce exact?

Mme Xavier : Je ne suis pas certaine de bien comprendre la question à savoir si l'on dispose de « fonds secrets ».

Le sénateur Moreau : Je parle de fonds qui ne sont examinés par personne, dont on connaît le montant global, mais dont on n'a aucune possibilité de savoir à quelles fins ils sont utilisés.

Mme Xavier : De façon publique, c'est un fonds à numéro global. Je cède maintenant la parole à ma collègue.

Julie Chassé, dirigeante principale des finances, Centre de la sécurité des télécommunications Canada : On n'a pas de fonds secrets. Ainsi, toute personne au Bureau du vérificateur général du Canada qui aurait la cote de sécurité requise pourrait avoir accès à notre information.

Le sénateur Moreau : Cette personne peut poser toute question à l'égard de toutes les sommes qui sont dépensées?

Mme Chassé : Exactement. On a aussi un comité de vérification interne, avec des membres externes, qui ont accès à toute l'information.

Le sénateur Moreau : Parfait.

Les gouvernements en général ont très mauvaise réputation en matière de services informatiques. On l'a vu ici, au fédéral, avec notamment le système de paie Phénix, et au Québec avec SAAQclic. Vous êtes dans un domaine de récupération d'informations délicates. Comment vous assurez-vous de la fiabilité des systèmes mis à votre disposition? J'ai quelques sous-questions à cette question.

Qu'est-ce que vous faites pour vous assurer de conserver la confidentialité des données collectées à des fins de sécurité pour éviter des situations comme WikiLeaks, par exemple?

Que faites-vous avec les gens qui quittent le CST? Le sénateur Carignan disait que vous en aviez très peu qui partent; devez-vous les tuer pour qu'ils gardent secrètes des informations collectées pendant qu'ils sont à votre emploi?

Comment vous assurez-vous de la chaîne de sécurité des informations récoltées?

Ms. Xavier: It's important to know that all employees who join us, especially ones working in highly sensitive areas, need to have enhanced top secret clearance. This is referred to as an "enhanced top secret security clearance." There is a very strict process to get that. Just the fact that someone wants to join us means that the person is already very committed.

Not to mention that the clearance is renewed every five years. If an employee's circumstances change, they are required to proactively share that information. We do a lot of training and pay close attention to how our employees act.

If someone starts acting strangely, we take swift action. Our managers and supervisors are very well trained to know what they need to keep an eye on.

We look very closely at tendencies. We work very hard to build a culture of values, ethics and compliance with the law. That's part of our values. Something else we put in place last year is a code of conduct that very clearly shows our expectations toward our employees.

I work with employees who are totally dedicated to what they do and are extremely passionate about it. That's why we try to keep them very engaged, because we do highly creative, interesting things, and the projects they work on are unique.

Senator Moreau: How do you ensure that?

Ms. Xavier: Being part of an organization like ours, we are all very dedicated.

[*English*]

We're all having to adhere to the Foreign Interference and Security of Information Act.

[*Translation*]

I think the act has a new name, so I might not be saying it right. If I quit my job, I need to follow the instructions.

[*English*]

I'm committed until death.

[*Translation*]

So yes, basically, they'd have to kill me.

We don't take it lightly. When someone leaves, we remind them that they can't repeat anything they've learned here or use it in any way. There are ex-employees who go on to write a

Mme Xavier : Il est important de savoir que tous les employés qui se joignent à nous, surtout ceux qui vont travailler dans les domaines très sensibles, doivent avoir une cote Très secret; on appelle cela une « cote de sécurité Très secret approfondie ». Cela veut dire que c'est quand même un processus assez rigoureux. Juste le fait que quelqu'un veuille se joindre à nous montre que la personne est déjà très investie.

Cela dit, c'est quelque chose qui est renouvelé tous les cinq ans. L'autre chose que les employés sont obligés de faire, c'est que, si leurs circonstances évoluent, ils doivent proactivement partager cette information. On fait beaucoup de formation et on examine très attentivement comment nos employés agissent.

Si quelqu'un commence à avoir un comportement bizarre, on agit rapidement. Il y a beaucoup de formation qui se fait avec nos gestionnaires et nos superviseurs pour qu'ils sachent ce qu'ils doivent observer.

On regarde les tendances de très près. On travaille très fort sur une culture de valeurs et d'éthique, de conformité et de lois. Cela fait partie de nos valeurs. Je dirais que l'autre chose que nous avons mise en place l'année dernière, c'est un code de conduite où nos attentes envers les employés sont très claires.

Je travaille avec des employés qui sont vraiment dévoués à ce qu'ils font, qui sont très passionnés. C'est pour cela que ce qu'on essaie de faire, c'est de les garder très engagés, parce qu'on fait des choses très créatives et intéressantes et qu'ils ont la chance de travailler sur des projets uniques.

Le sénateur Moreau : Comment vous assurez-vous de cela?

Mme Xavier : Puisque nous faisons partie d'une organisation comme la nôtre, nous sommes tous dévoués.

[*Traduction*]

Nous devons tous respecter la Loi sur l'ingérence étrangère et la protection de l'information.

[*Français*]

Je crois que la loi a changé de nom, donc je ne le dis peut-être pas de la bonne façon. À cause de cela, si je quitte mon poste, je dois respecter certaines consignes.

[*Traduction*]

Je la respecterai jusqu'à ma mort.

[*Français*]

Donc, à la fin, oui, il faudra me tuer.

Nous ne prenons pas cela à la légère. Lorsque vous partez, on vous rappelle que tout ce que vous avez appris ici, vous ne pouvez pas l'utiliser n'importe comment ou le répéter. C'est sûr

book, for example, but they need to share its contents with us before it's published.

We have a legal right to enforce the law, if necessary. We hope that people will continue to uphold Canadian patriotism and defence even after they leave.

[*English*]

Senator Galvez: I propose to change the subject. Communications Security Establishment Canada, or the CSE, must contribute to Federal Sustainable Development Strategy goals from 2023 up to 2026, specifically on Goal No. 10 and Goal No. 12 and, for me more important, Goal No. 13, "Take action on climate change and its impacts."

Now, we know that Canada relies heavily on both domestic and international satellite systems to track crucial environmental indicators. Actually, 26 of the 52 essential parameters come from satellites. We know that Canada depends significantly on the National Oceanic and Atmospheric Administration, or NOAA, and other U.S.-operated satellite platforms for early-warning systems related to wildfire, floods and extreme weather. We need more and more security for our infrastructure.

In light of the cuts that the U.S. administration has done to NOAA, and in light of Minister Guilbeault telling us that the Canadians satellites that can do this job will only be ready in 2027 or before 2030, how much funding has been allocated for you to do this work? Can you provide the committee with a brief summary on your progress? How do you secure the information technology and the infrastructure to help us to do this job?

Ms. Xavier: Thank you for the question. Part of the question, unfortunately, is not within my mandate. Again, my mandate is very much focused on ensuring the protection of the data that the satellites might collect and ensuring that the infrastructure linked to Canadian infrastructure is cyberdefended and protected.

In terms of the satellite itself, it's not something that we own. Again, this question might be better directed toward the Department of National Defence and the Canadian Armed Forces.

Senator Galvez: [Technical difficulties] — data that you collect?

Ms. Xavier: Yes. Again, in the collection of the data that we would collect from these satellites, if they're coming into my systems, our priority is ensuring it will be made available in real

qu'il y a des personnes qui partent, qui écrivent un livre, par exemple, mais elles doivent partager le contenu avec nous avant de le publier.

Il y a des lois qui nous permettent d'exécuter la loi, si nécessaire. On espère que les gens continueront de respecter le patriotisme et la défense du Canada même après leur départ.

[*Traduction*]

La sénatrice Galvez : Je propose de changer de sujet. Le Centre de la sécurité des télécommunications Canada, ou CST, doit contribuer aux objectifs de la Stratégie fédérale de développement durable de 2023 à 2026, plus précisément aux objectifs nº 10 et nº 12 et, ce qui est plus important à mes yeux, à l'objectif nº 13, « Prendre des mesures relatives aux changements climatiques et leurs impacts ».

Nous savons que le Canada dépend fortement des systèmes à satellites nationaux et internationaux pour surveiller des indicateurs environnementaux cruciaux. D'ailleurs, 26 des 52 paramètres essentiels proviennent de satellites. Les systèmes d'alerte précoce que le Canada utilise en cas de feux de forêt, d'inondations et de phénomènes météorologiques extrêmes dépendent beaucoup de la National Oceanic and Atmospheric Administration, ou NOAA, et d'autres plateformes satellitaires exploitées par les États-Unis. Nous devons accroître la protection de nos infrastructures.

L'administration américaine a imposé des compressions à la NOAA, et le ministre Guilbeault a déclaré que les satellites canadiens qui sont en mesure d'assurer cette surveillance ne seront prêts qu'en 2027, ou avant 2030. Dans ce contexte, quelles sommes avez-vous reçues pour accomplir ce travail? Pouvez-vous nous faire un bref résumé des progrès que vous avez accomplis? Comment assurez-vous la protection des technologies de l'information et des infrastructures dont nous avons besoin pour accomplir ce travail?

Mme Xavier : Je vous remercie de la question. Malheureusement, une partie de votre question ne relève pas de mon mandat qui, je le répète, consiste principalement à assurer la protection des données que les satellites pourraient recueillir et à veiller à ce que les infrastructures liées aux infrastructures canadiennes soient protégées contre les cyberattaques.

Pour ce qui est du satellite lui-même, il ne nous appartient pas. Il vaudrait donc mieux poser cette question aux représentants du ministère de la Défense nationale et des Forces armées canadiennes.

La sénatrice Galvez : [Difficultés techniques] données que vous recueillez?

Mme Xavier : Oui. Comme je l'ai dit, si les données que nous recueillons à l'aide de ces satellites aboutissent dans nos systèmes, notre priorité est de veiller à ce qu'elles soient mises à

time back to the users who will need access it to make decisions, either in the form of intelligence or potentially in this digital backbone that we're going to be building with the investments that have been made in Supplementary Estimates (A).

As well, the other part is in continuing to work toward what we call building secure communications so that we can ensure that information we collect will remain sovereign. In that way, it can be properly shared, again with decision makers or other individuals who will need that data to make decisions on future investments or to make defence decisions.

We have supported low Earth orbit Lightspeed projects by providing, again, that high-assurance, cryptographic equipment. Our focus is totally on securing the communications rather than worrying about the direct satellite placement, if you see what I mean.

Senator Galvez: These security methods, are they relying on Canadian technology or American technology or European technology?

Ms. Xavier: It is fair to say that, right now, especially in the Five Eyes, we are all collectively reliant on various types of technologies. Part of our focus with the investment we receive will be on continuing to build out that sovereign element of the technology.

It's not to say that we still might not rely on other partners for parts of the infrastructure, because we have to build up the defence industrial base here in the country to ensure we can also have Canadian producers of some of the products we may need. Having said that, many things that we have in Canada will continue to allow us to have sovereignty. But the piece we worry about the most is ensuring that the data, once collected, remains in sovereign, protected hands. That is what we help to do.

Senator Galvez: I'm curious. Do we use Elon Musk's technology?

Ms. Xavier: I don't know that I can answer that question to that level of detail. I'm sorry. Thank you.

Senator Galvez: Because it's confidential?

Ms. Xavier: For national security reasons.

Senator Galvez: Thank you.

Senator Loffreda: Thank you for being here. This is very interesting. My question is on cyber-threat landscape and adaptability. Given the rapidly evolving global cyber-threat

la disposition — et ce en temps réel — des utilisateurs qui en ont besoin pour prendre des décisions, soit sous forme de renseignements, soit, éventuellement, dans cette fondation numérique que nous allons développer grâce aux investissements prévus dans le Budget supplémentaire des dépenses (A).

Ensuite, nous devons poursuivre nos efforts pour mettre en place des communications sécurisées, afin de garantir la souveraineté des informations que nous recueillons. Ce faisant, elles pourront être partagées efficacement, avec, comme je l'ai dit, les décideurs ou d'autres personnes qui en auront besoin pour prendre des décisions relatives aux investissements futurs ou à la défense.

Nous avons soutenu les projets du réseau Lightspeed, un réseau de satellites en orbite basse, en fournissant, là encore, de l'équipement de chiffrement hautement sécurisé. Notre priorité est entièrement axée sur la protection des communications plutôt que sur l'installation des satellites, si vous voyez ce que je veux dire.

La sénatrice Galvez : Ces mécanismes de sécurité reposent-ils sur une technologie canadienne, américaine ou européenne?

Mme Xavier : Il convient de reconnaître qu'à l'heure actuelle, en particulier au sein du Groupe des cinq, nous dépendons tous de divers types de technologies. Une partie des investissements que nous recevons sera consacrée au développement de technologies proprement canadiennes.

Le fait de renforcer la base industrielle de défense ici, au Canada, qui nous permettra de compter sur des producteurs canadiens pour une partie des produits dont nous pourrions avoir besoin, ne veut pas nécessairement dire que nous n'allons plus compter sur d'autres partenaires pour certains éléments des infrastructures. Cela dit, de nombreux éléments dont nous disposons au Canada nous permettront de demeurer souverains. Le plus important, à nos yeux, est de veiller à ce que les données, une fois recueillies, demeurent souveraines et protégées. Voilà l'objectif de nos efforts.

La sénatrice Galvez : Je suis curieuse. Est-ce que nous utilisons la technologie développée par Elon Musk?

Mme Xavier : Je ne sais pas si je peux répondre à cette question de façon aussi précise. Je suis désolée. Merci.

La sénatrice Galvez : Parce que cette information est confidentielle?

Mme Xavier : C'est pour des raisons de sécurité nationale.

La sénatrice Galvez : Je vous remercie.

Le sénateur Loffreda : Je vous remercie de votre présence. C'est très intéressant. Ma question porte sur les cybermenaces et la capacité d'adaptation. Compte tenu de l'évolution rapide des

environment, including threats from state and non-state actors, how is CSE adapting its tools, training and intelligence-gathering strategies to respond in real time to new and emerging threats, particularly with the rise of generative AI and deep fake technologies?

Ms. Xavier: Thank you for the question. As you can imagine, Canada's not immune to cyber-threats. This is why we put out national cyber-threat assessments every couple of years. We also put out threats of democratic processes every couple of years. We put out regular publications because of the threats we are seeing coming toward Canada.

It's also because of all that we're learning in the defence of Government of Canada systems that we can know the types of threats out there, combined with what we learn from the foreign intelligence collection that we have.

In the business of cyberdefence of Canada — in the Government of Canada systems, in particular — we already use artificial intelligence. We already use automation. We already use machine learning to defend that in an automated way. We could not do our jobs in the effective way we do in stopping billions of actions per day against Government of Canada systems without those automated systems.

Senator Loffreda: Billions of actions per day. Wow. Billions.

Ms. Xavier: Billions of actions per day are prevented because of the fact that we are seen as very interesting target when you think of data in the Government of Canada systems.

That's in addition to the fact that many private sectors and critical infrastructure are also seeing cyber-threats. Which is why we work so hand-in-glove with partners like industry, academia and critical infrastructure in the form of governance communities where we share intelligence with them. We share threat pictures and do exchanges with them to better understand what their security domains are like. We learn a lot from them, as much as they learn from us — and we learn a lot in the defence of the Government of Canada systems. All of that gets fed back in, in an automated way, to continue to raise the resilience of our systems in the defence of Canada.

cybermenaces dans le monde, y compris des menaces provenant d'acteurs étatiques et non étatiques, comment le CST adapte-t-il ses outils, ses formations et ses stratégies de collecte de renseignements afin de répondre en temps réel aux menaces nouvelles et émergentes, surtout compte tenu de l'essor de l'IA générative et des technologies d'hypertrucage?

Mme Xavier : Je vous remercie de la question. Comme vous pouvez l'imaginer, le Canada n'est pas à l'abri des cybermenaces. C'est pourquoi nous publions tous les deux ans des évaluations nationales des cybermenaces. Nous publions également tous les deux ans un rapport sur les menaces qui pèsent sur les processus démocratiques. Nous présentons des documents régulièrement en raison des menaces auxquelles le Canada fait face.

Ensuite, grâce à tout ce que nous apprenons dans le cadre de nos activités de défense des systèmes du gouvernement du Canada, sans oublier ce que nous apprenons grâce à la collecte de renseignements étrangers, nous pouvons connaître les types de menaces qui existent.

Nous utilisons déjà l'intelligence artificielle — en particulier avec les systèmes du gouvernement du Canada — dans le domaine de la cyberdéfense du Canada. Nous utilisons déjà l'automatisation; nous avons recours à l'apprentissage automatique pour assurer une protection automatisée des systèmes. Sans ces systèmes automatisés, nous ne pourrions pas faire notre travail aussi efficacement et bloquer les milliards d'opérations lancées contre les systèmes du gouvernement du Canada chaque jour.

Le sénateur Loffreda : Des milliards d'opérations chaque jour. C'est incroyable. Des milliards.

Mme Xavier : Nous devons écarter des milliards de menaces chaque jour parce que nous sommes considérés comme une cible très intéressante. Il suffit de penser aux données que contiennent les systèmes du gouvernement du Canada.

Mais ce n'est pas tout. Bon nombre d'acteurs du secteur privé et d'infrastructures essentielles sont eux aussi confrontés à des cybermenaces. C'est pourquoi nous travaillons en étroite collaboration avec des partenaires de l'industrie, du monde universitaire et des infrastructures essentielles dans le cadre d'une gouvernance communautaire où nous échangeons des renseignements avec eux. Nous partageons des images de menaces et échangeons avec eux afin de mieux comprendre leur situation en matière de sécurité. Nous apprenons beaucoup d'eux, et vice-versa. Nous apprenons beaucoup de choses dans le cadre de la défense des systèmes du gouvernement du Canada. Toutes ces informations sont automatiquement intégrées à nos systèmes, ce qui renforce leur résilience en faveur de la défense du Canada.

Senator Loffreda: Thank you. My next question would be on public trust and institutional confidence. Public trust is important in today's day and age, especially with privacy concerns. CSE plays a critical role in safeguarding national security, but it operates largely behind closed doors, and rightfully so. You have to operate behind closed doors.

What efforts are being made to build public trust and institutional transparency without compromising operational security, which is so important, particularly as public concern about surveillance and data privacy grow?

Ms. Xavier: Thank you again for the question. The part that I think is worth re-emphasizing here is that, as an agency, we do not target Canadians nor any persons in Canada. Our apparatus in general is targeting foreign intelligence and foreign adversaries. With that itself, we hope that is already a foundational piece for building trust with Canadians.

The other part that helps us to build trust with Canadians are the publications we put out. We have a website called cyber.gc.ca, which is one that we take pride in because it really caters to the variety of individuals who are potentially interested in cybersecurity, from the expert in cybersecurity to the layman grandmother who may want to know what she needs to do to protect herself from anything on her mobile phone. This is where we take advantage of October as cyber month to be proactive in talking to various generations of people, so they know the things that they could do to be able to protect themselves.

The other thing is we do a lot in the outreach space. We work hard with communities, like the Indigenous communities, as I said earlier. We translate our publications in various languages, but we also do things with high schools and with various other groups to encourage — especially women in STEM — to not fear coming into the domain of cybersecurity or mathematics, because these are the types of talents we sometimes look for.

We try to make ourselves as available as we can in trying to lower the bar of entry into the domain of interest into cybersecurity. We recognize the importance of continuing to do our part to educate, to make sure that people understand the difference between misinformation and disinformation, and to become critical thinkers in how they are looking at information online. In doing that, we're raising the whole of society's resilience.

Le sénateur Loffreda : Je vous remercie. Ma prochaine question porte sur la confiance du public et la confiance envers les institutions. De nos jours, la confiance du public est importante, surtout en raison des préoccupations relatives à la protection des renseignements personnels. Le CST joue un rôle essentiel dans la protection de la sécurité nationale, mais ce qu'il fait demeure, en grande partie, confidentiel, et ce, avec raison. Vous devez travailler derrière des portes closes.

Quels efforts déployez-vous pour renforcer la confiance du public et la transparence au sein des institutions sans pour autant compromettre la sécurité des opérations, qui est si importante, en particulier à l'heure où les préoccupations de la population à propos de la surveillance et de la confidentialité des données ne cessent de croître?

Mme Xavier : Une fois de plus, je vous remercie de la question. Je tiens à souligner à nouveau que notre agence ne cible ni les Canadiens ni d'autres personnes au Canada. Nos activités se concentrent généralement sur les services de renseignement étrangers et les adversaires étrangers. Nous espérons que cela constitue déjà une base solide pour établir un lien de confiance avec les Canadiens.

Nos publications nous aident aussi à bâtir la confiance. Nous avons un site Web, cyber.gc.ca, dont nous sommes très fiers, car il s'adresse vraiment à toute personne qui pourrait s'intéresser à la cybersécurité, de l'expert en la matière au profane, comme une grand-mère, qui souhaite savoir comment se protéger contre des menaces sur son téléphone portable. C'est dans ce contexte que nous tirons parti du mois d'octobre, qui est le mois de la cybersécurité, pour communiquer de manière proactive avec des gens de diverses générations afin de les renseigner sur ce qu'ils peuvent faire pour se protéger.

Nous déployons également de nombreux efforts de sensibilisation. Nous collaborons de près avec les communautés, notamment avec les communautés autochtones, comme je l'ai dit plus tôt. Nous traduisons nos publications dans différentes langues. De plus, nous organisons des activités dans des écoles secondaires et avec d'autres groupes afin d'encourager les gens — surtout les femmes dans les domaines de la science, de la technologie, de l'ingénierie et des mathématiques — à ne pas avoir peur de se lancer dans le domaine de la cybersécurité ou des mathématiques, car nous recherchons parfois des gens qui possèdent ces compétences.

Nous nous efforçons de faciliter l'accès au secteur de la cybersécurité. Nous reconnaissons que nous devons faire notre part en matière de sensibilisation, pour veiller à ce que les gens comprennent la différence entre la mésinformation et la désinformation, et développent leur pensée critique au sujet des renseignements publiés en ligne. Ces efforts sont importants, car ils nous permettent de renforcer la résilience de l'ensemble de la société.

In February, the National Cyber Security Strategy was released by the Government of Canada where, again, a whole-of-society element is a very big part of what we're all collectively working on to raise cyber resilience.

Senator Loffreda: Thank you.

[*Translation*]

Senator Dalphond: In your June 2024 annual report, you claim to prevent 6.6 billion potential attacks per day. That's pretty impressive work.

In the same report, the minister at the time points out that in the 2024 budget, the government projected an additional $917 billion to CSEC over five years, so around $200 million per year. The estimates for 2024-25 are the same as for 2023-24, so it wasn't yet reflected in the costs. This year, there will be an increase. Which part is new in terms of the announcement? The supplementary estimates show $370 million, but I assume that there was probably $200 million already budgeted for 2024. Which is the old part and which part was added?

Ms. Xavier: I will let my colleague answer. I might have something to add afterward.

Ms. Chassé: The $200 million difference between last year's main estimates and this year's is the result of decisions made for the 2024 budget. There is $131.2 million from the 2024 budget to augment intelligence and cyber operations.

As Ms. Xavier mentioned in her opening remarks, there is also $21 million related to border management, meaning border security and fentanyl control. I'd say that these are the two largest items contributing to the discrepancy of around $200 million.

Senator Dalphond: The budget is around $150 million more than for 2024?

Ms. Chassé: Thereabouts.

Senator Dalphond: Ms. Xavier, in the annual report, you indicate that CSEC has 3,529 full-time employees.

Earlier, you mentioned 3,800 employees, almost 300 more, and you also said you had recruited 800 people. According to my calculations, there are 500 employees missing. At first, you had 3,529 employees, and now you have 3,800. That's an increase of 300 employees, yet you hired 800 people.

En février, le gouvernement du Canada a publié sa Stratégie nationale en matière de cybersécurité, qui, là encore, accorde une place très importante à l'ensemble de la société dans les efforts collectifs que nous accomplissons pour renforcer la cyberrésilience.

Le sénateur Loffreda : Je vous remercie.

[*Français*]

Le sénateur Dalphond : Dans votre rapport annuel de juin 2024, vous parliez de 6,6 milliards d'attaques potentielles empêchées par jour; c'est assez impressionnant comme travail.

Dans ce même rapport, le ministre de l'époque rappelle que, dans le budget de 2024, le gouvernement a prévu pour votre centre 917 milliards de dollars de plus sur cinq ans, donc environ 200 millions de dollars par année. Je regarde le budget des dépenses pour 2024-2025 et c'était la même chose qu'en 2023-2024, donc ce n'était pas encore reflété dans les coûts. Cette année, il y aura une augmentation. Quelle partie est nouvelle par rapport à l'annonce? Le budget supplémentaire indique 370 millions de dollars, mais je considère qu'il y avait probablement 200 millions de dollars qui étaient déjà prévus au budget de 2024. Alors, quelle est la partie ancienne et la partie qui a été ajoutée?

Mme Xavier : Je vais laisser ma collègue répondre. J'aurai peut-être des choses à ajouter ensuite.

Mme Chassé : Les 200 millions de dollars de différence entre les crédits principaux de l'année précédente et ceux de cette année sont le résultat de décisions prises dans le cadre du budget de 2024. Donc, j'ai 131,2 millions de dollars qui proviennent du budget de 2024 pour bonifier l'intelligence et les cyberopérations.

On a également 21 millions de dollars, comme Mme Xavier l'a mentionné dans ses remarques liminaires, qui sont liés à la gestion des frontières, donc la sécurité des frontières et le contrôle du fentanyl. Je dirais que ce sont les deux plus gros postes qui contribuent à la variation d'environ 200 millions de dollars.

Le sénateur Dalphond : Donc, c'est un budget d'environ 150 millions de dollars de plus par rapport à 2024?

Mme Chassé : Environ.

Le sénateur Dalphond : Madame Xavier, dans le rapport annuel, vous indiquez que le centre a 3 529 employés à temps plein.

Plus tôt, vous avez parlé de 3 800 employés, donc un peu moins de 300 de plus, et vous avez également dit que vous aviez recruté 800 personnes. Selon mon calcul, vous en avez donc perdu 500. Pouvez-vous expliquer la différence? À première vue, vous avez 3 529 employés et maintenant vous avez

Ms. Xavier: Let me clarify. In 2025, we had already hired over 400 people the previous year, which is 800 people over the two fiscal years. Last year, when the report was published, we had around 3,500 employees. In the fiscal year, we hired 400 more people, which brings us to over 3,800 employees.

The exact number of employees at the end of this fiscal year, March 31, is 3,841 people. We are currently in a phase of continuing growth, and we have close to 4,000 employees. This year, we plan to hire around 400 more people.

I hope that clarifies things for you.

Senator Dalphond: I understand. The figure of 800 is for two fiscal years rather than one.

Ms. Xavier: Exactly.

Senator Dalphond: That brings the rate to 5%; I get it.

My colleague Senator Moreau referred to technology. The government has proved that it is not the best at managing the costs associated with new technologies. You work with extremely new technology. What guarantees that you can do better than the rest of the government?

Ms. Xavier: I would never say that anything is risk-free, and I can't guarantee that we won't make mistakes. Our organization is always in learning mode, and we try to learn from the way others implement technology in order to improve.

That said, I have a lot of very brilliant tech employees who are very creative, skilled and innovative. I'm confident, especially since we give advice to the government about the best ways to protect their systems and set them up so that they work as they should. We also have good project management experts who love a challenge. We will do our best.

I don't want to give you the impression that we won't learn anything. We are already learning from our international counterparts by looking at the way they put in place certain techniques. That helps us learn how to do things better on our side.

3 800 employés. Il s'agit d'une augmentation de 300 employés, mais vous avez engagé 800 personnes.

Mme Xavier : Laissez-moi préciser. En 2025 nous avons embauché au-delà de 400 personnes l'année précédente, mais pour les deux années fiscales, on parle de 800 personnes. Donc oui, l'année dernière, au moment de la publication du rapport, on avait environ 3 500 employés. Donc, dans l'année fiscale, on a embauché 400 personnes de plus, ce qui nous amène au-delà de 3 800 employés.

Le nombre exact d'employés à la fin de cette année fiscale est de 3 841 personnes à partir du 31 mars. On est actuellement dans une phase de croissance continue et on a près de 4 000 employés. Cette année, nous allons embaucher environ 400 personnes de plus, selon nos plans.

J'espère que cela vous donne les précisions nécessaires.

Le sénateur Dalphond : Je comprends : le chiffre de 800 s'étendait sur deux exercices plutôt que sur un seul.

Mme Xavier : Exactement.

Le sénateur Dalphond : Cela permet de ramener le taux à 5 %; je comprends.

En ce qui concerne la technologie, mon collègue le sénateur Moreau y a fait allusion : le gouvernement a prouvé qu'il n'était pas le meilleur gestionnaire des coûts associés aux nouvelles technologies; vous travaillez dans la super nouvelle technologie. Qu'est-ce qui nous garantit que vous faites mieux que le reste du gouvernement?

Mme Xavier : Je ne voudrais pas dire qu'il n'y a jamais de risques et je ne peux pas vous garantir que l'on ne fera pas d'erreurs. Nous sommes une organisation qui est toujours en mode apprentissage, et nous essayons d'apprendre de plusieurs autres et de leur mise en œuvre pour être en mesure de nous améliorer.

Cela dit, j'ai un grand nombre d'employés très brillants dans le domaine des technologies, des gens très créatifs, habiles et innovateurs. Donc, je suis confiante, surtout parce que nous donnons les conseils au gouvernement sur les meilleures façons de protéger leurs systèmes et de les mettre en place pour que cela fonctionne de la bonne manière. On a également de bons experts en gestion de projets et on aime les défis. Nous allons faire de notre mieux.

Je ne voudrais pas vous laisser l'impression que l'on ne va pas apprendre des choses; on en apprend déjà de nos homologues internationaux en examinant la façon dont ils mettent en place certaines techniques; cela nous permet d'apprendre comment on peut faire les choses nous-mêmes d'une meilleure façon.

Senator Dalphond: How do you share this type of information with others? If Treasury Board audits you, they aren't able to supervise the costs themselves.

I hope you can compare technologies with your international counterparts and see what they're worth.

Ms. Xavier: Yes, in fact, we work closely with the Five Eyes, but we also learn from colleagues in France, for example, since we're diversifying our international partners.

I can tell you that I work very closely with my counterparts at Treasury Board and at Shared Services Canada.

The three of us make sure we're on the same page in terms of giving advice and implementing major upcoming projects.

The Chair: We had scheduled an hour with you, but you can see how interested and enthusiastic we are about this. We have time to continue and even go to a second round. Are you on a tight schedule?

Ms. Xavier: We do have other commitments. That said, I see the interest you have. If you don't mind, I would recommend that we finish the first round and then be on our way.

The Chair: You'll allow us another 15 or 20 minutes?

Ms. Xavier: Yes.

The Chair: Thank you.

[*English*]

Senator MacAdam: Thank you for being here. As part of the government's new strategic approach to defence and security, the Prime Minister announced that the government would establish the Bureau of Research, Engineering and Advanced Leadership in Innovation and Science, or BOREALIS. This commitment was also outlined in the Liberal platform, which describes its purpose as ensuring:

> . . . the Canadian Armed Forces and Communications Security Establishment have the made-in-Canada innovation solutions they need in areas such as AI, quantum computing, cybersecurity, and other advanced research and technology.

I wonder if you are able to provide more information on BOREALIS and how it will support your work. I understand that

Le sénateur Dalphond : Comment partagez-vous ce type d'information avec d'autres? Si c'est le Conseil du Trésor qui vous vérifie, ils ne sont pas en mesure de superviser les coûts eux-mêmes.

J'espère qu'avec vos homologues internationaux, vous pouvez comparer ces technologies et voir ce que cela vaut.

Mme Xavier : En effet, on travaille étroitement avec la collectivité des cinq surtout, mais en en apprenant auprès d'autres collègues, comme les Français par exemple, parce qu'il y a une diversification de partenaires internationaux.

En effet, je pourrais vous dire que je travaille de très près avec mon homologue du Conseil du Trésor ainsi que mon homologue de Services partagés Canada.

Tous les trois ensemble, nous nous assurons d'être sur la même longueur d'onde quant à la mise en place de nos conseils et la mise en œuvre des gros projets à venir.

Le président : Nous avions prévu une heure avec vous, mais voyez l'intérêt et la passion que nous avons pour ce domaine. Nous avons du temps pour continuer et même pour faire un deuxième tour. Votre temps est-il compté?

Mme Xavier : C'est sûr que nous avons d'autres engagements. Cela dit, je reconnais qu'il y a un intérêt. Je recommande, si vous êtes d'accord, que nous finissions le premier tour et de là, nous pourrions partir.

Le président : Donc, vous nous permettez encore un autre 15 à 20 minutes?

Mme Xavier : Oui.

Le président : Merci.

[*Traduction*]

La sénatrice MacAdam : Je vous remercie de votre présence. Dans le cadre de la nouvelle approche stratégique du gouvernement en matière de défense et de sécurité, le premier ministre a annoncé la création du Bureau de la recherche, de l'ingénierie et du leadership de pointe en sciences. Cet engagement a également été énoncé dans la plateforme électorale du Parti libéral, qui décrit son objectif comme étant de doter :

> ... les Forces armées canadiennes et le Centre de la sécurité des télécommunications de solutions d'innovation conçues au Canada, dans les domaines tels que l'intelligence artificielle, l'informatique quantique, la cybersécurité et d'autres secteurs de recherches et technologies de pointe.

Pourriez-vous nous donner plus de renseignements à propos de ce bureau et de la manière dont il vous appuiera dans votre

you cannot provide many details, but anything that you could provide would be useful.

Ms. Xavier: I will turn this question over to Ms. McDonald because as part of her duties. She also owns the Tutte Institute for Mathematics and Computing, which is our research and development institute.

Ms. McDonald: Thank you for the question. I will not speak directly to BOREALIS itself, but what I can say, as the chief mentioned, we do have our own research teams within CSE. The most well known is the Tutte Institute, which does a lot of the foundational math that is required to encrypt the code-breaking and code-making that our equipment requires, as does much across Canada. They also do a lot of data science work that then helps us be experts in the domain of artificial intelligence and other emerging technologies.

Those researchers are working both in classified spaces within our organization and then in unclassified spaces for those across the country. Then we are pulling that information and research and sharing it with our Five Eyes partners and other groups, such as the Canadian AI Safety Institute.

Through that work and through the work happening, as you would have heard in the announcement the Prime Minister made last week with the Defence Industrial Strategy, we know that much of what we need related to research and development, as well as to create industry in Canada, will require different partnerships.

Programs such as BOREALIS, as they unfold, we recognize will be very positive developments because we can't do this by ourselves internal to government. We have learned a lot through our partnership work with others, and those challenges include having spaces across Canada to work in secure physical spaces, as well as having personnel going through security processes. We want to work and partner with researchers specifically in the defence and security intelligence space who are cleared and we know have Canada's best interests at heart.

We also need to ensure that those institutions and individuals we are working with have cybersecurity protections on the system so that our intellectual property and economic prosperity in Canada are protected. As the Defence industrial base and BOREALIS are developed, we are excited to see those elements addressed so that we can further work with industry and academia in Canada.

travail? Je comprends que vous ne pouvez pas donner beaucoup de détails, mais toute information que vous pourriez nous fournir serait utile.

Mme Xavier : Je vais demander à Mme McDonald de répondre à cette question, car cela fait partie de ses fonctions. Elle est également responsable de l'Institut Tutte pour les mathématiques et le calcul, notre institut de recherche et de développement.

Mme McDonald : Je vous remercie de la question. Je ne parlerai pas directement du Bureau, mais comme la chef l'a mentionné, je peux vous dire que nous avons nos propres équipes de recherche au sein du CST. La plus connue travaille à l'Institut Tutte et effectue une grande partie des mathématiques fondamentales nécessaires au chiffrement du décodage et du codage qu'exigent nos équipements et de nombreux autres partout au pays. Les chercheurs de l'Institut effectuent également de nombreux travaux en science des données qui nous permettent d'être des spécialistes dans le domaine de l'intelligence artificielle et d'autres technologies émergentes.

Ces chercheurs travaillent à la fois dans des écosystèmes classifiés au sein de notre organisation et dans des écosystèmes non classifiés partout au pays. Nous recueillons les renseignements et les résultats de leurs recherches et les transmettons à nos partenaires du Groupe des cinq et d'autres groupes, comme l'Institut canadien de la sécurité de l'intelligence artificielle.

Comme vous l'avez appris la semaine dernière lorsque le premier ministre a présenté la stratégie industrielle de défense, nous aurons besoin, à bien des égards, de différents partenariats dans le domaine de la recherche et du développement et celui de la création d'industries au Canada.

Nous reconnaissons que des initiatives comme la création du Bureau de la recherche sont d'excellentes nouvelles, car nous ne pouvons pas faire tout ce travail tout seuls au sein du gouvernement. Nous avons beaucoup appris en travaillant avec d'autres partenaires. Il existe toutefois des défis, notamment la nécessité de disposer d'espaces de travail sécurisés partout au Canada et l'exigence selon laquelle les membres du personnel doivent obtenir une habilitation de sécurité. Nous voulons travailler et établir des partenariats avec des chercheurs dans le domaine du renseignement en matière de défense et de sécurité qui ont obtenu une habilitation de sécurité et qui ont à cœur les intérêts du Canada.

Nous devons également nous assurer que les institutions et les personnes avec lesquelles nous travaillons utilisent des systèmes assortis de mesures de protection en matière de cybersécurité afin de protéger notre propriété intellectuelle et la prospérité économique du Canada. Nous sommes impatients de voir ces éléments pris en compte dans l'établissement de la base industrielle de défense et du Bureau de recherche, afin de

Ms. Xavier: If you would permit, I would add that in the cybersecurity space especially, we are world class known for the technologies and expertise we bring. That is sovereign owned and sovereign created. Those will remain in the world-class space that we're in.

Senator MacAdam: I want to revisit a question asked by Senator Marshall when your organization appeared before our committee on the Main Estimates last October. Her question was around critical infrastructure and the energy sector.

An official testified that your cyber centre is constantly engaging with the energy sector across all levels, that you share threat information in real time and that energy providers are a high priority for your organization. The Prime Minister's mandate letter to ministers describes that Canada will need to build an enormous amount of new infrastructure at speeds not seen in generations, including to support Canada in becoming an energy superpower.

Can you outline how your funding will enable you to support this new growth and the system protecting the energy sector?

Ms. Xavier: Thank you for the question. To build on the comment you made, we already have great relationships with many sectors related to critical infrastructure, energy being one of those sectors. We regularly meet with energy sector experts, both with what we call their chief information security officers as well as their chief executive officers, in a way to ensure that they have a good understanding of the cyber-threats. We meet with them in a way that we can also share with them classified material because some of them have been security cleared. We do that in a way that enables us to go both ways.

The other thing with the launch of the National Cyber Security Strategy, We are also launching what we call the Canadian Cyber Defence Collective, or CCDC. That will permit the ability to have this governance that brings in various sectors of importance, like the energy sector but not only the energy sector. It is a governance we are going to be able to co-chair with Public Safety because Public Safety is the policy arm when it comes to cybersecurity, while we're the operational arm. We are jointly working with these various sectors and continuing to raise their cyber understanding and cyber resilience.

pouvoir poursuivre notre collaboration avec l'industrie et le milieu universitaire au Canada.

Mme Xavier : Si vous me le permettez, j'ajouterais que dans le domaine de la cybersécurité, plus précisément, nos technologies et notre expertise sont reconnues comme étant de calibre mondial. Elles sont détenues et créées par l'État. Elles conserveront cette renommée.

La sénatrice MacAdam : J'aimerais revenir sur une question que la sénatrice Marshall a posée lorsque des représentants de votre organisation ont comparu devant notre comité au sujet du Budget principal des dépenses en octobre dernier. Sa question portait sur les infrastructures essentielles et le secteur de l'énergie.

Lors de son témoignage, un fonctionnaire a déclaré que votre Centre pour la cybersécurité collabore en permanence avec des partenaires de tous les niveaux du secteur de l'énergie, que vous partagez des renseignements sur les menaces en temps réel et que les fournisseurs d'énergie sont une priorité pour votre organisation. La lettre de mandat que le premier ministre a envoyée aux ministres indique que le Canada devra construire de nombreuses nouvelles infrastructures à un rythme sans précédent depuis des générations, notamment pour contribuer à faire du Canada une superpuissance énergétique.

Pouvez-vous nous expliquer comment les fonds qui vous sont alloués vous permettront de soutenir cette croissance et le système qui protège le secteur de l'énergie?

Mme Xavier : Merci pour cette question. Pour ajouter à votre observation, je dirais que nous entretenons déjà d'excellentes relations avec de nombreux secteurs liés aux infrastructures essentielles, dont celui de l'énergie. Nous rencontrons régulièrement des spécialistes du secteur de l'énergie, tant les agents principaux de la sécurité de l'information que les directeurs généraux, afin de nous assurer qu'ils comprennent bien les cybermenaces. Nous les rencontrons de manière à pouvoir également leur communiquer de l'information classifiée, car certains d'entre eux ont une attestation de sécurité. Nous procédons ainsi pour qu'il puisse y avoir des échanges.

Par ailleurs, en plus de la Stratégie nationale de cybersécurité du Canada, nous lançons ce que nous appelons le Collectif canadien pour la cyberdéfense, ou CCCD. Nous pourrons ainsi avoir une gouvernance qui réunit des acteurs de divers secteurs importants, comme celui de l'énergie, mais aussi d'autres secteurs. Dans ce cadre, notre organisme sera en mesure d'agir à titre de coprésident avec Sécurité publique Canada, car c'est ce ministère qui est responsable de l'élaboration des politiques en matière de cybersécurité, tandis que notre organisme est chargé des opérations. Nous travaillons conjointement avec les différents secteurs et nous continuons de les aider à améliorer leur compréhension de la cybersécurité et leur résilience en la matière.

Many of them are what we call subscribers to our services, where they get automatic alerts on anything that we know with regard to cyber that we can share. We have ways in which we can communicate with them at a higher security level, so there are a myriad of ways we are able to connect with partners.

We have been working hard since the creation of the cyber centre, and even before, which is now over six years old, where we have been building these partnerships. This past year, to the point you made around the Mains Estimates of last year, we had made a conscious effort. We saw, based on the learnings from the war in Ukraine, how the energy sector, in particular, was being targeted. To be able to continue to have Canada ready and resilient, we wanted to ensure we were really targeting that sector.

Senator Kingston: Building on Senator MacAdam's question, the Communications Security Establishment's annual report from 2023-24 states that CSE works with other federal partners, and you have spoken about them throughout this hour or so — CSIS, the RCMP and Global Affairs Canada — on several files. I would like to ask a couple of questions.

Is the intelligence you gather shared with your federal partners, those I mentioned? In what form is the information provided by CSE integrated in the screening program or screening report from partner organizations to other organizations, such as Immigration, Refugees and Citizenship Canada? That is an extra organization. How do you interact? What do you provide to them?

Ms. Xavier: As mentioned, as the foreign signals intelligence organization for Canada, the intelligence we provide — its intent linked to the intelligence priorities provided by the Government of Canada — is to permit decision makers to make decisions. All the partners that you mentioned have access to intelligence either in an electronic way or via the use of what we call our client relationship officers, where they are physically brought intelligence, and that intelligence is taken back so we can track where it has gone, for example.

Most of those partners, especially CSIS, the RCMP and Global Affairs, are able to access the intelligence by electronic means because that is how we ensure that our intelligence gets to decision makers in a timely way. That includes the Department of Immigration, Refugees and Citizenship Canada. We are not specifically sending them intelligence that says, "Use this intelligence for X applicant." How they use the intelligence is a better question directed to them.

Beaucoup d'entre eux sont ce que nous appelons des abonnés à nos services. Ils reçoivent automatiquement des alertes sur tout ce que nous savons en matière de cybersécurité que nous pouvons transmettre. Nous avons des moyens de communiquer avec eux à un niveau de sécurité plus élevé, ce qui nous offre une multitude de façons d'entrer en contact avec nos partenaires.

Depuis la création du centre pour la cybersécurité, qui a maintenant plus de six ans, et même depuis plus longtemps, nous travaillons d'arrache-pied pour établir ces partenariats. Pour revenir à ce que vous avez souligné au sujet du Budget principal des dépenses de l'an dernier, nous avons fait des efforts délibérés au cours de la dernière année. Nous avons constaté, à la lumière des enseignements tirés de la guerre en Ukraine, de quelle manière le secteur de l'énergie était particulièrement visé. Afin que le Canada demeure prêt et résilient, nous voulions nous assurer que nous ciblions vraiment ce secteur.

La sénatrice Kingston : En continuité avec la question de la sénatrice MacAdam, dans le rapport annuel du Centre de la sécurité des télécommunications 2023-2024, on indique que le CST collabore avec d'autres partenaires fédéraux, dont vous avez parlé tout au long de cette heure — à savoir le SCRS, la GRC et Affaires mondiales Canada —, dans plusieurs dossiers. J'aimerais poser quelques questions.

Les renseignements que vous recueillez sont-ils transmis à vos partenaires fédéraux, ceux que j'ai mentionnés? Sous quelle forme l'information fournie par le CST est-elle intégrée dans le programme de filtrage ou dans les rapports de filtrage d'organisations partenaires pour d'autres organisations, telles qu'Immigration, Réfugiés et Citoyenneté Canada? Il s'agit d'une autre organisation. Comment interagissez-vous? Que leur fournissez-vous?

Mme Xavier : Comme on l'a mentionné, en tant qu'organisme chargé de recueillir du renseignement électromagnétique étranger pour le Canada, le CST fournit des renseignements — l'objectif est lié aux priorités en matière de renseignement établies par le gouvernement du Canada — qui visent à permettre aux décideurs de prendre des décisions. Tous les partenaires que vous avez mentionnés ont accès aux renseignements, soit par voie électronique, soit par l'intermédiaire de nos agents de relations avec la clientèle, qui leur transmettent physiquement les renseignements, lesquels sont ensuite rapportés afin que nous puissions suivre leur parcours, par exemple.

La plupart de ces partenaires, en particulier le SCRS, la GRC et Affaires mondiales Canada, peuvent accéder aux renseignements par voie électronique, car c'est ainsi que nous nous assurons que nos renseignements parviennent aux décideurs en temps opportun. Cela vaut aussi pour le ministère de l'Immigration, des Réfugiés et de la Citoyenneté. Nous ne leur envoyons pas spécifiquement des renseignements en leur disant « utilisez ces renseignements pour le demandeur X ». Il serait

Having said that, for a person to access the intelligence they access from us, they have to have the necessary clearance and the "need to know" to access that intelligence. Those are the principles that frame how intelligence is disseminated: that individual has the necessary indoctrinations, classification, security screening as well as the need to know to be able to make that decision.

Senator Kingston: The "need to know" brings me back to an extra question I have. We were talking about how you ensure that all your thousands of employees are remaining secretive about the work they do.

You must have levels within your organization. I worked in health care, and very often we used information on a need-to-know basis. Can you describe the layers you have in your organization in that way?

Ms. Xavier: That is exactly right. The majority of our employees come in with what we call an enhanced top secret. In coming in with an enhanced top secret, to a fundamental level you may have access to a certain level of documents that allow you to read intelligence at that classification. But even being able to have access to that intelligence has to be because it is something you require to do your duties or a part of your job. You cannot just have access to it because you have a classification that is a top secret clearance.

Under that we have various other subcategories. One can have what we call gamma or more compartmentalized versions of access of intelligence. Every level requires you to be indoctrinated. With that, we document all of that indoctrination to know whether someone should continue to have that indoctrination. If I were to leave a particular section of my area within my agency that no longer requires me to have a particular indoctrination, you are de-indoctrinated and no longer have access, despite the fact that you may still be an employee of the agency.

The way we take care of how we classify our data, our intelligence, to begin with, and then who has access, is something that we have care and rigour with because we are protecting Canada's intelligence, but also the intelligence of partners who entrust us to ensure that we classify and protect that information effectively. Ultimately, when I am impacting that, I am impacting many others.

Senator Kingston: Do you audit that? Do you not watch your employees but do random checks to ensure people are working on a need-to-know basis?

préférable de leur demander directement comment ils utilisent les renseignements.

Cela dit, pour qu'une personne puisse accéder aux renseignements dont nous disposons, elle doit posséder la cote de sécurité nécessaire et avoir besoin de connaître l'information. Tels sont les principes qui régissent la façon dont les renseignements sont diffusés : endoctrinements, classification, filtrage de sécurité et besoin de connaître l'information.

La sénatrice Kingston : Le principe du besoin de connaître me ramène à une autre question que je me pose. Nous parlions de la manière dont vous vous assurez que vos milliers d'employés restent discrets au sujet de leur travail.

Il doit y avoir des niveaux au sein de votre organisation. J'ai travaillé dans le secteur de la santé et, très souvent, nous utilisions les renseignements selon le principe du besoin de connaître. Pouvez-vous décrire les niveaux qui existent dans votre organisation?

Mme Xavier : C'est tout à fait exact. La majorité de nos employés sont embauchés avec ce que nous appelons une cote de sécurité Très secret approfondie. Avec cette cote de sécurité, vous pouvez, à un niveau fondamental, avoir accès à certains documents qui vous permettent de lire des renseignements classifiés à ce niveau. Or, si vous avez accès à ces renseignements, c'est parce que vous en avez besoin pour accomplir vos tâches ou dans le cadre de votre travail. Vous ne pouvez pas y avoir accès simplement parce que vous disposez d'une cote de sécurité de niveau très secret.

Ensuite, nous avons diverses autres sous-catégories. Il existe des versions plus compartimentées de l'accès au renseignement, par exemple. Chaque niveau nécessite un endoctrinement. Nous consignons le tout afin de savoir si une personne doit toujours avoir cet endoctrinement. Si je devais quitter un service au sein de mon organisme et que je n'avais plus besoin d'un endoctrinement particulier, je serais désendoctrinée et je n'aurais plus accès aux renseignements, même si j'étais toujours une employée de l'organisme.

Nous sommes rigoureux quant à la manière dont nous classifions nos données et nos renseignements, tout d'abord, puis dont nous contrôlons qui y a accès, car nous protégeons les renseignements du Canada, mais aussi ceux de nos partenaires qui nous confient la tâche de classifier et de protéger l'information de façon efficace. En fin de compte, si j'ai une incidence là-dessus, j'en ai une sur bien d'autres choses.

La sénatrice Kingston : Faites-vous des vérifications? Effectuez-vous des contrôles aléatoires pour vous assurer que les gens travaillent dans le respect du principe du besoin de connaître?

Ms. Xavier: Yes. We are a highly digital organization and have automated systems that help us to understand the logging of whom has access to what.

For example, when an investigation occurs, we clearly know who had access or who even printed a document. It is to that level of detail.

Yes, a part of the job is we have compliance individuals who do exactly that and confirm whether the right people had access for whatever information they had access to.

[*Translation*]

The Chair: You mentioned recruitment. Your field could be very attractive to young people, since you deal with matters related to the nation, defence, security and patriotism. You're an employer of choice, and young people are drawn to that.

I know the salaries, and some of them are more than what the Prime Minister of Canada makes. A young person of 32, for example, would find that appealing.

Is there anything in your pay scales or classifications that would allow you to go after these young people and offer them salaries that are competitive with other organizations?

It's one thing to get 10,000 résumés per year, but they won't all be top-notch, even though we have a very good rating system. Do you use headhunters to identify the whiz kids and approach them before they come knocking?

Ms. Xavier: Thank you for the question. Yes, there are many people who show interest and join us directly, but we also reach out to them. Last year, we made over 100 recruitment efforts across the country. When we look for employees, we don't just stay within the national capital region. Of course, when someone joins our ranks, we're not able to pay them exactly what the private sector offers. However, I can tell you that our organization's work and its mission, the patriotism you mentioned and the fact that we can do really interesting things that would be technically illegal anywhere else are all major draws. We apply strict rules when recruiting talent. We test them to make sure they have the required skills. After they are recruited and come to work with us, they develop their talent.

The fear I sometimes have as chief is losing them to other organizations. They're so happy with the way we help them develop their talent that we lose them, because they'll be better paid elsewhere. Most of our employees are very passionate. They

Mme Xavier : Oui. Le CST est une organisation hautement numérique. Nous disposons de systèmes automatisés qui nous aident à comprendre qui a accès à quoi.

Par exemple, lorsqu'une enquête a lieu, nous savons avec précision qui a eu accès à un document ou même qui l'a imprimé. Le niveau de détail est très élevé.

Oui, une partie du travail consiste à avoir des responsables de la conformité qui font exactement cela et qui vérifient si les bonnes personnes ont eu accès aux renseignements auxquels elles devaient avoir accès.

[*Français*]

Le président : Vous parlez de recrutement. Vous êtes dans un domaine qui peut être très attirant pour les jeunes, car vous traitez de dossiers liés à la nation, à la défense, à la sécurité et au patriotisme. Vous êtes un employeur de choix, donc c'est attirant.

Je connais les salaires, et il y a des salaires qui sont plus élevés que celui du premier ministre du Canada. C'est intéressant pour des jeunes de 32 ans, par exemple.

Avez-vous des barrières ou des éléments dans vos échelles salariales ou vos classifications qui permettent d'aller chercher ces jeunes et de leur offrir des salaires qui se comparent bien avec ceux de la compétition?

On a beau recevoir 10 000 curriculum vitæ par année, ce ne sont peut-être pas tous des premiers de classe, même si on a un très bon système de classement. Utilisez-vous aussi des chasseurs de têtes pour identifier les stars et aller les chercher, sans attendre qu'ils viennent frapper à la porte?

Mme Xavier : Merci de votre question. Oui, on a beaucoup de gens qui montrent leur intérêt et qui se joignent directement à nous, mais nous allons aussi les chercher. L'an dernier, on a fait au-delà de 100 efforts de recrutement à travers le pays. On ne reste pas seulement dans la région de la capitale nationale pour aller chercher nos employés. C'est sûr quand une personne rejoint nos rangs, on n'est peut-être pas capable de payer exactement ce que le secteur privé pourrait offrir. Cependant, je peux vous dire que le travail et la mission au sein de notre organisation, le patriotisme dont vous avez parlé, le fait qu'on puisse faire des choses vraiment intéressantes qui seraient techniquement illégales ailleurs, c'est un attrait très important. On s'assure d'être rigoureux dans le recrutement des talents. On fait des tests pour essayer de confirmer qu'ils ont le talent recherché. De plus, lorsqu'ils sont recrutés et travaillent avec nous, ils développent leur talent.

Je dirais que la crainte que j'ai en tant que chef, c'est de les perdre parfois au profit d'autres organismes. Ils sont tellement contents de ce qu'on leur a permis de développer comme talent que je les perds, car ils seront mieux payés ailleurs. La plupart de

understand the mission. They want to deliver on that mission for Canada and Canadians. That's why we continually remind them why we are here and what Canada's mission is.

We work very hard to give them a welcoming environment and give them room for creativity. That gives them a chance to do unique things that they can't do in other systems outside the government. In terms of salary, we are a separate employer with an allocation beyond what a regular department can offer. That's another draw. Even with that, we can offer slightly more than what a regular government employee is paid, but not as much as Google or Microsoft can offer them. However, our employees are proud to work with us.

The Chair: I imagine you have contracts with large companies that provide cybersecurity, for example. I won't name them, since I understand that might be classified information. I imagine that there are non-disclosure clauses for your staff?

Ms. Xavier: Absolutely. We have non-disclosure provisions in our contracts. That said, we don't have a ton of contracts with consultants to do the same type of work that we do. We're the experts. That's why it's sometimes the opposite: They recruit us to fulfill their needs. We work closely with a lot of industries. We try to be complementary. Part of the CSEC's mission and vision is to stay within our field, one in which no one else should or could work. That's one way of distinguishing ourselves from the private sector.

The Chair: Thank you.

[*English*]

I forgot Senator Pate. Sorry, senator.

Senator Pate: I have two questions. First, it was revealed earlier this year that CSE's Canadian Centre for Cyber Security was defrauded by nearly $330,000 as part of an IT overbilling fraud campaign.

In your 2023-24 annual report, the CSE noted that it has implemented a new cybersecurity certification required for all defence procurement contractors, and in the supplementary estimates it indicates that you are seeking $370 million as a part of a $550 million horizontal initiative with the Department of National Defence. The funds are needed, it says, for digital tools and capabilities.

nos employés sont très passionnés. Ils comprennent la mission. Ils veulent livrer la mission pour le Canada et les Canadiens. C'est pour cela que nous continuons de leur rappeler pourquoi nous sommes là et quelle est la mission du Canada.

On travaille très fort pour faire en sorte que l'environnement soit accueillant et leur donne la possibilité d'être créatifs. Cela leur donne l'occasion de faire des choses uniques que les autres systèmes qui existent à l'extérieur du gouvernement ne peuvent pas faire. Du point de vue du salaire, nous sommes un employeur séparé, nous avons ce qu'on appelle une allocation au-delà de ce qu'un ministère ordinaire pourrait offrir. C'est un autre attrait. Même pour cela, on est une coche au-dessus de ce qu'un employé régulier du gouvernement pourrait obtenir, mais peut-être pas une coche plus élevée que ce que Google ou Microsoft pourraient leur offrir. Cependant, nos employés sont fiers de travailler avec nous.

Le président : J'imagine que vous avez des contrats avec de grandes firmes qui font, par exemple, de la cybersécurité. Je ne vais pas les nommer, car je comprends que ce sont peut-être des éléments classifiés. J'imagine que dans les contrats, il y a des dispositions de non-divulgation pour votre personnel?

Mme Xavier : Absolument. On a des dispositions de non-divulgation dans nos contrats. Cela dit, on n'a pas une tonne de contrats qui sont liés aux consultants pour faire le même genre de travail que nous. On est les experts. C'est pour cela que c'est parfois l'inverse : ils nous recrutent parce qu'ils ont besoin de nous. On travaille de très près avec beaucoup d'industries. On essaie d'être complémentaire. Je dirais que faire partie de notre mission et de la vision du centre, c'est vraiment de continuer de rester dans notre domaine, un domaine dans lequel personne d'autre ne devrait ou ne pourrait travailler. C'est une façon d'être en mesure de se différencier du secteur privé.

Le président : Merci.

[*Traduction*]

J'ai oublié la sénatrice Pate. J'en suis désolé, sénatrice.

La sénatrice Pate : J'ai deux questions. Tout d'abord, plus tôt cette année, on a révélé que le Centre canadien pour la cybersécurité du CST a été victime d'une fraude de près de 330 000 $ dans le cadre d'une campagne de surfacturation dans les TI.

Dans son rapport annuel de 2023-2024, le CST indique qu'il a mis en place une nouvelle mesure de certification de cybersécurité pour toutes les entreprises qui souhaitent obtenir des contrats d'approvisionnement en matière de défense. En outre, dans le Budget supplémentaire des dépenses, vous demandez 370 millions de dollars dans le cadre d'une initiative horizontale de 550 millions de dollars avec le ministère de la Défense nationale. On indique que ces fonds sont nécessaires pour renforcer les outils et les capacités numériques.

I'm curious about two things. What changes have you made to your contracting processes in response to the fraud campaign, and how much of the funds proposed for this initiative will go to contractors?

My second question is: In the 2022 Auditor General's report on cyber crime, it concluded that our response to rising cyber crime was hindered by the siloed and disconnected approach of departments and agencies, and I note that Canada lags behind on dealing with money laundering and other cyber crime.

Given the rise of the threat of U.S. issues, I mean, much of what has been happening from the U.S. historically as well, are there new changes that have been made there to address that siloed approach?

Ms. Xavier: On the situation with regard to contracting, as my colleague said earlier, we do have in place what we call a contract review committee.

One of the big things that I have been focused on, going into year three since I have been chief in this role, is trying to add more controls and being able to ensure that when we are putting in contracts that we are being more rigorous in the follow-up.

We don't have a whole lot of contracts in place so there is no reason, to the point that you're making, to ensure that we are addressing that in an effective manner.

I won't go into details of exactly how the $270.1 million will be used and what number of possible contractors might make part of that. I can assure you we will have rigorous contracting mechanisms in place because of the learnings of this fraud element that was caught by the OAG.

I will hand it over to my colleague Ms. Chassé here who might have more to add, because that falls directly in her responsibility.

Ms. Chassé: In terms of fraudulent billings, we are collaborating with PSPC who, in turn, has referred that situation to the RCMP. We are actively involved in supporting the investigation over fraudulent billing. We take those matters very seriously and are fully collaborating with our federal partners.

Senator Pate: In terms of money laundering and cyber crime?

Ms. Xavier: In terms of money laundering or anything else we see in what we call the cryptocurrency space, that is very much a space we worry about when it comes to fraud or

Deux choses m'intriguent. Quels changements avez-vous apportés à vos processus de passation des marchés en réponse à la campagne de fraude, et quelle part des fonds proposés pour cette initiative ira aux entrepreneurs?

Ensuite, dans son rapport de 2022 sur la cybercriminalité, la vérificatrice générale a conclu que notre réponse à la montée de la cybercriminalité était diminuée par l'approche cloisonnée et déconnectée des ministères et des organismes. De plus, je souligne que le Canada est à la traîne dans la lutte contre le blanchiment d'argent et d'autres cybercrimes.

Étant donné la menace croissante que représentent les problèmes aux États-Unis, je veux dire, une grande partie de ce qui s'est passé aux États-Unis auparavant également, de nouveaux changements ont-ils été apportés pour remédier à cette approche cloisonnée?

Mme Xavier : Pour ce qui est de la situation concernant la passation des marchés, comme ma collègue l'a mentionné précédemment, nous avons mis en place un comité d'examen des contrats.

J'en suis à la troisième année de mon mandat et je me concentre entre autres sur une chose : essayer d'ajouter des mesures de contrôle et veiller à ce que nous soyons plus rigoureux dans le suivi lorsque nous concluons des contrats.

Nous n'avons pas beaucoup de contrats en place, de sorte qu'il n'y a aucune raison, concernant le point que vous soulevez, pour ce qui est de nous assurer que nous procédons de façon efficace.

Je n'entrerai pas dans les détails quant à l'utilisation des 270,1 millions de dollars et au nombre d'entreprises qui pourraient être touchées. Je peux vous assurer que nous mettrons en place des mécanismes de passation de marchés rigoureux, compte tenu des enseignements qui découlent de la fraude que le BVG a détectée.

Je vais maintenant céder la parole à ma collègue, Mme Chassé, qui pourra peut-être vous en dire davantage, car cela relève directement de sa responsabilité.

Mme Chassé : En ce qui concerne la facturation frauduleuse, nous collaborons avec SPAC qui, de son côté, a renvoyé le dossier à la GRC. Nous participons activement à l'enquête sur la facturation frauduleuse. Nous prenons ces questions très au sérieux et nous collaborons pleinement avec nos partenaires fédéraux.

La sénatrice Pate : Et pour ce qui est du blanchiment d'argent et de la cybercriminalité?

Mme Xavier : En ce qui a trait au blanchiment d'argent ou à tout autre phénomène observé dans ce que nous appelons l'espace des cryptomonnaies, c'est un secteur qui nous

cybersecurity. Working hand-in-glove, particularly with our RCMP colleagues, that is very much an area we are going to continue to strengthen and manage more effectively.

I would say the other opportunity we have, especially in the cryptocurrency space, because it occurs in the cyber realm, is being able to eventually use some of our foreign cyber operations to disrupt what we see as fraudulent behaviour, or networks that may be taking advantage of Canadian systems or vulnerabilities which may exist.

In keeping it the way we work with critical infrastructure, working with the finance sector to continue to raise that cyber resilience, to make sure the necessary protections are in place from a cybersecurity perspective. But, in addition, from the signals from our foreign intelligence collection, ensuring what we can do in either disrupting what could be networks that could be impacting Canada, and doing that hand-in-glove with our RCMP colleagues. That is definitely an area, as well as working with our FINTRAC partner.

Senator Pate: It is not clear to me how much of the money you have allocated in the Main Estimates will go to this work.

Ms. Xavier: Because foreign intelligence is part of our bread and butter, at the core of our business, it is becoming an ongoing priority for the government of Canada and will be part of our Mains Estimates. It wouldn't be allocated a separate line item in the budget, it would be a part of what we do in the federal intelligence collection and in the domain of our cyber security mandate already.

Senator Pate: If there's any details you can provide, I'm asking, in part, because we lag far behind even the U.S. in documenting money laundering, particularly through our main banks.

Ms. Xavier: This is where this question would be better directed to FINTRAC and the RCMP. Ultimately, we work with them, in partnership, from the foreign intelligence lens and the cyber security defence. In terms of understanding where we rank, they would be better to explain that than we would in our lane, but I will take that back for them.

préoccupe beaucoup lorsqu'on parle de fraude et de cybersécurité. En collaborant étroitement avec nos partenaires, notamment avec nos collègues de la GRC, nous allons continuer à renforcer nos processus et à gérer les choses plus efficacement dans ce domaine.

Je dirais que l'autre possibilité qui s'offre à nous, en particulier dans l'espace des cryptomonnaies, parce que cela a lieu dans le cyberespace, c'est de mener, dans le futur, des cyberopérations étrangères pour perturber ce que nous considérons comme des comportements frauduleux ou des réseaux qui pourraient profiter des systèmes canadiens ou des vulnérabilités qui pourraient exister.

Il s'agit de continuer à travailler comme nous le faisons avec le secteur des infrastructures essentielles et le secteur financier pour renforcer la cyberrésilience et veiller à ce que les mesures de protection nécessaires soient en place du point de vue de la cybersécurité. Mais, en plus, avec notre collecte de renseignements électromagnétiques étrangers, nous devons nous assurer que nous sommes en mesure de perturber les réseaux qui pourraient avoir des répercussions sur le Canada, et ce, en étroite collaboration avec nos collègues de la GRC. C'est certainement un élément, tout comme le travail avec notre partenaire, le CANAFE.

La sénatrice Pate : Je ne sais pas exactement quelle part des fonds dans le Budget principal des dépenses sera consacrée à ce travail.

Mme Xavier : Étant donné que le renseignement étranger fait partie intégrante de nos activités, cela devient une priorité permanente pour le gouvernement du Canada et cela fera partie du Budget principal des dépenses. Il ne s'agirait pas d'un poste distinct dans le budget, mais ce serait plutôt une partie de ce que nous faisons déjà dans le cadre de la collecte du renseignement à l'échelle fédérale et de notre mandat en matière de cybersécurité.

La sénatrice Pate : Si vous pouvez nous fournir des détails, je vous le demande en partie parce que nous sommes loin derrière les États-Unis lorsqu'il s'agit de réunir l'information sur le blanchiment d'argent, en particulier par l'intermédiaire de nos principales banques.

Mme Xavier : Il serait préférable de poser cette question au CANAFE et à la GRC. Au bout du compte, nous travaillons en partenariat avec eux dans le domaine du renseignement étranger et de la défense en matière de cybersécurité. Pour ce qui est de notre classement, ils sont mieux placés que nous pour vous renseigner, mais je leur transmettrai votre question.

[*Translation*]

The Chair: Thank you for being here and providing clear, direct and precise answers. I'm impressed. We realize how important it is to have chiefs at the table. The answers we get are less hesitant, to put it kindly.

(The committee continued in camera.)

[*Français*]

Le président : Nous vous remercions de votre présence et de vos réponses claires, nettes et précises. C'est impressionnant. On se rend compte de l'importance du fait d'avoir des chefs à la table; cela nous permet d'avoir moins d'hésitations dans les réponses, pour rester polis. Merci beaucoup.

(La séance se poursuit à huis clos.)