ICANN84 | Réunion générale annuelle – Réunion conjointe : GAC et ccNSO
Mercredi 29 octobre 2025 – 10h30 à 12h00 IST

NICOLAS CABALLERO Bienvenue à tous! Nous sommes sur le point de débuter.

GULTEN TEPE Merci Nico. Bienvenue à la réunion du GAC avec la ccNSO le mercredi 29 octobre à 10 h 30, heure locale. Cette session est enregistrée et régie par les normes de conduite requises de l'ICANN, le code de conduite des participants de l'ICANN et la politique anti-harcèlement de la communauté de l'ICANN. Pendant cette session, les questions ou les commentaires ne seront lus à voix haute que s'ils sont soumis dans le format adéquat dans le chat de Zoom. Il y aura de l'interprétation dans les six langues des Nations Unies et le portugais.

Si vous souhaitez vous exprimer pendant cette session, vous pouvez lever la main dans Zoom. Dites votre nom et la langue que vous allez utiliser si ce n'est pas l'anglais. Exprimez-vous à un rythme raisonnable pour permettre une interprétation plaisir. Je donne la parole au président du GAC, Nicolas Caballero.

NICOLAS CABALLERO Merci Gulten. Bienvenue à tous et à toutes. J'ai le plaisir de vous présenter mes collègues de la ccNSO et Alejandra, la présidente de

la ccNSO, à ma droite. Cette session va être très intéressante. Je ne sais plus comment on s'est organisé à Seattle, c'est ça? L'idée est que l'on puisse participer tous activement, que l'on puisse poser des questions, que l'on puisse interagir.

Il n'y a pas de mauvaise question. Alors, avant de planter le décor et d'ailleurs, nous avons une présentation sur les cryptomonnaies et la fraude à l'investissement que Gabe Andrews du FBI va nous donner. Mais avant d'écouter la présentation de Gabe, je vais donner la parole à Alejandra qui va nous donner quelques points d'intendance, notamment quant à la façon dont la session du jour sera organisée. Alejandra, à toi la parole!

ALEJANDRA REYNOSO Merci Nico. C'est un plaisir que de vous rejoindre ici au GAC et d'éprouver ces différentes méthodologies en votre compagnie. C'est toujours très productif. Alors, avant que l'on passe à l'interaction, je propose que l'on donne la parole à Gabriel et ensuite, on passera à la suite.

NICOLAS CABALLERO Merci Alejandra. Je donne la parole à Gabe Andrews du FBI. Gabe, à toi la parole.

GABRIEL ANDREWS Merci Nico, merci Alejandra. Alors passons à la prochaine planche. J'aimerais vous parler de la principale catégorie de cybercrimes signalés auprès du FBI. Il s'agit de fraudes à l'investissement par le

biais de la cryptomonnaie. On parle également de pig butchering en anglais. Nous espérons que cette présentation vous permettra d'éclairer davantage vos efforts de lutte contre l'utilisation malveillante du DNS.

Tout cela a débuté pendant le Covid. C'est une des nombreuses mauvaises choses qui a émané du Covid. Donc, il y avait des organisations criminelles du sud-est de l'Asie qui géraient des hôtels dans la région, mais pendant le Covid, il n'y avait plus de sources de revenus. Donc ils ont exploré d'autres méthodes pour dégager des revenus.

Donc, ils ont tenté d'attirer des migrants. Une fois les migrants arrivés, ils ont été réduits en esclavage et mis au travail pour escroquer des Occidentaux. Et donc le volet esclavagisme est très important.

Dans cette présentation, on va évoquer quelques-uns des gros titres des journaux, puis également un rapport des Nations Unies sur ces régimes de fraude à la cryptomonnaie a été publié. Ces sept derniers jours, l'Armée du Myanmar a organisé un raid sur l'un de ces camps de travail forcé.

SpaceX a coupé les services Starlink pour certains de ces camps de travail forcé au Myanmar. La semaine dernière également, le ministère de la Justice aux Etats-Unis a saisi plus de 15 milliards de dollars en bitcoins, résultant d'un seul de ces efforts de fraude. C'est l'une des plus grandes saisies du FBI depuis toujours.

Alors, comment cela fonctionne-t-il? Donc, il y a de l'hameçonnage. C'est le début de cette escroquerie. Mais ce n'est pas par voie électronique. Ce n'est pas par courriel. C'est plutôt par le biais de réseaux sociaux, de SMS ou de sites de rencontres. Vous recevrez un message qui vous invite à débuter une conversation. Souvent, vos interlocuteurs vont faire valoir qu'ils sont intéressés par une relation amicale, romantique ou un investissement commercial, mais toute la relation débute à vitesse mesurée. Le volet travail forcé/esclavagisme permet aux brouteurs de prendre leur temps.

La suggestion d'investissement ne survient qu'après une longue phase initiale de conversation. Ce n'est pas un simple courriel bien rédigé, c'est plutôt un processus d'hameçonnage qui est élaboré au fil de semaines et qui va tenter de convaincre la personne arnaquée. Et cela est simplement possible d'avoir autant de temps, car les personnes qui font ces escroqueries sont réduits en esclavage. Et ce travail ne représente pas un coût pour les criminels.

Le volet domaine est important ici, car lorsqu'on a finalement hameçonné une victime et que l'on parle de l'investissement qui soi-disant va beaucoup rapporter, il y aura un lien qui sera fourni vers une plateforme d'échange de cryptomonnaie.

Ces liens sont enregistrés en groupe. Donc on va parler d'accès API aux enregistrements groupés de noms de domaine. Et les criminels utilisent ce type d'approche. Donc ils enregistrent des centaines, voire des milliers de noms de domaines qui usurpent ces

plateformes d'échange de cryptomonnaies. Et lorsqu'ils mettent en place l'infrastructure. Je m'excuse. Par ailleurs, les caractères sont assez petits.

Mais alors, que se passe-t-il? À gauche, dans les rectangles rose et violet, il y a des noms de domaine qui ne sont utilisés que pendant trois mois. S'il y en a un qui est découvert, ils passent au suivant, car ils ont tellement de noms de domaines qu'ils peuvent choisir. Mais ils utilisent une technique qui s'appelle le CNAME forwarding, ou plutôt l'ajustement du nom canonique de ces noms de domaine. Et donc ils peuvent faire en sorte que le nom de domaine route vers un autre domaine, puis un autre domaine pour ensuite arriver sur le site d'échange de cryptomonnaie.

Et tout cela permet de garder le nom de domaine similaire qui est dans la fenêtre du navigateur. Mais tout cela va passer par différentes étapes. Je sais évidemment que tout le monde ne connait pas forcément la question des paramètres des noms canoniques, mais je sais que certains d'entre vous ici le savent, surtout si vous connaissez les ccTLD. Donc, je voulais que vous connaissiez cette tactique du CNAME Forwarding afin que si vous la rencontriez, vous sachiez ce que c'est.

Lorsque les enquêteurs se sont penchés sur cette question, ils se sont rendu compte qu'il était plus difficile d'approfondir l'infrastructure criminelle à cause de cette tactique. Donc, ils font cela pour deux raisons. C'est plus dur pour les enquêteurs et ça leur permet également de très rapidement utiliser les noms de domaine

enregistrés en groupe, tout en gardant un plus petit volume de nom de domaine réel et bien protégé.

Donc pour ce qui est de notre débat aujourd'hui, je voulais vous parler de cette fraude et je voulais vous demander si à la ccNSO, vous constatez les mêmes évolutions. Je sais que pour les gTLD, le .com, le .top, le .info, je n'ai pas une très grande visibilité là-dessus.

Mais je pense que oui, ils utilisent également des ccTLD pour le gTLD. Ils l'utilisent, c'est certain. Donc peut-être que différents groupes de criminels utilisent également ces infrastructures. Donc c'est une des questions que j'ai à vous poser, c'est vous demander s'il y a des rapports qui signalent des enregistrements groupés de sites de cryptomonnaies ou s'il y a cette technique du CNAME forwarding que vous pouvez constater.

Par ailleurs, nous allons également parler de l'élaboration de politiques dans le cadre des gTLD à l'ICANN. On peut envisager des politiques liées au contrôle des noms de domaine associés. Peut-être que vous recevez un signalement à propos d'un nom de domaine, et dans ce cas-là, il y aurait l'obligation de se pencher sur les autres noms de domaine enregistrés en même temps. Et s'il y a enregistrement groupé ou s'il faut une politique distincte pour le contrôle d'accès aux enregistrements groupés, tels que les API qui leur permettent de faire de tels enregistrements groupés. Je me demandais si la ccNSO avait des expériences qui les poussaient à se pencher sur de telles politiques.

Donc voilà, je pense que j'ai utilisé le temps qui m'était imparti. Je veux vous remercier de votre attention. Et je suis ravi de constater que tout le monde, de par le monde, réagit à cette escroquerie. Et je suis ravi d'écouter ce que vous avez à dire. Merci.

NICOLAS CABALLERO Merci beaucoup, Gabe. Eh bien, voici les questions qui nous sont posées. C'est particulièrement important pour les opérateurs de ccTLD. Est-ce que vous recevez des signalements d'utilisation malveillante? En fait, des enregistrements tout à fait infondés, pour ainsi dire, aux bogues ou encore des... Vous constatez effectivement du CNAME forwarding – du transfert de nom canonique. Mais avant, je vais passer la parole à Alejandra qui va nous expliquer comment nous allons organiser cette réunion au cours de cette séance de 75 minutes. Alejandra.

ALEJANDRA REYNOSO Merci Nico et merci Gabriel pour cette présentation. Je sais que vous n'aviez pas énormément de temps. Nous allons très certainement répondre à vos questions par la suite. Mais pour la prochaine activité, comme nous l'avons déjà fait par le passé, nous voulons avoir une séance plus interactive pour que nous puissions aborder ensemble plusieurs thèmes concernant l'utilisation malveillante du DNS avec des représentants du GAC, mais aussi les représentants de la ccNSO pour comprendre différents thèmes,

notamment l'utilisation de l'intelligence artificielle dans la prévention et la détection des utilisations malveillantes.

Les défis concernant les enregistrements de noms de domaine groupés, tout à fait en lien avec ce que nous venons d'entendre. Troisième étape, les enquêtes sur les utilisations malveillantes concernant les portefeuilles de noms de domaine. Et puis, dans un quatrième temps, la prévention de la fraude. Ça, c'était pour la séance quatre. Et puis les arrangements ou les accords entre entités de notifications fiables.

Alors, sur la base de vos retours la dernière fois, vous vouliez avoir davantage de cycles de conversation ou de dialogue, mais cela veut dire qu'on aurait moins de temps. Alors cette fois-ci, ce que nous allons organiser, c'est que nous allons organiser des cycles parallèles. Une fois que vous aurez épuisé le thème, vous pouvez passer à un autre cycle, une autre table et au final, nous allons également avoir une séance récapitulative de chacun des groupes de travail, pour ainsi dire des stations comme on les appelle.

Et on y va. Voilà les différentes stations, les différentes tables qui vous sont proposées. On va de reste garder cela à l'écran, question que vous puissiez passer peut-être d'une table de conversation à l'autre. Nous allons mettre un chronomètre à l'écran. Nico, on y va?

NICOLAS CABALLERO Merci beaucoup, Alejandra. Avant de lancer les tables de conversation, les différents cycles, peu importe comment on va les

appeler. Je voulais revenir sur ce que disait Gabe et les questions qu'il posait. J'aimerais quand même recevoir quelques réactions de la part de la salle ou de la salle virtuelle, si vous le permettez, Alejandra. Avant de lancer les tables de conversation, je vous propose peut-être de consacrer cinq minutes avant d'entamer ce championnat des poids-lourds. Est-ce que peut-être il y a quelques réactions au titre des opérateurs de ccTLD ou d'extension géographique? Donc est-ce que vous avez peut-être quelque chose à ajouter sur cette pratique du CNAME forwarding, donc ce transfert du nom canonique? Alors évidemment, nous ne nous attendons pas à ce que vous soyez expert en la matière. Alejandra.

ALEJANDRA REYNOSO Oui, j'aimerais peut-être revenir sur la question qui a été lancée à la ccNSO. C'est celle-ci. Est-ce que nous entendons lancer peut-être une politique à ce sujet? Je voulais simplement rappeler que nous avons un mandat très, très limité. En fait, les politiques peuvent porter sur les fonctions IANA en matière de gestion des ccTLD, par exemple retrait de ccTLD, transferts et tout ce genre d'activités dans le cadre des fonctions IANA.

Nous n'élaborons pas de politique enjoignant aux ccTLD de faire leur travail de telle ou telle manière. Et nous avons le Comité permanent sur l'utilisation malveillante du DNS. Et bien merci à lui, parce que c'est lui qui a organisé en grande partie cette séance avec vous tous. Et en fait, ce comité permanent est en train de recueillir les meilleures pratiques pour en faire un répertoire qui

peut être partagé avec le reste du monde, pour que vous sachiez comment les ccTLD font face à ces utilisations malveillantes du DNS. Bon, voilà, ce sont des activités que nous menons qui nous permettront peut-être d'élargir encore la discussion, mais c'est tout ce que nous pouvons faire.

NICOLAS CABALLERO Merci Alejandra pour ce petit retour. Une petite minute. Alors si vous me le permettez, concernant la deuxième question posée par Gabe, quelles sont les expériences qu'ont peut-être les opérateurs de la ccNSO et surtout les opérateurs d'extension géographique? Est-ce que vous avez des expériences qui pourraient nous permettre peut-être d'alimenter le débat sur une future politique? Pas de mains levées dans la salle, dans la salle virtuelle. Bon très bien, je vous repasse la parole, Alejandra. Gabe, si vous êtes encore en ligne, merci. Merci beaucoup pour cette très, très importante présentation qui est très pertinente pour tous les membres du GAC. Alejandra, je vous rends la parole.

ALEJANDRA REYNOSO Merci. Nous reprendrons ces questions justement très certainement. Nous allons les étudier et nous reviendrons vers Gabe pour y répondre. Voilà, Mesdames et Messieurs, je vous demande de vous lever, d'aller à la table qui vous intéresse le plus. Je garde ici mon chronomètre pour ce premier cycle. Vous avez 18 minutes et ça commence maintenant.

Eh bien voilà, les temps impartis sont terminés. Je vous demande maintenant de terminer vos discussions et de changer de table. Nous reprendrons les discussions dans une minute.

Je rappelle très, très rapidement que nous allons commencer la deuxième série de discussions. Je vous demande de changer alors de table de conversation ou de poste de conversation puisque vous êtes tous debout.

Bien deux minutes. Mesdames et messieurs, il ne vous reste plus que deux minutes pour vos discussions.

Très bien. Je vous demande de conclure vos discussions. Il est temps de changer de poste ou de station de discussion. Nous allons recommencer dans une minute.

Bien, alors j'espère que vous êtes déjà à votre troisième station de conversation. Nous recommençons. Nous remettons les compteurs à zéro, voilà 18 minutes.

Donc deux minutes. Plus que deux minutes. Voilà, je vous demande maintenant de vous asseoir.

Alors, s'il vous plaît. Eh bien, pour les rapporteurs et les animateurs, je vous demande de reprendre vos places également et je demande aux autres participants de se rasseoir pour que nous puissions présenter maintenant un petit récapitulatif des discussions. Dix secondes pour reprendre place, puis nous pourrons passer au résumé.

Je pense que nous sommes prêts. Il y aura un micro baladeur qui va aller de poste en poste. Et commençons avec le poste numéro un, Utilisation de l'intelligence artificielle pour la prévention et la détection de l'utilisation malveillante du DNS. Nico.

NICOLAS CABALLERO Merci. Pour ce qui est de l'utilisation de l'IA et de l'apprentissage automatique. Dans un premier temps, nous avons expliqué avec Christian de .nl ce de quoi il retournait. Donc nous avons eu une super session. Nous avons expliqué ce qu'est l'apprentissage profond, l'apprentissage automatique, l'IA, l'IA générative, la différence entre ChatGPT, Deep Singh, Gemini, Cloud, etc. Et la façon dont les algorithmes sont utilisés à proprement parler pour détecter les menaces DNS. Le trafic DNS et toute une autre série d'éléments qui ne sont pas nécessairement liés aux grands modèles de langage ou aux IA génératives, etc.

Et des mesures afférentes. Et dans ce cas, nous avons parlé des mesures déployées par l'équipe de .nl qu'ils déploient pour lutter contre les utilisations malveillantes du DNS. De bonnes questions, de bonnes et intelligentes questions, pas seulement relatives à la technologie, mais également à la mise en œuvre, la mécanique interne et la façon dont tout fonctionne sur le plan interne. En gros, ce qui se passe sous le capot.

Très intéressant. J'espère que les participants ont également apprécié cette session interactive. Merci beaucoup à Chris et à l'équipe .nl. Voici pour mon rapport du poste un.

ALEJANDRA REYNOSO Passons au poste deux. Les défis de l'enregistrement groupé de noms de domaine avec Pete Koch et Martina Barbero.

PETER KOCH On nous a parlé d'enregistrement groupé. Ne vous inquiétez pas, nous n'avons pas défini ce qu'est l'enregistrement, mais nous avons évoqué pourquoi c'était un défi, mais en même temps que ce n'était pas si crucial comme point. Nous avons également parlé d'enregistrement automatique, et nous avons parlé également des différents types de communication entre les bureaux d'enregistrement et les opérateurs de registre. Et nous avons parlé également de soutien automatique qui pouvait être fourni, et nous avons éventuellement évoqué la possibilité de se pencher sur ce point.

MARTINA BARBERO Oui, d'excellentes questions. Mais voilà, nous avons parlé de la façon dont on peut répondre aux préoccupations liées à l'enregistrement groupé. Nous avons parlé de la tension entre l'identification et la capacité à comprendre l'intention des enregistrements groupés. Parfois, ce sont des marques qui enregistrent plusieurs domaines et dans ce cas-là, c'est légitime.

Donc quel seuil mettre, quelle réflexion apporter pour ne pas décourager les enregistrements groupés légitimes? Pour ce qui est de l'identification, on a parlé de la différence entre l'identification d'entreprises et d'organisations et l'identification d'individus. Ce sont deux pratiques différentes.

Nous avons également parlé de différentes pratiques de ccTLD avec certains opérateurs de registre qui se penchent sur des comportements suspicieux, les comportements qui sont suspicieux dans le sillage d'enregistrements groupés, ou parfois il s'agit de comportements suspicieux en amont d'un enregistrement groupé.

Puis nous avons également parlé de l'importance d'être conscient des préjudices importants qui peuvent résulter de campagnes d'hameçonnage, et ce, en très peu de temps, comme on en a parlé avec Gabe. Nous avons parlé de la réactivité qu'il faut déployer pour réagir promptement aux comportements néfastes. Évidemment, c'est nécessaire, mais ce n'est pas forcément efficace. Il faut penser également aux recours. Nous avions également beaucoup d'idées formidables qui ont été évoquées, mais on ne peut pas tout évoquer.

ALEJANDRA REYNOSO Poste trois, Enquêter sur les abus dans le cadre des portefeuilles de domaine avec Crystal et Susan.

SUSAN CHALMERS

Je représente les États Unis et le régulateur pour le domaine de premier niveau géographique .us. Je suis également avec Crystal Peterson qui gère le ccTLD .us. Alors quelques points, puis je donnerai la parole à Crystal. Notre poste? Eh bien, nous avons évoqué les futurs PDP pour les contrôles de nom de domaine associé.

Lorsque l'on reçoit un signalement d'utilisation malveillante, l'opérateur de registre du .us est la source principale d'information liée aux titulaires de noms de domaine dans la zone .us, ce qui est unique. Par ailleurs, le TLD US interdit dans sa pratique l'utilisation de services d'anonymisation et d'enregistrement fiduciaire. Donc, les données qui figurent dans la base de données sont de véritables données de titulaires de noms de domaine, ce qui nous met dans une position unique et nous permet d'atténuer les utilisations malveillantes en se fondant sur les contributions qui sont reçues. Crystal, à toi la parole!

CRYSTAL PETERSON

Bien sûr! Merci Susan. Lors de nos trois sessions, nous nous sommes penchés sur la façon dont nous, en tant qu'opérateur de registre, on pouvait détecter les noms de domaine associés ou les portefeuilles de domaine. Ce qui revient à une question posée par Gabriel Andrews au début de notre session, lorsqu'il nous a présenté la politique en matière de cryptomonnaie.

Alors Susan l'a dit, aux États-Unis, il n'y a pas de service d'anonymisation ou d'enregistrement fiduciaire qui sont autorisés.

Nous avons également une vérification de l'exactitude du WHOIS et du point de vue de l'opérateur du registre, nous nous penchons sur la façon dont on peut épauler les efforts d'atténuation de l'utilisation malveillante consentie par la communauté, afin de pouvoir identifier les domaines associés par le biais des données de contact du titulaire du nom de domaine.

Notre session a été excellente, car nous avons été en mesure d'examiner la façon dont on définit les noms de domaine associés et la façon dont on mène l'atténuation, et nous avions d'excellentes questions en la matière. Merci beaucoup.

ALEJANDRA REYNOSO Poste quatre, Cadre national pour la prévention des escroqueries et de la fraude. Bruce Tonkin et Ian Sheldon.

IAN SHELDON Alors au poste quatre, nous avons eu une formidable discussion quant aux cadres nationaux de lutte contre les escroqueries. Bruce nous a parlé de la façon dont on peut répondre aux escroqueries d'envergure nationale, donc la gouvernance, la distribution, la prévention, la détection.

En Australie, nous avons un Centre national de lutte contre l'escroquerie qui a été mis sur pied pour lutter contre ce défi. C'est en quelque sorte un guichet pour que la population puisse signaler l'escroquerie et éventuellement recevoir des propositions de résolution de leurs défis. On collabore étroitement avec l'opérateur

du ccTLD .au. Le .au agit rapidement lorsqu'ils sont alertés d'une escroquerie.

Alors, les escroqueries sont-ils une question de cybersécurité? Une question de protection des consommateurs? C'est un débat actuel en Australie. Notre Centre national de lutte contre l'escroquerie est intégré à notre commission sur la concurrence et la protection des consommateurs. Donc, c'est perçu comme un problème de protection des consommateurs. Mais il y a une bonne interaction avec les autorités responsables de la cybersécurité.

Il y a également des mesures qui sont prises pour garantir la protection, avec beaucoup d'exigence autour du Nexus et qui nous permettent de lutter, de réduire certains de ces problèmes, mais pas complètement, car il y a encore beaucoup de problèmes liés aux vols d'identifiants. Et même si vous avez le Nexus qui est obligatoire, vous avez néanmoins parfois des vols d'identifiants. C'est tout pour nous. Merci.

ALEJANDRA REYNOSO Passons au dernier poste. Les accords avec les mécanismes de notification de confiance avec Jake Vincet et Tomonori Miyamoto.

JAKE VINCET Alors je vais rester bref. Nous avons parlé des accords de mécanisme de notification de confiance que nous avons avec le .UK. Nous avons parlé également des risques et des avantages d'avoir de tels accords en place. Alors de quoi on parlait? Les

mécanismes de notification de confiance ne sont pas si populaires et diffusés, et les défis que vous pouvez avoir avec des juridictions étrangères sont présents, notamment en matière de vérification. Vous voulez ajouter quelque chose? Non, C'est bon. Merci.

ALEJANDRA REYNOSO

Merci beaucoup à tous et à toutes. Alors, je vais bientôt lever la séance. Mais avant tout, rejoignez-nous dans Mentimeter pour recevoir un retour. Si vous pensez qu'il n'y avait pas suffisamment d'informations dans ces résumés, eh bien ne vous inquiétez pas, vous allez recevoir un résumé de tout ce qui a été dit afin que vous puissiez avoir accès à toutes les informations. Cela dit, Nico, je te donne la parole.

NICOLAS CABALLERO

Merci. Merci à la ccNSO. Merci Alejandra. C'était vraiment une session formidable. C'est l'une de mes favorites, avec tout le respect que j'ai pour les autres comités consultatifs, les autres unités constitutives. Je pense qu'il faut faire davantage de sessions de cet acabit avec d'autres unités constitutives. C'est très interactif, c'est très intéressant.

Merci beaucoup à la ccNSO. Prenez quelques instants pour compléter le Mentimeter. Peut-être qu'il y a suffisamment de temps qui avait été alloué à cette discussion : 18, 15 minutes. C'était trop long. C'était trop court. Peut-être qu'il faut plus de temps pour la conclusion, etc. C'est tout.

Désolé d'avoir dépassé le temps imparti de quatre minutes. Un point d'intendance. Nous allons déjeuner et c'est une bonne nouvelle. Vous aurez 15 minutes supplémentaires, car nous avons une réunion du leadership du GAC. Donc, on se retrouve à 13 h 30-13 h 45. Encore mieux, ça vous embête? Il y a des gens qui sont contre cela.

Je lève la séance. De retour à 13 h 45. Merci. Et on peut applaudir nos collègues de la ccNSO. Merci.

[FIN DE LA TRANSCRIPTION]