ICANN77 | Forum de politiques – Discussion du GAC sur l'utilisation malveillante du DNS et technologies émergentes
Mercredi 14 juin 2023 – 10h45 à 12h15 DCA

JULIA CHARVOLEN : Bonjour à tous, bienvenue à la séance du GAC consacrée à l'abus du DNS suivie par une discussion sur les technologies émergentes. Veuillez noter que cette séance est enregistrée et qu'elle est régie par les normes de comportement requises par l'ICANN.

Pendant cette séance, des questions seront lues à haute voix si elles sont faites dans le format approprié. Parlez clairement et à un rythme raisonnable pour permettre une interprétation appropriée de vos propos et mettez sur muet vos autres dispositifs.

Vous pouvez accéder aux différentes fonctionnalités d'interprétation sur le menu Zoom.

Sur ce, je vais donner la parole au président du GAC, Nico Cabellero.

PRÉSIDENT NICO CABALLERO : Bonjour à tous, merci Julia. Nous allons avoir Susan Chalmers du département du commerce des États-Unis, NTIA. Nous avons Karel Douglas de l'autorité de télécommunications de Trinité-et-Tobago et coprésident du groupe du GAC sur les régions faiblement desservies. Nous avons également Laureen Kapin qui est coprésidente du même

groupe et Chris Lewis-Evans du UK National Crime Agency et qui est coprésident du groupe de travail du GAC sur la sécurité publique.

Nous avons des invités, nous avons Russ Weinstein, j'espère ne pas avoir écorché votre nom de famille, qui est de l'organisation ICANN, division domaines mondiaux, et Peter Jansen d'EURid. Bonjour à tous, bienvenue.

Nous allons voir quel est l'ordre du jour pour aujourd'hui. Le premier point, c'est un aperçu des amendements contractuels proposés en matière d'abus du DNS et les menaces de la sécurité du DNS qu'ils sont censés résoudre. Nous allons parler également de .eu et des abus du DNS. Point 3, journée zéro atelier de renforcement des capacités du GAC sur l'abus du DNS et je vais à ce moment-là donner la parole à Karel qui va nous parler de ces activités. Finalement, nous aurons une discussion du GAC pour déterminer quelles seront les prochaines étapes.

Je vous souhaite à nouveau la bienvenue et je vais donner la parole à Chris.

CHRIS LEWIS-EVANS : Merci beaucoup.

Je vais tout d'abord passer la parole à Russ qui va nous donner un bref aperçu des amendements contractuels et ensuite, je vais reprendre la parole pour voir ce que cela représente du point de vue du groupe de travail sur la sécurité publique.

RUSS WEINSTEIN : Merci beaucoup de m'avoir reçu. Je suis vice-président à l'ICANN chargé des domaines mondiaux et stratégie. Ceci veut dire que je m'occupe de la relation avec les opérateurs de registre et les bureaux d'enregistrement du point de vue des contrats et je suis responsable de la coordination des programmes d'atténuation de l'ICANN concernant les abus du DNS. Vous voyez que mon intervention concerne ces deux pistes de travail.

Avant de passer aux amendements contractuels et ce qu'ils représentent, je voudrais tout d'abord voir d'où cela vient. Nous savons que l'abus du DNS fait l'objet de beaucoup d'intérêt au sein de la communauté de l'ICANN et ailleurs et il y a eu beaucoup de progrès de faits au cours des dernières réunions, notamment en ce qui concerne les meilleures pratiques qui ont été produites au sein de la communauté par les parties contractantes. Mais il fallait faire davantage.

Au cours de ces dernières années, les équipes de la conformité contractuelle se sont réunies et elles ont proposé des changements aux contrats pour créer des obligations afin de désamorcer et d'atténuer les abus du DNS. Nous avons eu également des discussions par rapport aux actions qui devaient être mises en œuvre du point de vue de l'élaboration de politiques pour lutter contre les abus du DNS. Tout d'abord, nous nous sommes focalisés sur les amendements contractuels.

Voilà ce que nous souhaitons faire : mettre en place des amendements contractuels qui permettent d'avoir, pour les opérateurs de registre et les bureaux d'enregistrement, des règles claires et contraignantes pour

lutter contre les abus du DNS ; voilà ce que sont ces amendements contractuels. L'idée, c'est de créer une nouvelle base pour les opérateurs de registre et les bureaux d'enregistrement.

Nous avons présenté tout cela à plusieurs reprises pendant une séance de la Prep Week dans une séance hier et lors d'une discussion avec le GAC lundi. Quelles sont ces changements proposés ? Nous avons pris comme point de départ les obligations contractuelles existantes. Nous ne voulions pas changer quoi que ce soit de ces obligations mais aller un peu plus loin. Par exemple, les informations de contact en cas d'abus devraient être disponibles sur les sites Web. Nous avons amélioré certaines fonctionnalités, par exemple permettre aux opérateurs de registre et bureaux d'enregistrement d'utiliser un formulaire pour collecter des informations différemment, que ce ne soit pas à partir des adresses de courrier électronique, parce que comme nous avons pu le constater ces derniers temps, les adresses de courrier électronique ne sont pas une source fiable. Nous voulions des informations de contact qui puissent être plus exploitables.

Nous avons ajouté une fonctionnalité pour les opérateurs de registres et bureaux d'enregistrement pour qu'ils ne doivent pas confirmer réception de ces signalements d'abus. Nous nous retrouvions dans une situation où une escalade était nécessaire. Ces amendements ajoutent une définition de l'abus du DNS aux fins de ces amendements et de ces contrats et cela crée une nouvelle obligation pour atténuer ou désamorcer les abus de DNS.

Avec ces changements apportés aux clauses contractuelles, nous avons ajouté un document supplémentaire qui a une quinzaine de pages où

l'on explique quelles sont ces exigences de manière détaillée, à quoi ressemble la mise en œuvre de ce type d'exigence. Et nous encourageons les personnes intéressées à ce sujet à lire ce document, il est facile à lire et très utile. Diapo suivante.

Nous rentrons dans le détail des obligations clés. Tout d'abord, nous avons ajouté une définition de l'abus du DNS pour les opérateurs de registres et bureaux d'enregistrement. L'abus du DNS concerne les logiciels malveillants, les réseaux zombies, l'hameçonnage, le dévoiement et le spam lorsque le spam est un vecteur pour commettre d'autres abus du DNS. Ces définitions viennent du travail qui a été fait au sein de la communauté de l'ICANN et cela remonte aux documents SAC 115. C'est un travail qui a été fait au sein de la communauté pour se mettre d'accord par rapport à ce qu'est l'abus du DNS ou l'utilisation malveillante du DNS. Ce travail fait par la communauté a été le point de départ de notre travail.

Une fois que l'on est d'accord par rapport à ce que sont les abus du DNS, il y a des obligations clés au niveau du contrat, à savoir que lorsque l'opérateur de registre ou le bureau d'enregistrement reçoit un signalement d'abus du DNS, il doit désamorcer ou arrêter l'utilisation de ce nom pour commettre des cas d'abus.

Il est important de se souvenir que tout dépend du contexte. Tous les cas ne font pas l'objet de la même approche d'atténuation et toutes les actions d'atténuation doivent essayer d'arrêter ou de suspendre les activités malveillantes. Diapo suivante.

Pour ce qui est des opérateurs de registre, c'est presque la même obligation, mais il y a d'autres considérations concernant le rôle des opérateurs de registre et des bureaux d'enregistrement, car les bureaux d'enregistrement sont plus proches des titulaires de nom, donc ils peuvent interagir avec les clients en cas de signalements d'abus. L'opérateur de registre a presque les mêmes obligations, mais il a un minimum d'actions qui doivent être mises en œuvre, à savoir faire remonter au bureau d'enregistrement le signalement pour que le bureau d'enregistrement puisse prendre des mesures ou directement arrêter le comportement malveillant. Mais l'opérateur de registre doit faire l'une de ces deux choses.

Voilà les obligations clés qui figurent dans les amendements proposés à ces contrats de registre.

CHRIS LEWIS-EVANS : Si vous voulez répondre à des questions après, ce serait bien.

Je voulais vous parler de la manière dont ces changements ont un impact sur l'activité du public et nous voulions savoir si tout est pris en compte. Est-ce que cela nous donne les outils dont nous avons besoin pour nous assurer que ces actions vont dans le sens de l'intérêt public ? Est-ce que cela couvre l'hameçonnage par SMS ? Est-ce que cela couvre d'autres cas ?

Nous avons trois ou quatre exemples ici – et d'ailleurs, cela le fait – et vous allez voir des captures d'écran sur des messages SMS envoyés à une personne en disant qu'il doit mettre à jour son compte ou sinon ce compte sera supprimé. Ensuite, il y a un lien sur lequel la personne doit

cliquer. Ce type de cas, on le voit tous les jours, ce sont des cas d'hameçonnage. On montre ici le lien où vous voyez que ce lien correspond à un site qui n'est pas vrai. Il faut pouvoir signaler ce cas avec des preuves à l'appui. Ceci nous permet de dire : « Il s'agit d'un cas d'hameçonnage. Il s'agit d'un abus du DNS » et le texte dit qu'il faut agir de manière rapide une fois qu'il y a des preuves. Dans ce cas, même si c'est un domaine enregistré des fin malveillantes, nous allons suspendre ce domaine et on peut recommander de contacter l'hébergeur de contenu pour prendre des mesures d'indignation. Tout cela est couvert. Si vous recevez des messages par e-mail, cela est couvert aussi si le nom de domaine sur lequel vous cliquez est malveillant.

Il y a également des domaines qui sont des faux domaines, par exemple avec une lettre supplémentaire, et l'exemple que vous voyez sur la droite fait partie de ce type de cas. C'est un service que beaucoup de gens utilisent. C'est le cas par exemple des réseaux sociaux ou quand on vous envoie un message en disant que vous avez reçu un colis et que vous devez vous connecter. À ce moment-là, ils vont utiliser votre mot de passe pour des activités malveillantes. Est-ce que tout cela est couvert par ces amendements ? Oui. Ces amendements apportent des précisions pour savoir quels sont les cas de figure qui sont considérés ou qui sont concernés.

À l'ICANN76, on a vu qu'une grande partie des activités malveillantes commence avec une activité ou un message d'hameçonnage. Le fait de s'attaquer à l'hameçonnage est très important pour pouvoir atténuer l'utilisation malveillante du DNS.

Un élément clé pour beaucoup de gouvernements en ce moment, c'est les rançon-logiciels. Est-ce que le rançon-logiciel est concerné par ces amendements ? Oui parce qu'il fait partie des logiciels malveillants et il consiste à distribuer des logiciels malveillants qui chiffrent les logiciels d'un ordinateur et ceci est considéré ou pris en compte dans les amendements. C'est un élément clé pour des gouvernements en ce moment ainsi que pour des entités commerciales ou pour des infrastructures critiques dans certains pays. Tout cela est également pris en compte par les amendements.

Ensuite, les logiciels espions qui sont installés dans les ordinateurs de certaines personnes, ceci fait partie également des amendements parce que cela fait partie des logiciels malveillants. Certains parlent de trojans qui subtilisent des données ; c'est une autre modalité de logiciels malveillants, car ils vous envoient un lien vers un domaine malveillant.

Ensuite, les publicités malveillantes, même cas de figure, vous cliquez sur un lien, vous pensez que c'est le bon site mais c'est un site qui va subtiliser vos informations. Et pareil, ce cas de figure est également considéré dans les amendements parce que cela permet aux attaquants d'avoir un impact sur les victimes. Ceci est également reflété dans la définition que nous utilisons.

De notre point de vue, c'est vraiment un pas en avant très important. Pour les bureaux d'enregistrement, les choses sont beaucoup plus claires par rapport à ce qu'ils doivent faire et je pense que c'est vraiment une étape majeure, un point clé, quelque chose de très positif.

Je vais passer la parole à Nico.

PRÉSIDENT NICO CABALLERO : Merci beaucoup, Chris.

Avant de passer la parole à Peter Janssen et avant de passer au point suivant, excusez-moi, c'est [inaudible], avant de passer la parole à EURid, je veux savoir s'il y a des questions en ligne ou ici dans la salle.

GULTEN TEPE : Nous avons une question de Ken-Yin du Taipei chinois et ensuite de Kavouss Arasteh. Taipei chinois s'il vous plaît.

TAIPEI CHINOIS : Merci beaucoup, Monsieur le Président. Je m'appelle Ken-Ying, je suis représentante du Centre d'information de réseaux de Taïwan et je représente le Taipei chinois.

Pour ce qui est des amendements contractuels concernant les abus du DNS, je pense que le libellé est très bien rédigé car il a trouvé un équilibre entre les intérêts des uns et des autres. Je pense que l'on devrait pouvoir rédiger le texte de manière à refléter la question de la stabilité, parce que cela doit servir de référence à toutes les parties pour la mise en œuvre de ces dispositions contractuelles à l'avenir.

J'ai des questions par rapport à l'interprétation de ce libellé. Tout d'abord, j'ai vu le terme « raisonnable » et je me demande quelle est l'interprétation de cette raisonnabilité. Est-ce que c'est depuis la

perspective des opérateurs de registre et des bureaux d'enregistrement ou du point de vue de l'ICANN ? Voilà ma première question.

Ma deuxième question concerne les problèmes transfrontaliers. Pour l'abus du DNS, très souvent, l'attaquant et la personne qui signale se trouvent dans des juridictions différentes et je me demande donc quelles sont les obligations que nous imposons aux opérateurs de registre et aux bureaux d'enregistrement. Et plutôt, je me demande si ces obligations tiennent compte du fait que ces attaques peuvent se produire parfois de manière transfrontalière.

RUSSELL WEINSTEIN : Merci pour votre question. La première question concerne le degré de responsabilité, comment interpréter cela. Tout d'abord, il y a une obligation pour les parties contractantes, ils doivent agir de manière raisonnable. Et ensuite, du côté de l'ICANN, l'ICANN doit déterminer la raisonnabilité de ces choix, et cela, basé sur notre longue expérience dans ce domaine, notre expérience par rapport à ces dispositions contractuelles. L'ICANN doit être raisonnable au moment de mettre en œuvre ces dispositions contractuelles.

CHRIS LEWIS-EVANS : Effectivement, vous avez raison, il y aura trois juridictions au moins, peut-être même cinq ou six dans certains cas. Ces éléments de langage, ce libellé ici ne permet pas simplement aux autorités d'imposer une mesure judiciaire. Cependant, cela permet les demandes transfrontalières auprès des bureaux d'enregistrement pour évaluer la situation et agir en fonction des résultats de leur examen. Les bureaux

d'enregistrement et les opérateurs de registre apprécient toujours les éléments de preuve qui sont fournis par les autorités. Lorsque nous les leur envoyons, c'est toujours apprécié en général effectivement. Nous commençons à échanger et parfois ils nous demandent des éléments plus précis pour pouvoir agir. Ce texte permet une collaboration transfrontalière, mais toute action judiciaire sera faite en utilisant les éléments de preuve.

PRÉSIDENT NICO CABALLERO : L'Iran demande la parole.

IRAN : Merci, Monsieur le Président. J'ai deux histoires à vous raconter.

J'ai reçu il y a quelque temps un message de l'Union internationale des télécommunications qui me demandait de venir au bureau du secrétaire général. Immédiatement, j'ai vérifié et évidemment, ce n'était pas un message véritable. Ensuite, j'ai reçu un autre message qui venait de Cristina je ne sais quoi soi-disant d'un groupe de travail de l'ICANN et elle me demandait d'accuser réception de ce message. Je me suis rendu compte ensuite que ce n'était pas une Cristina que je connaissais. Dans quelle catégorie d'abus tombent ces messages ? Et qu'est-ce que vous me recommandez de faire ? J'ai bien évidemment changé mon mot de passe immédiatement.

LAUREEN KAPIN : Oui Kavouss, effectivement, ce sont de très bons exemples parce que cela démontre la variété de types de communication. Certaines

peuvent juste être un peu irritantes, dérangeantes et d'autres peuvent être d'une envergure beaucoup plus vaste, avec des impacts économiques.

Je ne crois pas que ce que vous avez reçu tomberait dans la catégorie de l'utilisation malveillante du DNS. Il n'y a pas eu de préjudice causé, simplement c'est un peu dérangeant. Parfois, vous recevez juste une salutation ou juste un petit SMS et c'est parfois la première étape d'un processus beaucoup plus préjudiciable. Donc, il est important de lire ces messages et de ne pas emprunter le chemin qui vous mènera à divulguer des informations sensibles ou peut-être à permettre l'accès à vos ordinateurs.

Mais ces situations spécifiques que vous décrivez, Kavouss, ne seraient pas caractérisées comme étant des utilisations malveillantes du DNS même si elles sont effectivement très dérangeantes.

PRÉSIDENT NICO CABALLERO : La Malaisie, Mohamad Afiq demande la parole.

MALAISIE : Afiq pour l'enregistrement.

Cet amendement me semble être une excellente initiative et je pense qu'il est temps que nous atténuions mieux les effets de l'utilisation malveillante du DNS dans l'écosystème du DNS. Je ne sais pas s'il y a déjà d'autres documents ou d'autres dispositions qui couvrent déjà ces aspects, mais si jamais il y avait des incohérences dans les engagements des bureaux d'enregistrement ou des opérateurs de

registre, j'aimerais savoir s'il existe la possibilité d'adopter une décision qui pourrait permettre d'intervenir sur le nom de domaine en cas de désaccord entre les parties prenantes.

PRÉSIDENT NICO CABALLERO : Merci à la Malaisie. Russ ?

RUSSELL WEINSTEIN : Je n'ai pas très bien compris la question. Est -ce que vous pourriez la reformuler s'il vous plaît ?

MALAISIE : Lorsque l'évaluation a été faite par le bureau d'enregistrement ou l'opérateur de registre, que faire s'il y a des contradictions ? C'est-à-dire que faire s'ils ne sont pas d'accord concernant la détermination d'utilisation malveillante ou non du DNS ? Que faire dans ce cas-là ? Qui peut trancher ce différend ? Et quelle serait alors la décision qui serait prise concernant ce nom de domaine spécifique ?

RUSSELL WEINSTEIN : Les éléments de preuve doivent être présentés au bureau d'enregistrement en cas d'utilisation malveillante du DNS, d'hameçonnage, et si le bureau d'enregistrement détermine qu'il ne s'agit pas d'un cas d'utilisation malveillante du DNS, vous pouvez nous envoyer toutes les informations de l'affaire. Nous avons la possibilité, nous, d'être un mécanisme de recours pour déterminer ou non si c'est effectivement un cas d'utilisation malveillante de DNS et par

conséquent de demander rectification au bureau d'enregistrement. J'espère que cela répond à votre question.

MALAISIE : D'accord, donc il y a une instance de recours et c'est cette instance de dépôt de plainte de votre autorité qui prendra la décision finale concernant l'utilisation malveillante, n'est-ce pas ?

RUSSELL WEINSTEIN : Oui, effectivement. Le service de conformité de l'ICANN aura la possibilité d'analyser votre demande afin de déterminer s'il s'agit effectivement d'un cas d'utilisation malveillante du DNS pour déterminer si le bureau d'enregistrement a effectivement raison dans son évaluation, si les mesures appropriées ont été prises en cas de nom de domaine compromis, si par exemple une suspension a été réalisée ou pas. Cependant, les mesures à leur disposition sont diverses. Il est possible qu'une mesure qui soit adoptée par le bureau d'enregistrement ne vous satisfasse pas immédiatement, mais nous sommes en mesure d'analyser ces questions-là.

PRÉSIDENT NICO CABALLERO : Merci à la Malaisie.

Le Japon, Nobu, dans la salle.

JAPON : Merci beaucoup, Monsieur le Président. Permettez-moi d'abord de vous remercier pour tout le travail de rédaction de ce projet d'amendement. Une question concernant le contrat actuel avant l'amendement.

Le contrat actuel n'interdit pas aux parties contractantes d'adopter des mesures volontaires si nécessaire, y compris concernant l'utilisation du nom de domaine. Comme l'a dit Russ, la réaction du bureau d'enregistrement n'est pas toujours à la hauteur des attentes du plaignant et nous avons effectivement constaté certains cas de frustration dans l'industrie au Japon. Nous nous félicitons de l'ajout dans cet amendement de la possibilité d'une intervention plus directe dans le cas d'une insatisfaction du plaignant.

PRÉSIDENT NICO CABALLERO : Russ.

RUSSELL WEINSTEIN : Pardonnez-moi, cher délégué du Japon, j'ai quelques difficultés à comprendre véritablement votre question.

JAPON : Ce que je voulais dire, c'est que dans l'amendement, il y a un libellé très clair qui invite les bureaux d'enregistrement et les opérateurs de registre à agir. Mais dans le texte actuel, ils peuvent librement décider s'ils doivent agir ou pas sur une base volontaire, par exemple bloquer le serveur ou d'autres éléments tels que définis dans le SAC 115.

RUSSELL WEINSTEIN : Effectivement, cet amendement définit très clairement ce qu'est l'utilisation malveillante du DNS et quelles mesures peuvent être prises pour mettre fin à ces pratiques. Les dispositions concernant les possibilités d'intervention de la part des bureaux d'enregistrement vont continuer à exister. Les bureaux d'enregistrement auront plus de marge de manœuvre, plus de capacité d'action, mais ils devront continuer leurs enquêtes tel que c'est le cas aujourd'hui.

JAPON : Alors, qu'en est-il des opérateurs de registre ? Dans le cas d'une plainte, un avocat ou un plaignant peut envoyer une demande et l'opérateur de registre peut la recevoir. Et cet opérateur de registre peut agir s'il considère que l'action est nécessaire.

RUSSELL WEINSTEIN : Rien dans le contrat n'interdit les bureaux d'enregistrement ou les opérateurs de registre à agir s'ils le jugent nécessaire.

PRÉSIDENT NICO CABALLERO : La République démocratique du Congo.

RÉPUBLIQUE DÉMOCRATIQUE DU CONGO : Merci beaucoup, Monsieur le Président. Je souhaite remercier d'abord Chris pour les informations qui nous ont été transmises dimanche ainsi que pour cet amendement qui définit très clairement quels sont les cas d'utilisation malveillante du DNS puisque

c'était quelque chose qui inquiétait encore les régions faiblement desservies. Un commentaire supplémentaire.

La plupart du temps, les fournisseurs de services Internet font face à une difficulté. Ce ne sont pas nécessairement des utilisations malveillantes, mais je ne sais pas si cela pourrait être une excuse pour les fournisseurs de services Internet lorsqu'ils obligent certains utilisateurs à acheter des services et sur les factures que les utilisateurs reçoivent apparaissent soudain des services que les utilisateurs doivent payer alors qu'à aucun moment les utilisateurs n'ont reçu une demande explicite d'y souscrire ou une proposition explicite. Bien sûr, cela n'est pas explicitement malveillant tel que peut l'être l'hameçonnage, mais ces mesures ou ces services ne sont pas explicitement fournis avec l'accord de l'utilisateur. Alors, peut-on caractériser cette pratique ?

CHRIS LEWIS-EVANS : Je pense que ce serait du spam. Mais étant donné que ceci ne mène pas à des activités malveillantes, ça ne pourrait pas être caractérisé comme une utilisation malveillante. C'est peut-être plutôt une violation de la protection des données personnelles.

LAUREEN KAPIN : Blaise, je pense qu'il s'agit plutôt d'une question de protection du consommateur dans le domaine de la facturation, c'est-à-dire que les utilisateurs ne peuvent pas recevoir des factures de service qu'ils n'ont pas demandé.

PRÉSIDENT NICO CABALLERO : La Commission européenne, Gemma.

COMMISSION EUROPÉENNE : Merci, Monsieur le Président. J'essaierai d'être aussi brève que possible et de réagir à ce que certains collègues ont dit, en particulier le collègue du Japon.

Tout d'abord, nous nous félicitons de ce progrès. C'est une avancée d'importance critique et le succès de cette initiative sera très important pour le fonctionnement du modèle de l'ICANN et pour toute notre communauté. C'est pourquoi nous souhaitons contribuer de façon constructive à l'occasion de cette séance et nous avons participé à la séance sur le renforcement des capacités dimanche et nous continuerons à travailler pour apporter des contributions constructives.

Deux ou trois commentaires, si vous me le permettez, que j'ai déjà formulés pendant la séance de formation dimanche.

Notre collègue du Japon parlait de l'importance de la vitesse pour intervenir dans les cas d'utilisation malveillante du DNS. Est-ce qu'il existe réellement des outils de suivi de l'utilisation malveillante du DNS pour les bureaux d'enregistrement et les opérateurs de registre ? Ceci nous semble fondamental et il serait peut-être préférable de le mettre directement dans les contrats.

Deuxièmement, nous vous remercions pour l'avis qui complète les contrats. Cependant, il serait important de s'assurer que les

dispositions concernant l'application soient claires. C'est important pour la conformité et pour l'évaluation des conséquences de la non-conformité.

Pour finir, il y a un point important sur la transparence dans les contrats compte tenu de l'obligation de transparence et de présentation de rapports de la part des opérateurs. Nous pensons qu'il serait important de clarifier la transparence pour que les opérateurs sachent exactement quelles sont leurs obligations et pour que les rapports qui soient présentés soient clairs, par exemple que le rapport dise : « Voilà la quantité d'usage malveillant que nous avons constatée, voilà ce que nous avons fait » puisque ceci nous permettrait de comprendre comment ces contrats, qui sont des outils importants, sont appliqués en pratique.

RUSSELL WEINSTEIN : Merci beaucoup, Gemma. Effectivement, c'est un sujet épineux. Je pense que pour la prochaine phase de contrats, ce serait un commentaire utile pour prendre cela en compte la prochaine fois.

En ce qui concerne la clarté sur les initiatives de conformité, je pense que c'est quelque chose qui est utile du point de vue du GAC. Ce serait une initiative intéressante pour le GAC.

CHRIS LEWIS-EVANS : Merci beaucoup pour ces commentaires. Et comme Chris l'a dit, j'espère que ces amendements et dans l'avis tout ceci sera clair. Mais d'après votre question, je vois que ce n'est peut-être pas le cas.

Le service de conformité a la possibilité, en cas d'identification d'une violation, de mettre fin à un accord avec un bureau d'enregistrement ou un opérateur de registre, à le résilier de façon unilatérale. C'est quelque chose que nous essayons de faire pour nous assurer que tout le monde respecte ces mesures et ainsi protéger notre industrie. Nous avons présenté ces nouvelles dispositions dans l'amendement.

PRÉSIDENT NICO CABALLERO : Merci beaucoup, merci Chris. Merci Russ, merci la Commission européenne. Je ne vais pas prendre d'autres questions. Je vais donner la parole à Peter Janssen.

PETER JANSSEN : Bonjour à tous. Le vois que mes diapos sont déjà sur l'écran. Je m'appelle Peter Janssen, je suis directeur général d'EURid. C'est une organisation à but non lucratif belge qui gère le nom du pays qui est dans trois scripts, grec, latin et un autre script utilisé dans l'Union européenne.

Maintenant, je voudrais vous donner un aperçu de ce que nous faisons en matière d'atténuation et de prévention des abus du DNS, quelles sont les mesures que nous avons mises en place. Je m'excuse d'avance de tout résumer parce que c'est un sujet sur lequel je pourrais parler des heures et des journées. Certains me disent que je parle trop et très vite et je m'excuse d'avance auprès des interprètes qui auront du mal peut-être à me suivre. Merci de votre aide. Diapo suivante, s'il vous plaît.

Je vais vous donner un peu une idée de ce dont je vais parler et pour cela, je vais vous donner un aperçu du processus de délégation et d'enregistrement.

Vous voyez qu'il y a plusieurs acteurs, nous avons le titulaire de nom de domaine à gauche, c'est la personne qui va enregistrer un nom de domaine et qui entre en contact avec un bureau d'enregistrement. Il utilise des interfaces de l'opérateur de registre, ce sont les flèches 2, pour essayer de l'enregistrer dans le domaine.

Une fois que l'opérateur de registre reçoit cette demande de la part du bureau d'enregistrement et que des vérifications sont mises en place par rapport à certains critères d'éligibilité, par exemple le titulaire doit avoir domicile en Union européenne, une fois que ces critères d'éligibilité sont confirmés, évalués et acceptés, se met en place le processus marqué par la flèche 4 qui donne lieu à un enregistrement du nom de domaine dans la base de données d'enregistrement. C'est ce que nous appelons le processus d'enregistrement. Bien sûr, il y a davantage de détails, c'est une simplification aux fins de cette explication.

Une fois que le nom de domaine est enregistré, les gens peuvent aller sur un site Web et voir que le nom de domaine est enregistré et ne peut plus être enregistré par d'autres personnes. Mais cela ne veut pas dire que le nom de domaine fonctionne déjà sur l'Internet. C'est la deuxième partie du processus, ce qu'on appelle le processus de délégation. Ici, vous voyez que les flèches sont jaunes pour faire une distinction entre les deux processus.

La deuxième partie concerne le processus de délégation de nom de domaine où l'on doit prendre toutes les informations de la base de données concernant le nom de domaine, le nom du serveur et d'autres éléments clés de DNSSEC relatifs à ce nom de domaine, et toutes ces informations sont insérées dans ce que nous appelons le fichier de zone. Ici, vous voyez les trois fichiers de zone qui correspondent aux trois scripts de noms de géographiques. La tâche de cette fonction est confiée à un serveur qui est appuyé par des serveurs secondaires qui feront en sorte que ce nom de domaine fonctionne. C'est ce que l'on appelle le processus de résolution et je ne vais pas rentrer dans les détails de ce processus.

Voilà donc le processus d'enregistrement versus le processus de délégation. Si vous regardez le processus de délégation de nom de domaine, il y a des informations qui sont tirées de la base de données d'enregistrement et qui sont introduites dans le fichier de zone primaire. Que faisons-nous ? Nous ajoutons une fonctionnalité à ce processus de délégation de nom de domaine. Une fois que le processus de délégation de nom de domaine a délégué le nom de domaine, nous demandons…

PRÉSIDENT NICO CABALLERO : Peter, excusez-moi de vous interrompre, on nous demande que vous parliez plus lentement.

PETER JANSSEN : Je m'excuse. Je m'attendais à cette remarque. Je vais essayer de parler plus lentement.

Le processus de délégation de nom de domaine extrait des informations de la base de données et les insère dans le fichier de zone. Nous avons ajouté une fonctionnalité à ce processus de délégation de nom de domaine. Au moment de la délégation, on demandera au moteur de décision si l'on doit déléguer ce nom de domaine ou pas. Cette décision sera prise en fonction d'un certain nombre d'attributs qui seront pris en compte. Si le nom de domaines a potentiellement été enregistré à des fins potentiellement malveillantes, nous devrions être en mesure de prévoir si ce nom de domaine sera ou non délégué. Je vais vous donner davantage de détails plus tard.

Si le moteur de décision décide qu'il s'agit d'un enregistrement potentiellement malveillant, à ce moment-là on va reléguer. Qu'est-ce que cela veut dire ? On va réinsérer ce domaine dans le fichier de zone. Techniquement, il sera enregistré, mais il ne sera pas inséré dans le fichier de zone. Ensuite commence le processus de validation où on demandera au titulaire de nom de valider les données d'enregistrement. Comme vous l'imaginez, s'il s'agit de l'entité qui est enregistrée à des fins malveillantes, cette validation n'aura pas lieu car cette entité ne voudra pas être retrouvée. À ce moment-là, la validation ne sera pas faite et nous allons suspendre la délégation du nom de domaine. Si le moteur de décision trouve que le domaine n'a pas l'air malveillant et que l'on peut procéder à la délégation, c'est ce que l'on fait, on procède à la délégation du nom de domaine. Diapo suivante.

Ce moteur de décision est connu sous l'acronyme APEWS. Vous voyez à quoi ceci correspond. C'est un système de prédiction d'abus et d'alertes précoces. L'objectif de ce système est de prévoir au moment de

l'enregistrement si un nom de domaine sera enregistré à des fins malveillantes. Cela est fait en faisant un certain nombre de modèles d'apprentissage par machine passer sur un certain nombre d'attributs. Quels sont ces attributs ? Bien entendu, les données du titulaire de nom, nom, adresse, courrier électronique, le bureau d'enregistrement concerné qui va enregistrer le nom de domaine, ce que l'on appelle le caractère aléatoire du nom de domaine, c'est-à-dire si on peut détecter par exemple un nom qui est très difficile à prononcer avec des noms, des lettres, etc., cela donne déjà des indications par rapport aux intentions et ensuite des informations sur le DNS.

Comment tout cela fonctionne ? Ce modèle prédictif d'un côté prend une liste de noms de domaine malveillants déjà connus, des noms qui ont déjà été utilisés pour envoyer des attaques de spam ou d'hameçonnage. De notre côté, on a les données d'enregistrement de noms de domaine correspondant à ces domaines qui ne sont pas malveillants. Ces informations sont renseignées dans une machine qui va faire des prévisions. Cette machine va prendre ses décisions et va rendre sa décision pour voir si l'on pourrait ou non déléguer ce nom de domaine.

Vous me direz que c'est bien d'essayer de prédire si un nom de domaine sera malveillant ou pas, c'est bien. Est-ce que cela est bien ou pas ? Ce que vous voyez ici, c'est un graphique sur les résultats. Sur l'axe des x, vous voyez début 2019, c'est assez récent et sur l'axe des y, vous voyez le nombre de noms de domaine qui sont enregistrés tous les mois et les pourcentages de ces domaines qui ont été signalés par notre système

comme étant potentiellement malveillants. Vous voyez 0,02 et ceci correspond à 2 %.

Il y a un certain nombre de conclusions que l'on peut tirer de ce schéma. D'un côté, la plupart des noms de domaine sont signalés comme n'ayant pas de souci particulier. La plupart des noms de domaine sont délégués normalement et il n'y a pas de problème.

Deuxièmement, si vous regardez les années 2018 et 2019, vous voyez qu'il y a eu un problème par rapport au nombre de domaines qui ont été signalés comme étant malveillants et cela peut dire peut vouloir dire plusieurs choses. D'un côté, les attaquants s'améliorent et ils sortent de notre radar ou c'est que notre système a découragé les attaquants à agir de manière malveillante. Notre système montre qu'en mettant cela en place, il s'agit d'un système tout à fait automatique, le nombre d'enregistrements à des fins malveillantes a diminué au fil du temps. Vous voyez sur l'axe des x que le nombre de ces domaines a diminué.

Certains de ces acteurs malveillants arrivent à contourner, bien sûr, ces systèmes, mais nous essayons de mettre à jour nos systèmes en permanence pour qu'ils possèdent des informations mises à jour.

Modèle de prédiction. Comme tous les apprentissages par machine, il doit être mis à jour en permanence. Nous avons deux manières : d'un côté, on voit combien des noms de domaine qu'on voulait chercher ont été trouvés et ensuite on a la précision, combien de ces noms de domaine ou de ces termes recherchés ont été corrects. On doit savoir si

les noms de domaine que l'on pensait être malveillants étaient définitivement malveillants.

Ensuite, nous avons le système qui fonctionne en temps réel et nous n'avons pas arrêté les délégations, mais nous avons essayé d'affirmer ou de confirmer si ces noms de domaine avaient été utilisés à des fins malveillantes. Nous avons conclu qu'il y avait une précision de 80 %. Cela veut dire que dans quatre ou cinq cas, il y a eu des noms de domaine qui avaient été prévus comme étant enregistrés à des fins malveillantes qui ne se sont pas avérés malveillants.

Bien sûr, il faut être prudent avec les systèmes automatisés, on ne peut pas tout avoir. C'est pour cela que nous essayons en permanence de mettre à jour notre système pour qu'il soit aussi sûr que possible, en ce sens que si nous signalons un domaine comme étant malveillant, nous voulons être raisonnablement sûr que c'est le cas. C'est pour cela que nous optimisons notre système en permanence.

Mais si nous signalons un nom de domaine en tant que malveillant et que le nom de domaine est utilisé de manière normale, on appelle ceci un faux positif. Dans ce cas, le titulaire de nom est invité à valider ses données d'enregistrement. Nous validons par le biais de certains paiements bancaires et c'est très facile de vérifier ces données d'informations. Y compris dans les cas des faux positifs, il est très facile de pouvoir remettre les choses en route en faisant cette validation de données auprès du titulaire de nom. Diapo suivante s'il vous plaît.

Où peut-on utiliser ce système ? Nous l'avons dans ce que nous appelons post-enregistrement pré-délégation. Le système commence

à fonctionner après l'enregistrement du nom de domaine mais avant le déploiement de ce nom de domaine dans le fichier de zone. De cette manière, on s'assure que le nom de domaine ne puisse pas être utilisé s'il est enregistré à des fins malveillantes.

Ensuite, nous avons la possibilité de faire un pré-enregistrement, c'est-à-dire ne pas permettre l'enregistrement si la prédiction dit que le système pourrait être malveillant. Pour mettre en place ce type de système avant l'enregistrement, le système devrait être suffisamment rapide pour éviter qu'il y ait des faux positifs parce qu'autrement, nous ne pourrions pas déléguer des systèmes qui pourraient ne pas être enregistrés à des fins malveillantes. Le pré-enregistrement, c'est une possibilité.

Une autre possibilité, c'est post-enregistrement post-délégation. On pourrait utiliser ce système pour détecter si ces domaines enregistrés il y a 20 ans commettent des activités malveillantes. Mais il y a d'autres informations qui sont disponibles qui rendent plus facile de savoir si un nom de domaine et malveillants ou pas, par exemple le contenu des sites Web, des [inaudible] de sécurité, etc.

Finalement, un projet très intéressant que nous avons en ce moment, c'est les TLD croisés. Nous voyons certaines tendances entre différents TLD. On parle de certains scripts du même registre mais nous voyons que les mêmes mauvais acteurs enregistrent des noms de domaine avec d'autres extensions. Il serait intéressant de voir quelle synergie on pourrait faire en combinant ces informations. C'est ce que nous faisons en ce moment, nous travaillons avec d'autres ccTLD en Europe pour aboutir à un système joint où l'on puisse utiliser les informations des

différents registres en un même centre pour avoir une meilleure visibilité. Bien entendu, à ce moment, il faut considérer le RGPD, les questions liées à la confidentialité des données ainsi que les différentes juridictions auxquelles appartiennent différents registres. Ceci pourrait être résolu en anonymisant les données d'enregistrement. Cela permettrait d'avoir des informations qui ne peuvent pas être lues par les humains mais qui sont quand même là pour que l'on puisse les utiliser. Les modèles d'apprentissage par machine utilisent certaines tendances, certains patrons et ceci est utile et ne peut pas être en lien avec le RGPD.

Voilà ma présentation. L'idée, c'est de combiner des informations différentes des ccTLD sans avoir des problèmes liés à la confidentialité des données. Ce sont des informations que nous allons incorporer dans le système de manière aléatoire. Diapo suivante.

Je pense que c'est la fin de ma présentation. Merci de votre attention. Si vous avez des questions, je serai ravi d'y répondre.

PRÉSIDENT NICO CABALLERO : Merci beaucoup Peter, c'est vraiment fascinant. Désolé de vous avoir interrompu. Je pense que nous n'avons pas énormément de temps. Nous pourrons répondre à quelques questions. Merci beaucoup de cette présentation détaillée.

Est-ce qu'il y a des questions ou des commentaires dans la salle ou dans le chat ? Je vois qu'il n'y en a pas. Je vais redonner la parole à Susan ou à Karel ? Karel, d'accord.

TRINITÉ-ET-TOBAGO : Je suis Karel Douglas, représentant de Trinité-et-Tobago auprès du GAC. Je sais qu'il nous reste quelques minutes, je vais être très bref. J'avais quelques notes, mais ce sera plus facile de parler sans mes notes.

Pour revenir à la diapo que vous avez affichée sur l'écran, le 11 juin, nous avons fait un atelier de renforcement des capacités qui était consacré aux personnes qui sont nouvelles au GAC ou peut-être à celles qui font partie du GAC depuis longtemps pour comprendre les enjeux et les différents dossiers sur lesquels doit se pencher le GAC. Nous voulions avoir un maximum de contributions.

Le 11 juin, nous nous sommes focalisés sur les questions relatives à l'utilisation malveillante du DNS et également sur le processus de consultation publique. Le processus de consultation publique est d'un processus qui est employé par l'ICANN pour recueillir l'avis de la communauté sur certains dossiers. Nous voulions nous assurer que tous les membres du GAC comprennent les différentes étapes du processus de consultation publique. Nous voulions également mieux comprendre la question de l'abus du DNS. Nous avons eu des présentations extraordinaires par rapport à cette thématique.

Combiner ces deux problématiques clés n'était pas facile. Nous avons donc créé un travail en groupe. Les participants ont été regroupés par langue : français, arabe, chinois et anglais. L'idée était de donner aux gens la possibilité de discuter en petit comité des questions qui étaient importantes pour eux. Nous avons eu des gens qui se sont portés

volontaires pour faire des restitutions et nous avons eu cinq personnes qui se sont portées volontaires pour aider dans le processus de consultation publique concernant les abus du DNS. Différents sujets ont été traités dans les petits groupes, à savoir le processus lui-même, mais aussi des questions particulières concernant l'abus du DNS. Il y a eu un certain temps qui a été consacré à la question de la raisonnabilité.

Nous avons exploré ces questions qui, en général, sont définies en fonction de certaines circonstances spécifiques alors que nous nous penchions sur un scénario plutôt large. Qu'est-ce qu'un délai raisonnable ? Dans certains cas, les définitions sont établies de manière très large pour qu'elles puissent s'appliquer à différents cas. Je vois que Nigel Cassimire est là, il a participé au groupe anglophone. Voilà ce que nous avons fait il y a quelques jours et nous espérons que ce sera reflété dans un document sur nos contributions à la question de l'abus du DNS.

Ensuite, l'atelier de renforcement de capacités sur l'abus du DNS est dirigé par le groupe de travail sur les régions faiblement desservies et il est dirigé par Tracy Hackshaw et d'autres. Nous voulions mettre en place d'autres ateliers de renforcement des capacités, non seulement sur l'abus du DNS mais sur d'autres sujets ou thématiques, pour que tout le monde soit à l'aise lorsque nous allons aborder ce type de question.

PRÉSIDENT NICO CABALLERO : Malheureusement, je ne pourrais pas accepter des questions pour le moment. Susan Chalmers, je vous donne la parole.

SUSAN CHALMERS : Merci Monsieur le Président, je serai très brève.

L'ICANN a ouvert la phase de consultation publique concernant les amendements le 13 juillet dernier. Nous avons un échéancier ambitieux, vous le voyez à l'écran, concernant les contributions du GAC. À partir d'aujourd'hui, nous allons commencer à demander des contributions de la part des membres du GAC sur un Google Doc qui sera assorti de questions d'orientation.

Ensuite, les volontaires du petit groupe vont élaborer un premier projet de document à partir de ces contributions. Ce projet sera distribué au sein du GAC. Chacun pourra ajouter quelques commentaires et le document devra faire l'objet d'un consensus avant la date du 13 juillet. Je vous invite à formuler vos commentaires autant que possible en tant que membres du GAC pour pouvoir assurer un bon échange avec la communauté.

PRÉSIDENT NICO CABALLERO : Laureen des États-Unis, un commentaire peut-être ?

LAUREEN KAPIN : Cette session est terminée mais Nico nous a permis de disposer de cinq minutes pour juste planter quelques petites graines dans vos esprits. Nous n'allons pas récolter tous les fruits maintenant, mais d'ici au processus de rédaction du communiqué, je pense que ce pourra être le cas.

Voilà les questions que je souhaite vous présenter. D'abord, quels sont les aspects positifs de ces amendements ?

Ensuite, deuxième question, il y a un point concernant l'application. Est-ce que ces libellés sont suffisamment applicables ?

Troisièmement, quelles sont vos réflexions concernant la proposition de définition de l'utilisation malveillante du DNS ? Est-ce qu'elle est trop large ? Est-ce qu'elle est trop précise au contraire ? Est-ce qu'elle est suffisamment flexible ?

Quatrième question : quelles sont vos réflexions sur l'avis de l'ICANN sur ces amendements ? Bien sûr, c'est un document qui va évoluer en fonction de l'évolution de vos observations, de vos points de vue. Est-ce que c'est un document qui est suffisamment informatif concernant les termes qui ont déjà été abordés, tels qu'adapté à l'action, suffisamment rapide, etc. ? Diapositive suivante. Pardon, je parle un petit peu vite, je m'excuse auprès des interprètes.

Ensuite, cinquième question, il a été dit que c'est la première étape sur un long chemin pour cette question complexe et il est donc important de réfléchir à ce qui vient ensuite. Cet aspect a déjà été abordé et il s'agit de la question d'un processus de développement de politique extrêmement ciblé sur des questions très précises. Par exemple, il pourrait y avoir un PDP sur la meilleure façon de gérer ou d'aborder la question de l'hameçonnage ou nous demander quel pourrait être l'objet d'un travail politique futur sur l'utilisation malveillante du DNS et pas seulement son contenu, mais également sa temporalité. Est-ce que cela devrait être fait avant la nouvelle série de gTLD, etc. ? Le rôle également de l'intérêt public, c'est le point 5b, et des engagements volontaires des opérateurs de registre. Ensuite, bien sûr, que faire avec les récidivistes, les titulaires de noms de domaine, les opérateurs, les

bureaux d'enregistrement ? Doit-il y avoir un degré de priorité, des calendriers qui s'appliquent à ces questions ?

Je ne veux pas de réponses maintenant ; je vous les présente simplement pour que vous les gardiez à l'esprit. C'est à vous maintenant d'y réfléchir et j'espère que vous vous mobiliserez pour nous assurer que la contribution du GAC soit aussi solide et profonde que nécessaire.

PRÉSIDENT NICO CABALLERO : Merci beaucoup Laureen, merci à Susan, Karel, Chris qui nous a quittés ainsi que Russ et Peter.

Nous devons en finir maintenant. Est-ce qu'il y a peut-être une dernière question, un dernier commentaire ? Ce n'est pas le cas. Nous allons lever cette séance. Nous allons prendre une pause peut-être de cinq minutes, Rob ?

GULTEN TEPE : Nous sommes prêts à continuer, Nico

PRÉSIDENT NICO CABALLERO : Notre séance suivante concerne les technologies émergentes. Les objectifs de cette séance sont de créer une liste de sujets technologiques que le GAC souhaite connaître plus en profondeur et suggérer les préférences et les priorités. Le second objectif est d'identifier des options pour élaborer des cadres d'information pour le

GAC et son partage d'informations à l'avenir. Je remercie encore Karel, Susan, Laureen et ceux qui quittent le podium.

L'idée est de créer une liste de sujets technologiques afin de travailler sur cette question. Les membres du GAC ont manifesté leur intérêt de prendre en compte des nouveaux sujets qui peuvent avoir un impact sur le DNS et sur l'Internet en général à l'avenir.

Les suggestions que nous avons reçues jusqu'à maintenant sont au nombre de trois : les racines alternatives du DNS, le blockchain et l'intelligence artificielle.

Notre collègue du Taipei chinois a demandé la parole. Est-ce que vous avez une présentation ?

TAIPEI CHINOIS : Merci, Monsieur le président. Oui, effectivement, je peux vous expliquer pourquoi j'ai proposé ce sujet.

Tout d'abord, je pense que tout le monde ici doit être conscient du fait que les technologies émergentes sont devenues un sujet brûlant au cours des dernières années. Le blockchain et d'autres sujets sont devenus extrêmement importants. Et en ce qui concerne l'intelligence artificielle, nous avons vu, bien sûr, l'évolution de ChatGPT et c'est une technologie de plus en plus importante à travers le monde.

C'est pourquoi je propose au GAC de l'ICANN d'étudier la question des technologies émergentes et de leur impact possible sur le DNSSEC et dans cette mesure quelles devraient être nos actions.

Pour l'intelligence artificielle, la présentation de Peter est un excellent exemple. Il semble que l'ICANN ou que d'autres parties prenantes aient déjà adopté l'intelligence artificielle dans la lutte contre l'utilisation malveillante du DNS. Par conséquent, nous pourrions peut-être y réfléchir un peu plus. Est-ce que l'intelligence artificielle pourrait améliorer nos interventions face aux menaces de sécurité ? Ou est-ce qu'elle pourrait même nous permettre de prévenir certaines activités malveillantes dans le domaine du DNS ? Voici mes réflexions.

PRÉSIDENT NICO CABALLERO : Merci beaucoup, Ken-Ying. Y a-t-il des réactions, des commentaires ou des questions suite à l'intervention de Ken-Ying ? Je n'en vois pas. La diapositive suivante, s'il vous plaît, Gulten.

JULIA CHARVOLEN : Nous avons une main levée de la part de Kavouss de l'Iran en ligne.

PRÉSIDENT NICO CABALLERO : Kavouss, allez-y mais merci d'être bref. L'Iran, vous avez la parole.

GULTEN TEPE : Ana Neves de la délégation du Portugal demande la parole.

IRAN : Je voulais savoir ce que vous vouliez dire par les alternatives au DNS racine.

PRÉSIDENT NICO CABALLERO : Taipei chinois, est-ce que vous voulez répondre à cette question ?

TAIPEI CHINOIS : Le DNS alternatif signifie les autres identifiants. Par exemple pour le blockchain et le Web3, il existe des identifiants Web qui sont semblables à notre système par couches, mais ceci n'est pas toujours le cas auprès de tous les bureaux d'enregistrement ou les opérateurs de registre. C'est là ce que je comprends, mais je ne sais pas si d'autres spécialistes peuvent être compléter cette réflexion.

PRÉSIDENT NICO CABALLERO : Taipei Chinois, merci beaucoup.

Les Pays-Bas ont la parole.

PAYS-BAS : En ce qui concerne les systèmes de nommage alternatif du DNS, j'ai préparé trois questions.

PRÉSIDENT NICO CABALLERO : Je voulais m'excuser auprès du Portugal, je n'ai pas vu votre main levée, mais allez-y cher collègue des Pays-Bas.

PAYS-BAS : Je crois qu'il y a une question qui a été préparée dans un sondage sur Zoom. J'espère que tous les membres du GAC sont connectés sur Zoom pour qu'ils puissent répondre à ce sondage en ligne. Je pense que ceci nous permettra de répondre à la question de Kavouss, c'est-à-dire est-

ce que tout le monde sait ce que sont les systèmes alternatifs de DNS. Voilà le sondage à l'écran et sur Zoom.

PRÉSIDENT NICO CABALLERO : Merci beaucoup aux Pays-Bas.

Le Portugal a la parole.

PORTUGAL : Je vais m'adresser à vous en portugais. Je vous invite à utiliser les récepteurs pour écouter l'interprétation.

Je souhaite faire part de mon soutien à l'intervention du Taipei chinois ainsi que des Pays-Bas. Il est fondamental de renforcer nos capacités de compréhension de l'impact des technologies émergentes sur le DNS. Je pense que ceci serait très intéressant pour le GAC et il serait utile de comprendre quel est exactement l'impact de ces nouvelles technologies. Ces technologies émergentes sont importantes et nous devons en comprendre l'impact pour l'avenir. Il est urgent d'en parler dans le contexte de la session du GAC.

PRÉSIDENT NICO CABALLERO : Merci beaucoup.

Nigel Hickson du Royaume-Uni et ensuite l'OMPI demande la parole.

ROYAUME-UNI : Je voulais simplement savoir si nous avions déjà quelques résultats du sondage.

PAYS-BAS : Non, allez-y. Vous pouvez poser vos autres questions. Est-ce que nous avons les résultats ? Est-ce que nous avons des résultats du sondage ? Il semblerait que 53 % ont entendu parler de l'alternative au DNS racine et l'autre moitié n'en a jamais entendu parler.

Il y a une deuxième question dans ce sondage. Comme vous le constatez, j'essaie simplement de préparer mon intervention.

PRÉSIDENT NICO CABALLERO : Oui, c'est parfait. C'est l'idée de toute cette séance. Allez-y, les Pays-Bas.

PAYS-BAS : La deuxième question maintenant à l'écran.

JULIA CHARVOLEN : La deuxième question se trouve maintenant à l'écran.

PAYS-BAS : Merci Julia. Pendant que vous répondez, donnons peut-être la parole à Nigel ou à Brian.

PRÉSIDENT NICO CABALLERO : Merci les Pays-Bas. Brian, vous avez la parole.

OMPI : Bonjour chers collègues, je suis Brian Beckham de l'Organisation mondiale de la propriété intellectuelle. En ce qui concerne ce sujet, j'avais deux observations.

En septembre se tiendra la huitième conversation de l'OMPI sur la propriété intellectuelle et les technologies de pointe. Nous avons un département qui s'intéresse à l'intersection entre l'intelligence artificielle et la propriété intellectuelle que nous appelons le département des technologies frontières ou des technologies de pointe.

Tous les résultats de la septième conversation sont déjà disponibles sur notre site Internet. Elle s'intéressait aux technologies financières, aux blockchains, au métavers et à d'autres questions de ce genre.

En avril de cette année, l'INTA, l'Organisation internationale des marques déposées, a produit un document qui concernait l'étude de trois domaines. Je vais partager cette ressource sur la liste du GAC, mais permettez-moi de vous lire des recommandations de ce document. Je cite : « La confiance de la part des consommateurs est nécessaire et par conséquent, l'OMPI pourrait considérer la possibilité d'adopter une politique de règlement des différends dans ce domaine pour pouvoir accompagner l'évolution de ces écosystèmes numériques, des jetons non fongibles, du métavers, etc. L'OMPI a été prié par les États membres en 1998 de produire une recommandation concernant le problème de l'Internet, en particulier l'intersection entre les noms de domaine et les marques déposées que l'on appelle en anglais le cybersquatting. » Vous vous souviendrez peut-être de la révision de

politiques prévue entre l'ICANN et nos services. Nous avons déjà informé le GAC sur cette question par le passé.

Je voulais également mentionner très concrètement qu'hier à l'occasion de la réunion de l'IPC, Namebase qui est l'un des opérateurs de cette alternative au DNS racine est une option alternative particulière pour les différends en matière de marques déposées et ceci constitue une évolution très positive pour les propriétaires des marques et nous espérons que ceci permettra d'entamer de nouvelles conversations.

Merci beaucoup.

PRÉSIDENT NICO CABALLERO : Merci Brian.

Le Royaume-Uni suivi de la Chine. Allez-y, Nigel.

ROYAUME-UNI : Nigel Hickson, représentant du Royaume-Uni.

Je voulais insister sur l'importance de cette séance. On ne va pas parler de tout bien évidemment parce qu'on approche de l'heure du déjeuner, mais pour rebondir sur ce qui a été dit par Taïwan et les Pays-Bas, nous avons une responsabilité, les vice-présidents, le président, les membres du GAC, de prévoir ce type de discussion, notamment en ce qui concerne les blockchains et les racines DNS alternatives. Nous savons également que l'intelligence artificielle fait l'objet de beaucoup de

scrutin en ce moment et ce sont des sujets importants sur lesquels nous allons devoir nous pencher. Merci beaucoup.

PRÉSIDENT NICO CABALLERO : Merci beaucoup, le Royaume-Uni.

J'ai la Chine. Ensuite, on reviendra aux Pays-Bas et si nous avons un peu plus de temps, on ouvrira le micro à d'autres intervenants.

CHINE : Je trouve que cette séance est intéressante. Mais pour ce qui est d'autres séances de ce type, si nous envisageons d'en avoir à l'avenir, nous pourrions peut-être convoquer des experts informatiques ou des experts dans d'autres domaines des technologies émergentes pour qu'ils nous parlent de ces sujets. En tant que GAC, la plupart d'entre nous sont intéressés à écouter ce type de présentation. C'est ma suggestion en ce moment.

PRÉSIDENT NICO CABALLERO : C'est bien noté, la Chine. L'idée au départ, c'était d'identifier des sujets pour établir un ordre du jour, savoir également si le GAC souhaite aborder ce type de problématique. Si nous nous mettons d'accord par rapport à cela, nous pourrons penser à quelque chose de plus structuré.

Désolé, on n'a pas beaucoup de temps, il ne nous reste que cinq minutes. Les Pays-Bas, s'il vous plaît.

PAYS-BAS : Les résultats sont sur l'écran. Je vois qu'il y a différentes réponses. La plupart des gens déclarent qu'ils ne connaissent pas trop le sujet. Diapo suivante.

Je ne vais pas lire tout ce qui est affiché sur l'écran, mais en gros, ce que l'on veut dire, c'est que la racine alternative de DNS est un sujet qui est abordé par un rapport de l'OCTO de 2022, je crois, et il s'agit d'un rapport très intéressant qui a éveillé mon intérêt par rapport à cette question.

J'ai préparé une troisième question. Est-ce que vous voulez avoir des ateliers de renforcement des capacités par rapport à ces questions ? Je pense que la réponse à ma question est déjà claire à partir des interventions qui m'ont précédée. L'idée serait de présenter un sujet et j'invite les collègues à lire le rapport dont je vous ai parlé pour pouvoir approfondir ensuite sur les questions qui sont abordées dans le rapport.

PRÉSIDENT NICO CABALLERO : Merci beaucoup, les Pays-Bas.

Ensuite, j'ai la Suisse. Jorge Cancio, s'il vous plaît, je vous prie d'être bref, nous n'avons pas beaucoup de temps.

SUISSE : Très brièvement, si le GAC est intéressé à savoir ce que le Conseil de l'Europe fait en matière d'intelligence artificielle, notre prédécesseur Thomas Schneider préside le comité qui s'occupe de ce sujet au Conseil de l'Europe. Je pourrais le contacter si cela vous intéresse.

PRÉSIDENT NICO CABALLERO : Merci, ce serait très bien.

Est-ce qu'il y a d'autres éléments à ajouter, les Pays-Bas ?

PAYS-BAS : Un dernier élément. Hier, j'ai brièvement parlé à John Crane, le directeur de la technologie, qui nous a fait part de son intention de nous aider si nous le souhaitons dans ces ateliers de renforcement des capacités.

PRÉSIDENT NICO CABALLERO : Merci les Pays-Bas.

Nous avons le représentant de la Suède à mes côtés qui souhaite prendre la parole, le vice-président du GAC.

VICE-PRÉSIDENTE OLA BERGSTRÖM : Je pense que nous avons abordé beaucoup des sujets que nous voulions traiter. Maintenant, passons au comment, à savoir quelles sont les options des approches, les outils que nous allons adopter pour mener à bien ce type d'activité. Nous devons avoir une discussion par rapport à cela. Nous n'allons pas trouver une solution unique pour tout, il faudra garder une approche flexible.

Nous sommes tout à fait intéressés par vos commentaires même si nous n'avons pas le temps en ce moment de tous les écouter. Bien sûr, nous y reviendrons le moment venu.

PRÉSIDENT NICO CABALLERO : Merci beaucoup. Est-ce qu'il y a des questions ou des commentaires, des réactions dans la salle ou en ligne ? Gulten ? Julia ?

GULTEN TEPE : Nous avons le représentant de la délégation chinoise.

CHINE : Merci, Monsieur le Président. Je voulais rebondir sur l'un des sujets que nous avons identifiés pour cette séance, à savoir les blockchains. J'aimerais ajouter un élément et peut-être les NFT, les jetons fongibles. C'est en lien avec les blockchains. Il s'agit d'un identificateur particulier. Les NFT sont peut-être un sujet sur lequel nous voudrions nous pencher car ils ont un lien avec le DNS.

PRÉSIDENT NICO CABALLERO : Les NFT seront ajoutés à notre liste, les jetons fongibles.

Est-ce qu'il y a d'autres questions ou des commentaires ? S'il n'y en a pas, Julia, est-ce qu'il y a d'autres interventions ?

JULIA CHARVOLEN : Non.

PRÉSIDENT NICO CABALLERO : Très bien. Merci beaucoup.

Nous allons nous retrouver à 13 h 45 dans cette même salle. Merci beaucoup.

[FIN DE LA TRANSCRIPTION]