ICANN77 | Semaine de préparation – Point sur les modifications apportées au contrat d'utilisation malveillante du DNS
Mardi 30 mai 2023 – 14h00 à 15h30 DCA

MICHELLE WILSON: Bonjour, bienvenue à cette séance sur les amendements aux contrats relatifs à l'utilisation malveillante du DNS. Je serai responsable de la participation pour cette séance. Sachez que cette séance sera enregistrée et régie par les normes de comportement de l'ICANN.

Pendant la séance vous devrez utiliser la fenêtre questions/réponses si vous avez des questions. Toutes les questions du chat seront lues à voix haute au micro.

L'interprétation pour cette séance inclura le français, l'arabe, le russe, le chinois et le portugais. Cliquez sur l'icône d'interprétation dans Zoom et sélectionnez la langue dans laquelle vous allez écouter la séance.

Si vous souhaitez parler, veuillez lever la main dans Zoom et une fois que le facilitateur de la séance vous appellera, veuillez mettre en marche votre micro et prendre la parole. Avant de parler, assurez-vous de bien avoir sélectionné la langue dans laquelle vous parlerez dans le menu d'interprétation. Veuillez donner votre nom et la langue dans laquelle vous parlerez si ce n'est pas l'anglais. Assurez-vous d'éteindre tous les autres dispositifs et notifications quand vous parlerez. Parlez

clairement et à un rythme raisonnable pour permettre une bonne interprétation de vos propos.

Cette séance inclut une transcription en temps réel. Sachez que cette transcription n'est pas officielle et ne fait pas autorité. Pour la lire, cliquez sur le bouton Close Caption dans Zoom.

Pour assurer la transparence de la participation au modèle multipartite de l'ICANN, nous vous demanderons de vous inscrire en utilisant votre prénom et nom de famille. Il est possible que vous soyez retiré de la session si vous n'utilisez pas votre nom.

Russ, à vous.

RUSS WEINSTEIN: Merci, Michelle et merci à tous d'être avec nous. Je suis vice-président des comptes et services, révision des domaines mondiaux.

Dans mon équipe, nous sommes responsables des contrats et des relations avec les opérateurs de registre et bureaux d'enregistrement. Et je suis également responsable des programmes d'atténuation des menaces.

Aujourd'hui nous allons vous faire part d'informations sur des évolutions très anticipées, il s'agit des amendements relatifs aux contrats dans le cadre de l'utilisation malveillante du DNS. C'est un effort de toute la communauté, surtout de l'équipe stratégie et demande, l'équipe OCTO, la conformité et l'équipe de négociation des parties contractantes.

Pour m'aider à présenter aujourd'hui je suis avec Leticia Castillo, de l'informatique contractuelle, avec Owen Smigelski de Namecheap, des représentants des bureaux d'enregistrement et Chris Disspain qui est au groupe des représentants des opérateurs de registre.

Ensuite, diapositive suivante.

Alors, nous allons vous présenter un peu l'ordre du jour et vous donner un peu le contexte ainsi que la portée des amendements. Ensuite nous présenterons de manière générale les amendements, les nouvelles clauses, et ensuite il y aura une courte discussion sur l'utilisation malveillante du DNS, les techniques, les considérations du point de vue des parties contractantes. Nous vous fournirons des informations sur l'interprétation et l'applicabilité de ces amendements. Et ensuite nous présenterons un aperçu général du processus de la procédure globale pour mettre en place ces amendements, et ensuite nous aurons une partie questions/réponses.

Nous avons 90 minutes et nous espérons que nous aurons 30 minutes, si ce n'est pas 45 minutes pour la partie questions/réponses. Nous avons également une séance prévue pendant la semaine de réunion où nous pouvons davantage discuter de ces sujets.

Diapo suivante.

La période de commentaires publics a déjà démarré sur ces propositions d'amendements. Elle a été lancée hier et elle restera ouverte jusqu'au 13 juillet.

Donc 45 minutes pour prendre en compte le temps que nous allons consacrer à l'ICANN 77.

Voilà les changements qui ont été proposés. D'abord au RAA, celui-ci concerne la section 3.18. Il y a les propositions de changements au RAA, spécification 6 section 4 et spécification 11.3b. En plus, nous avons un document de soutien qui est en fait un conseil de l'ICANN qui aide à fournir les attentes de conformité relatives à ces obligations proposées.

Nous avons lancé ce travail en janvier et il vient de se terminer en mai. C'est assez rapide dans le contexte de l'ICANN. Cela veut dire qu'il y a eu une bonne coopération dans le cadre de cet effort puisque nous sommes arrivés à un résultat assez rapidement.

Je vais céder la parole à Chris qui va vous expliquer comment nous en sommes arrivés à ce point.

CHRIS DISSPAIN: Merci, Russ. Bonjour à tous. Je suis ravi de voir qu'il y a beaucoup de personnes qui nous écoutent aujourd'hui. J'espère que ce sera informatif et utile.

Je vais vous présenter un petit peu le contexte sur plusieurs diapositives et vous expliquer comment nous en sommes arrivés là.

Le point de départ c'est que les parties contractantes - en fait vous le savez tous, l'utilisation malveillante du DNS c'est un sujet de conversation depuis très longtemps, il y a différents points de vue là-dessus, il y a différentes parties de la communauté qui en parlent, selon

leurs perspectives, etc. Et donc les parties contractantes, en l'absence d'obligations fortes et applicables se demander comment interrompre ou entraver l'utilisation malveillante du DNS.

Nous nous sommes dit qu'il serait sans doute intelligent de commencer à y travailler. Donc voilà un peu le contexte sur la diapositive. Mais j'aimerais passer à la suivante qui est importante.

Voilà. Il y a eu deux étapes. Nous avons décidé qu'il fallait se mettre d'accord sur des changements significatifs et applicables pour élever la barre en fait. C'est ça la question. Ce n'est pas une question de meilleures pratiques mais d'élever le niveau pour avoir une norme minimale que tout le monde comprenne et qui soit acceptable.

Ensuite, nous nous sommes dit qu'il fallait le faire en créant des obligations pour atténuer l'utilisation malveillante du DNS. Et donc la portée de ces changements, c'est de traiter ces [inaudible] définis par la chambre des parties contractantes. Donc aucun sujet de divulgation de données d'enregistrement et pas d'obligation de clause de transfert de responsabilité.

Voilà où on en est. Et, ce que nous avons fait pendant 12 mois c'était pratiquement exactement il y a 12 mois que nous nous sommes rassemblés pour nous dire qu'il fallait faire les choses de cette manière.

Pour ceux qui sont à l'ICANN depuis longtemps, vous savez que c'est rapide d'être partis de cette étape il y a 12 mois et d'y arriver maintenant. C'est rapide.

Deuxième étape, processus communautaire. Nous sommes passés à cette étape après la première. Nous avons reconnu que le travail du processus d'élaboration de politique multipartite implique toute la communauté pour façonner les attentes de politique. C'est une étape importante. Ensuite il fallait qu'il y ait tout un échafaudage solide d'obligations contractuelles applicables, qui était un prérequis de manière à ce que ce soit applicable, entendu, compris et des politiques sur lesquelles on puisse travailler. Et, ensuite, il fallait donc que ces décisions permettent d'entraver toute utilisation malveillante du DNS.

Ensuite, les principes directeurs dans les amendements qui en sont sortis, donc se concentrer sur l'objectif cible d'interrompre ou d'entraver l'utilisation de noms de domaine à des fins d'utilisation malveillante du DNS. C'est l'objectif. Les bureaux d'enregistrement et les opérateurs de registre doivent agir rapidement pour atténuer lorsqu'un nom de domaine est utilisé à des fins malveillantes. Ensuite l'abus du DNS est très contextuel, donc les circonstances correspondant à chaque cas sont importantes, il n'y a pas de taille unique, une seule taille ne correspond à personne. En fin de compte, la question est le contexte : est-ce qu'il y a malveillance ? Et on en reparlera un petit peu plus après.

Les bureaux d'enregistrement et les opérateurs de registre ont besoin d'avoir une certaine discrétion dans le cadre de leurs actions et ces actions doivent être proportionnelles et prendre en compte la possibilité de dommage collatéral avant d'agir.

Et, enfin, et c'est très important, reconnaitre les différents rôles des bureaux d'enregistrement et des opérateurs de registre. Vous le verrez dans le détail après, il y a différents contrats, différents niveaux de changements suivant qu'on parle du contrat des bureaux d'enregistrement ou de celui des opérateurs de registre.

Donc les équipes de négociation des deux groupes ont travaillé pendant 12 mois en étroite collaboration avec l'ICANN. Et c'est deux équipes qui ont fourni leurs points de vue, principalement, et qui ont fait avancer les négociations. Mais, constamment en contact avec nos collègues pour avoir leurs points de vue.

Voilà, j'espère que ceci suffit en termes de contexte, qu'il y a suffisamment de détails ; et je suis là pour répondre aux questions si nécessaire.

RUSS WEINSTEIN: Merci, Chris. Nous allons passer à la diapositive suivante et nous allons vous présenter chacun des amendements proposés. D'abord les obligations des bureaux d'enregistrement.

Avant de passer à ce qui est nouveau, il ne faut pas oublier ce que nous avons déjà, ce qui existe. Les obligations relatives à l'abus dans l'accord des bureaux d'enregistrement se trouvent à la section 3.18 du RAA. Et l'obligation c'est d'agir de manière raisonnable et rapide pour faire l'investigation et répondre, de maintenir un point de contact, des coordonnées consacrées pour les forces de l'ordre, les agences de protection des consommateurs et puis donc informer ces autorités dans

les 24 heures, afficher publiquement des informations de contact sur les abus et entretenir des enregistrements relatifs à toute réponse, et reçu de signalement d'abus.

Donc ça, c'est la base. Et nous sommes partis de là pour réfléchir à ces obligations de traiter des cas d'abus.

Diapositive suivante.

Ce que nous avons essayé de faire, c'est donc d'ajouter aux obligations existantes dans la section 3.18, voilà un niveau très élevé de ce que nous avons fait. Nous avons d'abord clarifié les contacts des bureaux d'enregistrement pour qu'ils soient accessibles. Nous avons ajouté une obligation de fournir les confirmations d'accusé de réception des signalements d'abus.

Nous avons ajouté une définition de l'utilisation malveillante du DNS dans le cadre de ce contrat, précisément quelles sont obligations, de quoi parle-t-on.

Et, enfin, nous avons ajouté une nouvelle section, la 3.18.2, et c'est ceci qui est au cœur de l'obligation, d'agir en vue d'atténuer pour interrompre ou entraver l'utilisation malveillante du DNS. Et nous rentrerons dans le détail de tout ceci.

Diapositive suivante.

Alors, commençons par les nouvelles obligations et, en particulier, par le signalement d'un cas d'utilisation malveillante à un bureau d'enregistrement. Les contacts où envoyer ces signalements doivent

être disponibles sur la page, le bureau doit confirmer d'avoir ce signalement. Les bureaux d'enregistrement doivent utiliser soit une adresse email soit un formulaire web pour pouvoir recevoir ces informations, pourvu que ce formulaire soit facilement accessible à partir de leur page d'accueil. Les informations de contact et d'email doivent être clairement identifiées de sorte que le bureau d'enregistrement puisse contacter la personne qui signale le cas d'abus. Les adresses email publiques, en général, reçoivent énormément de pourriels, de spam et donc compliquent l'identification d'un vrai signalement de cas d'abus. Donc nous encourageons vivement l'utilisation des formulaires web.

Deuxième étape, le bureau d'enregistrement doit confirmer avoir reçu ce signalement d'utilisation malveillante, ce qui aide la personne qui dépose cette plainte ou qui signale ce cas d'abus à faire le suivi de leur signalement et de la création du dossier.

Si rien ne se passe, elle peut porter plainte par la suite au bureau de conformité contractuelle.

Et, finalement, ces exigences doivent être en lien avec les contacts indiqués à la réception de signalement du côté des forces de l'ordre.

Tout est spécifié maintenant dans le chapitre 3.18.3 au lieu de 3.18.2 comme auparavant.

Nous avons beaucoup travaillé à la définition d'utilisation malveillante du DNS. Dans ce contrat, comme dans le document récapitulatif et informatif que nous avons publié, aux fins du RAA, du RA et du

document, l'utilisation malveillante du DNS comprend les réseaux zombies, le hameçonnage, le dévoiement, le logiciel malveillant ou le spam quand il est utilisé comme mécanisme pour envoyer les autres formes d'abus de DNS.

Et donc tous ces termes sont définis dans la section 2.1 du document 515. Mais tout cela comprend ce que l'on entend pas utilisation malveillante du DNS.

Lorsqu'il y a des preuves claires qu'un nom enregistré est sponsorisé par un bureau d'enregistrement, est utilisé à des fins malveillantes et d'abus, le bureau d'enregistrement doit prendre les mesures d'atténuation appropriée immédiatement pour pouvoir interrompre ou empêcher l'utilisation malveillante de ce nom enregistré à des fins d'abus.

Les actions peuvent varier en fonction des circonstances, compte tenu de la cause et la profondeur des dégâts que génèrerait l'utilisation malveillante et la possibilité associée aux différents dommages collatéraux.

Et donc c'est ce qui représente les obligations du bureau d'enregistrement en fonction du RAA qu'il signe.

Voilà, en somme, les changements au contrat d'accréditation des bureaux d'enregistrement. Passons au contrat des opérateurs de registre.

Les contrats d'accréditation des opérateurs de registre sont similaires, nous allons tout d'abord voir les obligations existantes. Nous avons

d'une part la spécification 6 dans le chapitre 4 où les opérateurs de registre doivent publier et fournir à l'ICANN des détails de contact pour gérer des requêtes liées à des comportements malveillants dans le TLD et supprimer les registres orphelins lorsqu'ils sont utilisés pour des comportements malveillants.

Dans la spécification 11 du chapitre 3 a et 3 b, en fonction de laquelle ils sont tenus d'inclure une disposition dans leur accord avec les bureaux d'enregistrement leur interdisant d'entretenir certaines activités et leur exigeant de prendre des mesures pour les bureaux d'enregistrement qui entreprennent de telles activités, y compris la mise en suspension du nom de domaine, de mener périodiquement une analyse technique pour évaluer si les domaines sont utilisés pour générer des menaces à la sécurité. Et puis, ils doivent également élaborer des rapports statistiques avec la quantité de menaces à la sécurité qu'ils identifient.

Voilà ce qui correspond aux obligations contractuelles pour lutter contre l'utilisation malveillante du DNS, du côté des opérateurs de registre, donc très similaire à ce qu'on a vu déjà pour les bureaux d'enregistrement.

Diapo suivante.

Alors, pour revenir à la spécification 6 du chapitre 4, nous avons encore une fois précisé pour les opérateurs de registre qu'ils peuvent utiliser soit une adresse mail de contact soit un formulaire pour recevoir les signalements des cas d'abus. Et nous signalons et clarifions également qu'ils doivent confirmer la réception d'un tel signalement d'abus.

Diapo suivante.

Nous avons ajouté au contrat la même définition que nous utilisons avec les bureaux d'enregistrement. Donc cette définition s'applique à l'ensemble du contrat d'accréditation des opérateurs de registre et les termes utilisés sont définis à la section 2.1 du document SAC115.

Diapo suivante.

Nous avons ajouté les obligations d'atténuation d'utilisation malveillante pour les opérateurs de registre. Lorsqu'un opérateur de registre reçoit des preuves exploitables qu'un nom de domaine enregistré dans le TLD est utilisé à des fins malveillantes, l'opérateur de registre doit prendre les mesures d'atténuation appropriées immédiatement, dans la mesure du raisonnable, pour pouvoir arrêter ou empêcher l'utilisation d'un nom de domaine à des fins d'abus du DNS. Ce qui comprend la référence aux domaines qui sont utilisés pour l'abus du DNS ensemble avec les preuves et tout envoyer au bureau d'enregistrement le parrainant, ou la prise d'une mesure directe de la part de l'opérateur de registre s'il l'estime nécessaire. Et ces actions peuvent varier en fonction des différentes conséquences secondaires qu'aurait cette utilisation malveillante du DNS.

Diapo suivante.

Nous avons également apporté une légère modification à la spécification 11.3.b pour remplacer le terme « menace à la sécurité » avec le terme défini d'utilisation malveillante du DNS, ce qui clarifie l'analyse technique qui doit être effectuée pour évaluer si les noms de

domaine dans le gTLD d'un opérateur de registre est utilisé afin de générer une utilisation malveillante du DNS, ça précise également les rapports statistiques qui doivent viser à identifier les cas d'utilisation malveillante du DNS. Et cela définit également plus clairement ce qui doit être analysé et rapporté.

Et tout cela aux fins d'atténuer l'utilisation malveillante du DNS.

Voilà, en somme, les modifications que nous avons apportées aux deux types de contrats. Je vais maintenant passer la parole à Owen qui va nous parler des techniques et des considérations pour l'atténuation de l'utilisation malveillante du DNS.

OWEN SMIGELSKI: Merci. Je suis le co-président de l'équipe de négociation du groupe des représentants des parties prenantes des bureaux d'enregistrement.

Diapo suivante.

Alors, Russ nous disait que les mesures d'atténuation de l'utilisation malveillante du DNS ne sont pas générales, on n'a pas de recette miracle et chaque cas doit être évalué individuellement. On ne peut pas automatiser la prise de mesures parce qu'il y a énormément d'informations dans le rapport lui-même, qui doit être évalué, mais il y a également des informations qui doivent être disponibles pour les bureaux d'enregistrement et les opérateurs de registre, à savoir les informations du client, le nom de domaine, et d'autres mesures qui pourraient être prises pour évaluer la situation par l'opérateur de

registre et par le bureau d'enregistrement avant qu'on ne puisse atténuer l'utilisation malveillante du DNS.

Et, malheureusement, ce n'est pas une question de recette miracle pour lutter contre l'utilisation malveillante du DNS, c'est un peu plus complexe et détaillé.

Du côté des bureaux d'enregistrement et des opérateurs de registre, l'outil qu'on a est la mise en suspension du nom de domaine. Ce qui peut se faire de diverses manières, à savoir le nom de domaine ne peut plus générer une utilisation malveillante ou un abus. Il ne va pas être résolu, il ne va amener nulle part, il ne va plus fonctionner. Et ça peut être annulé, comme mesure. Donc ça fonctionne.

Du point de vue d'un bureau d'enregistrement, ça peut se faire en envoyant le code de statut [inaudible] au bureau d'enregistrement. Du côté de l'opérateur de registre le code correspond à Serveur Hold.

Il y a également d'autres moyens pour que l'opérateur de registre ou le bureau d'enregistrement agissent, il s'agit de mesures plus drastiques. Ils peuvent supprimer le nom de domaine de la zone, il disparait complètement, mais il y a également d'autres manières d'agir qui sont un peu moins drastiques. Et cela va varier en fonction du type d'abus qui est signalé et des circonstances.

D'autres manières appropriées de prendre des mesures pour pouvoir atténuer, empêcher ou arrêter l'utilisation malveillante du DNS sont de travailler avec le fournisseur des services d'hébergement qui peut souvent mieux voir ce qu'il se passe dans un réseau, ce qu'il y a. Ou peut-

être que le bureau d'enregistrement n'est même pas au courant de ce qu'il s'y passe.

Et je signale ici que même si le bureau d'enregistrement est souvent le fournisseur de service d'hébergement, ce n'est pas nécessairement le cas. Et il existe des noms de domaine pour lesquels il y a deux entités différentes qui s'occupent de ces deux fonctions. Voilà pourquoi le fournisseur de service d'hébergement ou le bureau d'enregistrement seraient en général les contacts qui peuvent agir le plus rapidement.

Mais il y a également le verrouillage d'un nom de domaine, c'est-à-dire qu'on ne peut plus transférer ce nom de domaine à un autre bureau d'enregistrement, ce qui pourrait probablement être un peu moins extrême dans la manière d'aborder l'utilisation malveillante.

On peut également rediriger un nom de domaine pour qu'il ne puisse plus accéder à un fournisseur abusif. Et ça permet de contrôler ce qui arrive avec les réseaux zombies par exemple, mais ça peut être utilisé pour identifier et aider les victimes en général et ça permet d'enregistrer quel est le trafic qui a lieu entre les serveurs de noms.

Et puis on peut également escalader ces évidences exploitables que l'on a et tout transférer à quelqu'un qui puisse être plus à même de prendre des mesures susceptibles d'arrêter l'utilisation malveillante du DNS.

Diapo suivante.

Nous avons parlé de domaines compromis et de dommages collatéraux. Les noms de domaine qui font partie de l'abus ne sont pas tous enregistrés à ces fins. Il y a un grand pourcentage de noms de domaine,

je ne sais plus quel est le pourcentage spécifique, mais il y a un grand pourcentage de noms de domaine qui sont enregistrés à des fins légitimes et qui sont compromis. C'est-à-dire que sans la connaissance du titulaire du nom de domaine, quelqu'un prend des mesures pour contrôler l'ensemble ou une partie d'un nom de domaine. Et, dans ces cas-là, souvent, la suspension dont on parlait avant pourrait ne pas être la mesure à prendre.

On a peut-être un site web qui fait partie d'un nom de domaine qui est plus grand et ça peut faire partie d'une université, d'un hôpital ou un autre nom de domaine qui correspond à un site qui comprend énormément de pages et de trafic où seul un petit pourcentage du trafic est utilisé à des fins abusives.

Et dans ce type de cas, il est mieux de ne pas mettre en suspension mais de travailler directement avec le bureau d'enregistrement ou le fournisseur de service d'hébergement.

Par exemple, à ICANN 76 à Cancún, le groupe des représentants des bureaux d'enregistrement a annoncé l'accès à un site web que nous avons créé pour rechercher des informations à propos des bureaux d'enregistrement et des fournisseurs d'hébergement, ce qui est utile au moment de lutter contre les utilisations malveillantes. .Alors, une semaine plus tard, ce site web a été la cible d'énormément d'attaques de DDOS et, finalement, une partie du site web a pu être compromise. Et donc au lieu de supprimer tout le site, nous avons travaillé avec notre équipe technique pour supprimer ce plugging qui avait été compromis. Nous l'avons mis à jour, nous avons entrepris les mesures nécessaires

pour pouvoir résoudre cela. Ce qui veut dire que le site web était toujours opérationnel et aidait les utilisateurs à signaler ou à identifier des cas d'abus du DNS.

Cela est également valide lorsqu'il y a un sous-domaine au 3ième niveau, c'est-à-dire qu'un bureau d'enregistrement ou un opérateur de registre n'est plus impliqué à ce niveau-là, c'est un TLD de troisième niveau, car ils ne travaillent pas au-delà du deuxième niveau. Donc s'ils identifient un problème, ils doivent mettre en suspension tout le domaine à partir du second niveau. Ils ne peuvent pas faire autrement.

Comme on ne veut pas générer des dommages collatéraux pour le titulaire du nom de domaine, on travaille avec tout le monde, avec toutes les parties prenantes pour nous assurer que l'utilisation malveillante soit résolue ou atténuée sans que ce soit nuisible pour l'ensemble du nom de domaine.

Voilà tout de mon côté.

LETICIA CASTILLO: Oui, je vais prendre la suite. Je suis avec la conformité contractuelle de l'ICANN. ICANN Org a produit un conseil ou un avis préalable pour réfléchir à ces nouvelles exigences. Cet avis contient est posté dans la page de commentaires publics, il a été mis en place et il décrit les nouvelles exigences ainsi que leur applicabilité et applications.

Nous y répétons que toutes les obligations existantes demeurent et continueront d'être applicables.

Ensuite il y a des termes clefs par rapport aux actions d'atténuation concernant les noms de domaine. Donc redirection et autres actions, expliquées par Owen. Il y a également dans cet avis plusieurs exemples des différentes instances d'utilisation malveillantes du DNS et des actions d'atténuation qu'une partie peut entreprendre pour interrompre l'utilisation de ce nom de domaine à des fins d'utilisation malveillante du DNS. Et donc, pour interrompre cet abus du DNS en lien avec le nom de domaine.

Nous y expliquons également la révision que la conformité contractuelle de l'ICANN effectuera pour déterminer si oui ou non il y a un lancement de cas, avec la partie contractante.

Diapositive suivante.

Dans le cadre du processus, nous allons appliquer ces obligations via le traitement de plaintes externes reçues par notre plateforme qui y est consacrée, mais nous surveillerons également et nous mettrons en place des activités d'audit.

Cet avis explique comment nous ferons une révision complète de chaque cas, y compris les enregistrements de plainte et autres informations disponibles, telles que les données affichées dans le RDDS, dans le DNS Look Up pour voir quelles sont les informations que nous avons sur le domaine.

Pour toute plainte valide, nous lancerons un dossier avec la partie contractante et nous demanderons pour déterminer quelle est la conformité. Généralement, nous devrions recevoir une explication de

l'initiative entreprise, de la rapidité de cette initiative et de la décision d'interrompre ou d'entraver, suivant le cas. Ceci inclura toute explication applicable relative à la disproportionnalité des actions au niveau du DNS et tout dommage collatéral. S'il n'y a pas de preuves exploitables, nous demanderons également une explication de pourquoi et quelle est l'évaluation qui a été mise en place.

Et, comme nous le faisons dans d'autres cas, y compris pour des obligations d'abus, la conformité collectera des moyens de mesure par rapport à ceci pour que la communauté soit informée.

Voilà, c'est tout pour cet avis. Et je vais maintenant passer la parole à Russ.

RUSS WEINSTEIN: Merci. Je vais maintenant conclure avec quelques diapositives qui décrivent le processus par rapport à cette proposition d'amendement et à son entrée en vigueur.

C'est un processus qu'on appelle la procédure d'amendement globale ORA et ORAA. Cela peut, peut-être, vous sembler familier puisque nous venons d'utiliser cette procédure pour les changements en 2013 au RAA pour ajouter le protocole d'accès aux données d'enregistrement, donc le RDAP. Nous l'avions également utilisé en 2017 pour un amendement global au RA de base.

Pour résumer, il s'agit d'une renégociation, d'une période de commentaires publics. Il y aura un vote par les parties contractantes. Il y aura leurs considérations d'approbation et ensuite l'entrée en vigueur.

Le RAA est un petit peu plus clair parce qu'ils ont à peu près tous le même. Pour les opérateurs de registre il y a le RA de base, mais il y a quelques-uns d'entre eux qui n'utilisent pas ce RA de base, le .COM et le .NET sont dans cette situation. Mais pour la plupart, ils se sont déjà engagés à adopter ces changements, s'ils sont appropriés, dans le cadre d'une lettre d'intention qui est incluse dans notre négociation. Il y avait une lettre d'intention avec VeySign pour élaborer et pour inclure des obligations d'atténuation d'abus du DNS. Et donc cette obligation est maintenant proposée dans le cadre du contrat du .NET qui va bientôt être renouvelé.

Donc tous les grands TLD seront couverts par ces changements s'ils sont approuvés, ce qui est très bien parce que cela couvre à peu près tous les enregistrements de TLD.

Diapositive suivante.

Donc, je ne reviens pas sur tous les détails, mais vous savez qu'il y a des seuils qui doivent être atteints pour approbation, donc ils doivent revoir et approuver ces amendements. Il faut 2/3 de la majorité par rapport au montant total des frais payés et les frais payés, c'est à la fois les TLD et les noms enregistrés dans ces TLD. Et donc c'est à ce moment-là qu'il y aura une approbation s'il y a un résultat aux 2/3.

Et pour les bureaux d'enregistrement le seuil est de pratiquement 90 %, donc plus élevé par rapport aux noms enregistrés, et 90 % des bureaux d'enregistrement doivent voter oui pour l'approbation de ces amendements.

Donc nous devons travailler avec eux pour nous assurer d'avoir les voix pour approuver ces amendements qui sont tout à fait positifs pour notre écosystème.

Diapo suivante.

Voilà le processus global, je l'ai déjà dit au début, mais donc nous étions à la négociation, nous sommes maintenant à la phase de commentaires publics et voilà un petit peu la ligne du temps, la chronologie de ce processus. Nous reverrons les commentaires à la fois du point de vue des parties contractantes et du point de vue de l'ICANN pour voir s'il y a des changements à apporter à ces amendements avant de finaliser. Et ensuite il y aura un vote et donc l'objectif pour ce vote est au quatrième trimestre de cette année, entre octobre et décembre. Et si on atteint le seuil de majorité, pour les deux groupes, et bien nous présenterons ceci au conseil d'administration au premier trimestre 2024.

Si c'est approuvé, ces amendements pourraient être inclus au contrat avant la fin de l'année, ce qui – encore une fois – est avancé à la vitesse de l'éclair dans le cadre de l'ICANN.

Donc nous sommes très heureux d'en être déjà là. Nous ne pourrons qu'aller plus vite et avancer mieux. Et donc nous attendons avec impatience de lire vos commentaires.

Dernière diapositive.

Ici, avant de lancer la partie questions/réponses, d'ailleurs je vois qu'il y a déjà des questions qui ont été postées, nous avons une séance de sensibilisation pour la chambre des parties contractantes pendant

l'ICANN 77, ce sera le 13 juin à 13 h 45, le mardi. Donc venez nous rejoindre si cela vous intéresse. Voilà, donc il y aura également une partie questions/réponses pendant cette séance.

Je remercie les intervenants, merci de nous avoir écoutés. Maintenant nous sommes à votre disposition pour vos questions.

Un petit instant, nous allons lire les questions et nous pouvons également vous écouter si vous voulez poser votre question à voix haute.

YUKO YOKOYAMA: On pourrait peut-être commencer par les questions posées oralement, Russ ?

Donc s'il n'y en a pas je vais commencer par lire les questions.

Première question de Sivasubramanian : est-ce que le rôle de l'opérateur de registre se termine lorsqu'il a éliminé un domaine malveillant comme mesure d'atténuation ? Est-ce que ce ne serait pas utile si l'opérateur de registre et le bureau d'enregistrement partageaient des informations pour identifier les modèles, les empreintes des abuseurs et s'ils s'aident les uns et les autres à identifier les titulaires abusifs, les acteurs malveillants ? Qui veut répondre à cette question ?

RUSS WEINSTEIN: Je peux répondre. Alors merci pour la question. C'est une excellente question. Nous en avons déjà parlé au début, au cœur de cet effort l'idée

était de définir un niveau pour l'utilisation malveillante du DNS. L'objectif de ce niveau, de cette barre, c'était de créer des obligations lorsqu'on observait une utilisation malveillante du DNS, que ce soit au niveau du bureau d'enregistrement ou du TLD. Donc, on pourrait se dire que ceci est en dehors de la portée de notre travail, mais il y a une discussion qui a lieu à ce niveau dans notre groupe. Donc n'oubliez pas votre question, je crois qu'il pourrait y avoir des réponses à l'avenir.

YUKO YOKOYAMA: Autre question de Sivasubramanian : si les abus sont identifiés au troisième niveau ou à un niveau plus profond, est-ce que ceci réduit la responsabilité ou la redevabilité de l'opérateur de registre ou du bureau d'enregistrement ?

RUSS WEINSTEIN: Est-ce que vous voulez répondre à cette question, Leticia ?

LETICIA CASTILLO: Est-ce que vous pouvez répéter la question ?

YUKO YOKOYAMA: Est-ce que ceci élimine la responsabilité si l'abus est à un niveau plus profond que le deuxième niveau ?

LETICIA CASTILLO: La responsabilité c'est d'agir et d'atténuer lorsqu'il y a une preuve comme quoi le domaine est utilisé à des fins malveillantes. Donc nous

reverrons tous les détails de ce dossier et il est tout à fait possible que si l'abus est au troisième niveau nous ayons besoin que le bureau d'enregistrement ou l'opérateur de registre évaluent et nous disent s'il y a suffisamment de preuves comme quoi le domaine est utilisé à des fins malveillantes. Donc cela n'élimine pas l'obligation, mais comme dans tous les autres cas, il nous faut les détails. C'est très spécifique à chaque affaire. C'est difficile de répondre oui ou non en fait, ça dépendra.

RUSS WEINSTEIN: Merci, Leticia.

YUKO YOKOYAMA: Question suivante de Brian King, on a déjà répondu un petit peu à cette question par écrit. Il semblerait que c'est un changement d'approche bienvenu. Comme suivi, est-ce qu'avec l'ICANN vous pourriez partager le raisonnement derrière les différentes normes apparentes dans le RA et dans le RAA ? De manière plus spécifique pourquoi dans le RA l'obligation mentionne une détermination raisonnable alors que dans le RAA l'obligation est déclenchée lorsque le bureau d'enregistrement a des preuves exploitables ? Est-ce qu'on pourrait répondre à Brian King ? Russ ?

RUSS WEINSTEIN: Oui. Merci. Donc effectivement, le texte est un petit peu différent. La différence principale c'est reconnaitre le rôle de l'opérateur de registre et du bureau d'enregistrement. Le bureau d'enregistrement, c'est un

petit peu la pointe en fait de la lance dans la lutte contre l'abus du DNS puisqu'il est en lien avec le titulaire de nom de domaine. Donc lorsqu'il a des preuves exploitables il peut déterminer, voir quoi faire. L'opérateur de registre pourra agir directement s'il a des preuves ou alors il pourra renvoyer le dossier au bureau d'enregistrement.

Donc une toute petite nuance dans le langage ou le texte, mais de toute façon, le bureau d'enregistrement et l'opérateur de registre ont tous les deux à agir.

YUKO YOKOYAMA: Merci, Russ. Questions suivantes, peut-être qu'on peut les mettre ensembles, toutes les deux d'Alan Greenberg. La première : quand est-ce que les changements du RAA seront en vigueur pour l'opérateur de registre ? Deuxième question : quand est-ce que les changements au RAA entreront en vigueur ? Immédiatement ou dans 5 ans ?

RUSS WEINSTEIN: Je vais répondre à cette question. Si tout va bien selon le plan, les contrats avec les bureaux d'enregistrement et les opérateurs de registre pourraient entrer en vigueur au deuxième trimestre de l'année prochaine. C'est un petit peu l'idée, cela dépendra des différentes étapes dans le processus, si tout fonctionne comme prévu. Mais, dans le meilleur des cas, ce sera deuxième trimestre de l'année prochaine.

YUKO YOKOYAMA: Merci. La question suivante est de Rick Lance qui demande quel le pourcentage du vote de VerySign suivant ces critères pour le transfert pour le transfert de responsabilité entre opérateurs de registre.

RUSS WEINSTEIN: Alors, il ne vote que pour les TLD pour lesquels ils ont postulé dans la série 2012. C'est-à-dire les TLD qu'ils ont demandés à ce moment-là. Les contrats historiques ne participent pas au vote pour les contrats de registre de base. Mais, comme je le disais, ils se sont engagés à entreprendre ces amendements à travers une lettre d'intention qu'ils ont ajoutée à leur contrat. Donc ils ont participé au processus tout au long des négociations, ils ont toujours soutenu cette initiative.

YUKO YOKOYAMA: Merci. Question suivante de [Inaudible] : comment les bureaux d'enregistrement et les opérateurs de registre peuvent-ils faire la distinction entre une utilisation malveillante du DNS au niveau technique et au niveau du contenu ? À quel niveau l'utilisation malveillante du DNS devrait-elle être évitée et empêchée ? Qui devrait être responsable de définir cette limite ?

OWEN SMIGELSKI: Très bien. Je répondrai à cette question. Merci pour cette question. Je vais commencer par cela, le plus souvent on s'en rend compte à simple vue. Russ nous disait pendant la présentation qu'il s'agit d'une définition très spécifique de l'utilisation malveillante du DNS et de ce à quoi s'appliqueront ces modifications. Alors, ça correspond aux spams,

aux réseaux zombies, au dévoiement, à l'usurpation de nom de domaine. C'est technique, on n'a pas défini l'utilisation malveillante comme quelque chose qui est en lien avec les contenus.

C'est beaucoup plus facile parce que toutes les parties prenantes peuvent se mettre d'accord sur cette définition, c'est une définition qui peut être utilisée partout dans le monde. Alors que l'utilisation malveillante au niveau des contenus peut varier selon la région, selon le type de partie prenante.

Donc ce n'est pas qu'on ignore l'abus au niveau des contenus, mais ça ne fait pas partie de nos amendements. La communauté de l'ICANN continuera à agir là-dessus, ce n'est qu'une première mesure, il y en aura une deuxième et une troisième, sans doute, mais cela appartiendra à la communauté de l'ICANN de considérer ce qui correspond à un abus de contenu.

Alors, qui va s'occuper de définir ces limites ? Ce sera la communauté de l'ICANN. Mais, du côté des bureaux d'enregistrement, si un abus est lié au contenu, parfois on pourra agir, mais c'est très spécifique au type d'abus. Merci.

YUKO YOKOYAMA: Merci, Owen. Y a-t-il un représentant de l'ICANN qui souhaite intervenir ? Autrement je passe à la question suivante.

RUSS WEINSTEIN: Non, je pense qu'Owen a tout répondu.

YUKO YOKOYAMA: Très bien. La question suivante est de [Inaudible] qui nous demande : ce processus d'atténuation et révision de l'utilisation malveillante du DNS détaillé et exhaustif au sein de la communauté de l'ICANN n'est-il pas trop lent pour pouvoir arrêter véritablement les attaques malveillantes par les acteurs malveillants ? Quelles sont les stratégies existantes pour garantir que l'on puisse identifier rapidement l'abus et entreprendre des mesures pour s'y prendre ?

RUSS WEINSTEIN: Je pense pouvoir répondre. Ce processus a été un peu lent, peut-être, ce que font périodiquement les bureaux d'enregistrement et les opérateurs de registre est de recevoir des signalements de la part de la communauté et des utilisateurs, ils ont toujours eu ces données de contact et ils doivent évaluer et examiner et prendre les mesures nécessaires pour atténuer cet abus lorsqu'il y a des preuves exploitables. Beaucoup de bureaux d'enregistrement et d'opérateurs de registre sont également abonnés aux services qui fournissent des informations sur les menaces à la sécurité qui circulent sur internet. Ils suivent ces rapports constamment et ils vont réagir du mieux possible pour pouvoir prendre des mesures.

Et puis les bureaux d'enregistrement comme les opérateurs de registre ont des exigences en lien avec des activités de délinquances et aux forces de l'ordre. Lorsque les forces de l'ordre et les différents organismes leur demande de prendre des mesures pour lutter contre un

comportement spécifique, ils vont agir presque en temps réel, dans les 24 h.

Donc je pense que ce qu'on a ici n'est pas un processus lent ou excessivement complexe, les bureaux d'enregistrement et les opérateurs de registre peuvent identifier les cas d'abus et agir au niveau de leur registre et ils sont prêts à le faire.

Je ne sais pas si Owen ou les veulent veulent ajouter quelque chose ?

OWEN SMIGELSKI: Oui, moi je veux rebondir là-dessus. C'est très bien dit. Effectivement, ce n'est pas quelque chose qui est nécessairement lent. Il est difficile de savoir ce qui en résultera. On ne veut pas supposer que quelqu'un est coupable avant qu'il ne fasse quoi que ce soit. Donc il peut être très compliqué d'arrêter un nom de domaine, si nous le mettons en suspend en général ce sera un manquement au contrat que nous avons signé avec notre client. Et donc la nature de nos actions doit être réactive et non pas prédictive. Voilà pourquoi il y a différents moyens pour signaler l'utilisation malveillante auprès des bureaux d'enregistrement et des opérateurs de registre. Et donc ça ne peut pas prendre des jours, des semaines, des mois, mais c'est en l'espace de quelques jours, quelques heures et même de minute qu'on doit agir surtout lorsqu'on a clairement identifié un cas d'abus.

Donc ici, nous travaillons tous ensemble pour définir quels sont les moyens d'agir et comment toutes les parties contractantes doivent entreprendre ces actions.

Et tout au long de la présentation, je pense qu'on a montré les actions que les bureaux d'enregistrement et les opérateurs de registre entreprennent déjà. Ce que nous faisons c'est clarifier tout cela, mettre noir sur blanc pour que ce soit clair pour tous et pour que ce soit de bonnes pratiques et que cela corresponde à une approche de toute l'industrie à l'avenir. C'est ce que nous essayons de faire, ce n'est pas une nouveauté. Merci.

YUKO YOKOYAMA: Merci à tous les deux. Je n'ai plus de question à travers la fonction questions/réponses, je recède la parole à Michelle.

MICHELLE WILSON: Merci, Yuko. Si vous avez d'autres questions ou si vous souhaitez intervenir, levez la main sur Zoom, quand le facilitateur vous l'indiquera, veuillez allumer votre micro et prendre la parole. Avant d'intervenir, veuillez sélectionner la langue dans laquelle vous voulez intervenir à partir du menu d'interprétation de Zoom. Dites votre nom et la langue dans laquelle vous allez parler si ce n'est pas l'anglais.

YUKO YOKOYAMA: Merci, Michelle. Je vois que Jonathan Zuck a levé la main. Jonathan, nous vous invitons à allumer votre micro et poser votre question.

JONATHAN ZUCK : Merci. Je suis Jonathan, de l'ALAC. J'ai envoyé ma question et elle a été répondue par écrit, d'une certaine manière, mais je sens que ma

question n’est pas complètement répondue. Et je pense que ce changement est motivé en partie par ce que disait Owen, cet essai d’avoir une réaction normalisée face à l’utilisation malveillante du DNS.

Et, par le passé, il y a eu des discussions où on disait que ceux qui n’agissent pas suivant les normes ou qui étaient plus généralement longs, ou quel que soit le terme, en général on parlait d’acteurs malveillants mais c’est un terme qui n’est pas toujours utilisé à juste titre, mais en tout cas pour prendre des mesures, les parties contractantes qui, pour une raison ou une autre, refusent de répondre doivent maintenant se conformer à ces nouvelles mesures.

Donc ma question, si vous voulez, est que je voudrais savoir si le service de conformité contractuelle considère que ces nouvelles dispositions donnent aux opérateurs de registre et bureaux d’enregistrement suffisamment d’outils pour que, face à un patron de négligences, face à un processus normalisé, il soit tenu de suspendre ou de révoquer un contrat pour un bureau d’enregistrement ou un opérateur de registre.

J’espère que ma question est claire, mais je voulais savoir si le service de conformité contractuelle a suffisamment d’outils pour pouvoir révoquer ce contrat face à un manquement constant.

YUKO YOKOYAMA: Qui souhaite répondre ?

LETICIA CASTILLO: Je vais commencer et puis Jamie pourrait également intervenir si elle le veut.

Alors, les modifications permettent une plus grande flexibilité pour reconnaitre que les actions nécessaires doivent être entreprises, mais toutes les mesures devraient viser à lutter contre l'utilisation malveillante du DNS. Ce n'est pas une question de résiliation de contrat. Lorsqu'on identifie un cas d'utilisation malveillante, on vérifie qu'il y a des actions d'atténuation qui ont été entreprises compte tenu de tous les détails associés à ce cas-là.

Si on ne reçoit de telles preuves, on suit un processus ordinaire et on l'utilise pour pouvoir faire appliquer les normes.

Peut-être que Jamie pourra ajouter à cela, mais en général, nous allons faire appliquer ces mesures d'atténuation dans les circonstances qui sont expliquées dans le RAA. Et vous trouverez tous ces détails dans le document récapitulatif.

JAMIE HEDLUND: Merci pour cette question. Je n'ai pas beaucoup d'autre chose à dire, outre ce qu'a déjà dit Leticia. Si vous avez d'autres questions, nous pouvons y répondre ensuite ou si vous voulez on peut continuer cette discussion à la fin de la réunion.

Dans le document nous avons énormément d'informations sur les manières dont nous comptons appliquer ces nouvelles modifications. Du point de vue de la conformité contractuelle, ce serait un grand changement que de pouvoir mettre en œuvre ces modifications. Et il

faut les reconnaitre surement comme un premier pas. Nous espérons bien sûr pouvoir accumuler plus d'expérience au fil du temps pour pouvoir aider la communauté et l'aider à lutter contre l'utilisation malveillante du DNS et mettre en œuvre ces nouvelles obligations dès lors qu'elles seront approuvées.

JONATHAN ZUCK : Merci.

YUKO YOKOYAMA: Très bien. Leticia, Jamie. Je ne vois pas d'autres mains levées. Croyez-vous qu'on devrait attendre encore une trentaine de secondes avant de clore cet appel ?

Toujours pas de question ni de main levée. Ah, attendez, je viens de voir apparaitre une nouvelle question, donc nous n'allons pas lever la séance. Une question de Steinar Grotterod qui demande : les preuves seront-elles vérifiées vis-à-vis des données enregistrées dans le DAAR ?

OWEN SMIGELSKI: Oui, je peux répondre très rapidement et je cèderai la parole à John. Merci pour cette question. Le DAAR, le travail de l'ICANN, tout cela est utile, ça nous montre les progrès. Mais du point de vue des bureaux d'enregistrement, je dirais qu'on n'a pas d'accès au DAAR et donc ce n'est pas une considération que l'on a. Une plainte d'utilisation malveillante doit être bien fondée, doit être exploitable, on devrait pouvoir voir la plainte et prendre les mesures nécessaires

correspondantes. On ne doit aller chercher ailleurs, demander à d'autres personnes ou quoi que ce soit. Ce sont des exigences pour être sûr que ces preuves soient apportées. Parce qu'il est parfois difficile de voir à quoi correspond quelque chose ou des abus qui sont spécifiques à un emplacement.

John peut nous parler plus du DAAR.

JOHN: Merci, Owen. Donc cet outil de signalement, le DAAR, est basé sur les données de réputation, donc c'est ce que disent les gens sur les noms de domaine, ce n'est pas nécessairement quelque chose qui est prouvé par des données probantes. Il y a différentes normes, il y en a qui sont plus strictes que d'autres. Donc non, il n'y aura pas de lien direct.

Le DAAR, avec ses données de réputation, est indicatif. C'est donc un moyen de continuer de faire des recherches par rapport à certaines preuves.

Nous avons d'autres projets au bureau du CTO, nous avons le DNS Sticker qui existe depuis un moment et qui permet de signaler aux bureaux d'enregistrement sur la base de preuve. En général, ça peut donner lieu à des actions. Mais le DAAR n'est pas un outil qui présente des preuves.

RUSS WEINSTEIN: Merci. Pardon, Yuko.

YUKO YOKOYAMA: Je voulais simplement dire qu'il n'y a plus de question et que je ne vois pas de main. Donc je vous recède la parole.

RUSS WEINSTEIN: Merci à tous, la période de commentaires publics est lancée, regardez le document, consultez-le et partagez votre feedback. Si vous êtes à Washington, ou si vous participez à distance, venez nous rejoindre le mardi 13 et on pourra discuter davantage.

En tout cas je vous souhaite une excellente Prepweek et à tous ceux qui voyageront je vous souhaite un excellent voyage.

MICHELLE WILSON: Nous allons maintenant interrompre l'enregistrement, la séance est levée.

[FIN DE LA TRANSCRIPTION]