ICANN80 | Forum de politiques – ccNSO : amendements des RA et RAA - que peuvent apprendre les ccTLD ?
Mardi 11 juin 2024 – 13h45 à 15h00 KGL

CLAUDIA RUIZ : Bonjour, et bienvenue la séance sur les amendements RA et RAA que doivent avoir les ccTLD. Je suis accompagnée de mes collègues Bart et Joe et nous sommes responsables de la participation à distance pour cette séance.

Veuillez noter que cette session est enregistrée et qu'elle est régie par les normes de comportement attendues à l'ICANN.

Au cours de cette session, les questions ou commentaires soumis dans le chat ne seront lus à voix haute que s'ils sont formulés correctement, comme expliqué dans le chat. Je lirai les questions et commentaires à haute voix pendant la durée fixée par le président ou le modérateur de cette session.

L'interprétation pour cette session comprendra l'anglais, l'espagnol, le français et l'arabe. Cliquez sur l'icône d'interprétation dans Zoom et sélectionnez la langue que vous écouterez cette session. Si vous souhaitez prendre la parole, levez la main dans la salle Zoom et une fois que l'on donnera votre nom. Avant de prendre la parole, assurez-vous d'avoir sélectionné la langue dans laquelle vous allez vous exprimer.

Veuillez indiquer votre nom pour l'enregistrement, mettez tous vos instruments en sourdine. Veuillez parler lentement pour permettre une interprétation adéquate.

Cette session comprend une transcription en temps réel. Veuillez noter que cette transcription n'es pas officielle et ne fait pas autorité. Pour la visualiser, cliquer sur le bouton close caption dans la barre d'outils Zoom.

Pour assurer la transparence de la participation au modèle multipartite de l'ICANN, nous vous demandons de vous connecter aux sessions Zoom en utilisant votre nom complet.

Avec cela, je vais passer la parole à Nick.

NICK WENBAN-SMITH : Merci beaucoup et bienvenue à cette session. Nous pensons pouvoir partager de très bonnes informations et nous allons vous éduquer sur le comité.

Je suis conseillé général pour l'opérateur de registre .UK.

Quelques points de logistique. Nous allons discuter des éléments d'un univers parallèle des gTDL, sachant qu'il y a eu beaucoup de changements ces dernières années. Tout d'abord, l'objectif de cette séance est de sensibiliser les personnes sur ce qui a été au niveau des modifications et changements ces derniers temps, à savoir quels sont les impacts sur les ccTLD.

Une mission assez simple et nous allons voir si vous pouvons accomplir tout cela.

Lorsqu'il s'agit d'utilisation malveillante, je voudrais faire quelques commentaires d'introduction.

Tout d'abord, au Royaume-Uni, nous avons des élections en ce moment et durant les élections, des personnes adorent apporter des statistiques ou des déclarations de statistiques. Par exemple, la semaine dernière le gouvernement a dit que tous les foyers au Royaume-Uni devaient payer plus de 2000 livres sterling en impôts. Il y a plein de choses comme ça.

Pour nous, la communauté ccTLD, nous avons beaucoup moins d'enregistrements malveillants que les gTLD, dis fois moins. Et, d'ailleurs, au contraire des commentateurs sur la politique, je peux vous dire mes données sont basées sur des évidences, sur des preuves.

À Hambourg, nous avons eu une session sur les outils et les outils de mesures et nous avons maintenant en place des outils pour mesurer, justement, ces abus malveillants pour les ccTLD. Nous avons donc beaucoup de ressources. D'ailleurs nous n'avons pas constaté beaucoup d'utilisation malveillante que pour les ccTLD.

Donc lorsqu'il s'agit des opérateurs de gTLD, des bureaux d'enregistrement, on sait que pour ce qui des registrares les données sont beaucoup plus intéressantes que pour les ccTLD.

Au Royaume-Uni, par exemple, nous avons eu une petite augmentation des utilisations malveillantes des enregistrements. Cela s'est produit quand le domaine TK a été lancé. Nous savons que les gTLD vont pouvoir s'améliorer pour ce qui est de gérer les utilisations malveillantes. Donc les ccTLD deviendront, évidemment, beaucoup plus ciblés.

Alors, dans ce secteur, que nous soyons des ccTLD ou des gTLD, nous sommes toujours des TLD. Donc il nous faut unir nos intérêts et nous savons qu'il y a là une grande opportunité de pouvoir collaborer à travers les réseaux. Donc, c'est dans l'intérêt de tous, dans cette salle, car nous savons que c'est moralement correct et c'est dans l'intérêt des activités de tous de collaborer pour que notre industrie, notre secteur, reste en bonne santé.

Alors, dans ce sens, je suis heureux de pouvoir vous dire que nous avons des experts divers et nous allons pouvoir recevoir la perspective de consulter avec beaucoup de personnes. Nous avons James Bladel qui est vraiment expert de gTLD, il a même un ccTLD, il fait partie aussi du conseil des opérateurs de ccTLD. Donc il pourra vraiment nous parler de cette perspective.

Ensuite, nous aurons un autre intervenant qui nous viendra du Nigéria. Nous aurons donc plusieurs aspects du secteur, ce qui pourra nourrir cette conversation.

Il y a aussi Samantha Demetriou. Elle fait partie du groupe des parties prenantes des opérateurs de registre. Ensuite, nous allons avoir Babagana du Nigéria, nous aurons Barrack Otieno aussi, de AFTLD. Il n'est pas encore arrivé, mais je suis sûr qu'il nous rejoindra tout à l'heure.

Très bien, voilà les diapositives standards que nous allons utiliser pour le Comité permanent sur l'utilisation malveillante du DNS. Il s'agit là de partager des informations, de promouvoir le dialogue et de travailler sur les meilleures pratiques.

À la base, nous voulons vous donner, à vous les opérateurs de ccTLD, des outils pour pouvoir comprendre, mesurer et atténuer les problèmes s'il y en a pour les ccTLD.

Encore une fois, nous fournissons beaucoup de ressources, d'outils, il y a là des outils QR, vous pouvez accéder à la bibliothèque d'information. J'ai aussi quelques documents ici, si vous en avez besoin.

Encore une fois, nous mettons beaucoup d'efforts pour pouvoir apporter autant d'expertises que possible pour combattre cette utilisation malveillante.

Alors, nous n'allons pas parler beaucoup de la définition de l'utilisation malveillante, car cela a été fait à de nombreuses reprises. Nous allons parler des amendements, des contrats. Vous voyez ici les différentes définitions à l'écran. Il y a beaucoup de membres de l'équipe qui travaillent sur cela. Nous en parlons beaucoup au cœur du travail du SSAC et sur le site du SSAC vous trouverez les définitions adéquates.

Je vais passer la parole à Sam.

SAMANTHA DEMETRIOU : Oui, c'est une grande responsabilité. Merci de votre introduction, de votre présentation, merci à la ccNSO de nous avoir invités à participer à cette séance. Je suis présidente du groupe des parties prenantes des opérateurs de registre. Nous allons fournir un peu de contexte et nous allons parler de la raison pour laquelle nous avons continué à travailler sur les amendements.

Les amendements ont un impact sur l'accord de base, c'est un contrat qui est renforcé par la plupart des bureaux d'enregistrement. C'est un contrat pour les bureaux d'enregistrement qui veulent enregistrer des noms de domaine ccTLD.

Donc au début de 2022, un petit groupe d'entre nous s'est rassemblé pour discuter de l'état des lieux sur l'utilisation malveillante du DNS, à travers la communauté ICANN, mais aussi avec d'autres parties prenantes telles que d'autres régulateurs ou gouvernements. C'est là que nous avons reconnu que l'utilisation malveillante du DNS était un problème.

En tant que bureaux d'enregistrement et opérateur de registre, nous avions un rôle à jouer pour faire face à ces problèmes. Malgré tout, nous continuions à entendre que le département des conformités de l'ICANN n'avait pas l'outil adéquat pour forcer les opérateurs de registre et les bureaux d'enregistrement pour qu'ils puissent agir, justement, dans le cas des abus.

Le contrat était verrouillé, si on peut dire, et il y avait un manque de clarté pour ce qui est des exigences.

Quand il s'agit du sujet de l'utilisation malveillante du DNS, et bien il est assez large. Nick en a parlé tout à l'heure, la conversation est toujours difficile. La raison pour laquelle nous avons décidé de continuer avec ces amendements c'est que nous avons pensé que cette approche pourrait nous donner la possibilité d'agir assez rapidement, si on peut dire, pour commencer à faire face à ce problème très concret auquel nous faisions face.

Donc on parle là du manque de clarté lorsqu'il s'agit des obligations dans les amendements.

Et nous voulions établir une fondation sur laquelle nous pourrions construire notre communauté pour créer des obligations qui soient un petit peu plus minimales, ou du moins une base sur laquelle les bureaux d'enregistrement et les opérateurs de registre pourraient agir lorsqu'ils se trouvaient face à des abus du DNS. Nous voulions mettre en œuvre des standards assez élevés, mais aussi de lever la barre à travers le secteur pour que tout le monde soit régi par ces standards minimums.

Nous savons très bien que beaucoup de travail à faire dans ce domaine et que ce travail devait bénéficier des retours de toutes les parties prenantes.

Voilà ce que je voulais résumer, les impacts sur les opérateurs de registre, les impacts provoqués par les amendements au contrat, les amendements du RA et du RAA sont assez similaires, mais il y a tout de même de petites différences.

Donc les amendements requièrent maintenant que les opérateurs de registre doivent agir de façon appropriée pour atténuer les utilisations malveillantes du DNS quand un rapport est reçu et cela basé sur des éléments probants.

Les opérateurs de registre ont donc la discrétion de déterminer les actions et cela est dû au fait que l'utilisation malveillante du DNS peut être spécifique. Donc ce qui correspond à des actions appropriées peut être différent, dans différents cas.

Pour le contexte de ces amendements, je peux vous dire que nous laissons les prérequis un petit peu plus ouverts, peut-être, et cela permettrait dont aux bureaux d'enregistrement et opérateurs de registre de prendre des actions un petit peu plus spécifiques en fonction des cas particuliers. Donc nous pensions que c'était plus approprié.

Donc, une action pour les opérateurs de registre pourrait représenter, par exemple de laisser les noms de domaine aux bureaux d'enregistrement pour qu'ils prennent les actions pour les utilisations malveillantes. C'est la manière de définir le rôle des bureaux d'enregistrement et des opérateurs de registre dans l'espace du DNS et le fait que les bureaux d'enregistrement ont plus de relation avec le titulaire du nom de domaine et donc puisse prendre la responsabilité.

Donc il y a eu un ajustement ici, cela changera peut-être la manière dont nous recevons les rapports de l'utilisation malveillante du DNS. Donc, en général on nous envoie un mail, mais cette plateforme peut peut-être résoudre ces problèmes.

Toutes ces informations, si vous voulez regarder comment les amendements sont écrits, vous pouvez aller voir sur la section 6 et la section 4 de l'accord de base.

Maintenant, nous avons les amendements qui ont été approuvés par les groupes et ont été mis en œuvre en avril, le 5 avril exactement de cette année.

La deuxième chose que nous regardons désormais est de savoir comment nous pouvons mesurer l'impact et l'efficacité de ces amendements. Bien

sûr, il est encore très tôt, il ne s'est passé que deux mois. Nous allons y travailler les prochains mois et nous parlerons du bureau des plaintes de l'ICANN, mais également de toute la communauté.

Je voulais vous montrer quelques statistiques qui sont disponibles, qui ont été publiées dans un article de blog de l'ICANN vendredi dernier. Donc, depuis le passage de l'amendement il y a eu 38 investigations de conformité avec les bureaux d'enregistrement et les opérateurs de registre. Il y a eu plus de 2500 noms de domaines malveillants qui ont été suspendus et 328 sites internet de fishing qui ont été désactivés.

Donc ce qu'on peut conclure c'est que les amendements entrainent des actions sur l'utilisation malveillante du DNS. Ce que nous ne savons encore pas et que nous ne pouvons pas encore évaluer, c'est de savoir si cela a changé vis-à-vis des amendements ou si c'était déjà quelque chose qui se passait avant qu'ils entrent en vigueur. Mais c'est encore quelque chose que nous pouvons rechercher avec l'ICANN.

Voilà donc ce que nous avons fait. Pourquoi nous avons choisi des amendements plutôt que d'autres processus d'élaboration des politiques.

Je suis prête à répondre aux questions si vous en avez.

NICK WENBAN-SMITH : Merci beaucoup, Sam. C'était très clair. Je crois qu'il n'y a pas besoin de question parce que= tout était vraiment bien expliqué. J'ai beaucoup de questions comme par exemple pourquoi il faut des contrats, mais ça, c'est peut-être une question un peu philosophique, donc on peut passer à la

suite, la question de savoir de ces administrations de fishing, de toute façon, aurait été réglée même sans ces amendements aux contrats.

On va passer pour entendre le point de vue des bureaux d'enregistrement, ceux qui sont les plus à même de nous parler de ces changements et des prérequis de l'ICANN. James d'abord.

JAMES BLADEL: Merci beaucoup, Nick. Voilà ma prochaine diapositive. Je suis le vice-président de Government and Industriy Affairs. Je travaille énormément dans le secteur des ccTLD et en partenariat et en accord avec, par exemple, le .ME pour le Monténégro.

Notre expérience a trait aux utilisations malveillantes du DNS, mais elle ne porte que sur les derniers mois, comme Sam l'a expliqué, depuis la mise en œuvre de ces amendements.

La question c'est pourquoi les bureaux d'enregistrement ont accepté plus de restreintes sur ces contrats avec ces amendements. En réalité, la question c'est pourquoi on dirait oui à ce type de changement et qu'est-ce que ça nous apporte.

Bien sûr, l'utilisation malveillante du DNS est un problème à l'échelle de l'industrie et c'est un problème qu'il nous faut résoudre. Même avec les meilleures intentions, nous ne pouvons pas faire grand-chose si nous travaillons seuls, donc il est toujours mieux de travailler en tant qu'industrie entière.

Les bureaux d'enregistrement font également beaucoup d'investissements dans la technologie, dans les personnes, pour créer la technologie disponible pour détecter l'utilisation malveillante du DNS.

Nous étions donc désavantagés par rapport aux bureaux d'enregistrement qui étaient déjà sur ce terrain. Donc nous avons décidé de mettre cela en œuvre pour, principalement, rentrer en concurrence et être un petit peu au même niveau que nos concurrents.

Nous avons également accepté de nous engager sur l'autorégulation dans le cadre de l'utilisation malveillante du DNS de l'ICANN. Donc que ce soit au sein de l'ICANN ou en dehors grâce à la législation.

Un élément de cela est important, comme Sam l'a dit, c'est l'harmonisation d'une définition de l'utilisation malveillante du DNS puisque ne pas avoir la même définition était un vrai problème.

Pour celles et ceux qui sont avec nous depuis longtemps, vous savez très bien que les définitions c'est ce qui nous prend le plus de temps lorsque nous écrivons les politiques.

Donc ce qui est nouveau ici, Sam l'a déjà bien dit, mais pour nous, nous avons une obligation d'investigation lors d'un rapport d'une utilisation malveillante du DNS pour pouvoir l'empêcher le plus vite possible.

L'ICANN a désormais le pouvoir de gérer ces processus au cas où les bureaux d'enregistrement ne fassent pas assez pour répondre à cet engagement.

Mais il est très important de noter, si on revient à la définition, que les définitions ne définissent pas d'autres types d'utilisations malveillantes du DNS. Donc, nous en revenons à cette idée que la définition est très importante, il est important pour nous d'être très clair sur ce qui relève de l'utilisation malveillante du DNS ou non.

Comme Sam l'a dit, ces amendements sont assez nouveaux, nous sommes toujours dans une phase de collecte de données pour comprendre quels impacts cela aura eus sur le problème.

Ce qui est très intéressant c'est que les bureaux d'enregistrement n'ont pas vu de changement dans leurs pratiques d'atténuation.

Nous nous étions engagés à suivre ce contrat sur l'utilisation malveillante du DNS qui était, à l'époque, quelque chose de volontaire pour réduire les impacts d'abus du DNS. Et nous avons décidé de travailler sur les amendements de ce contrat et les bureaux d'enregistrement et opérateurs de registre ont participé à cette élaboration du cadre sur l'utilisation malveillante du DNS.

Il y a donc une question encore ouverte pour savoir si le volume des rapports va augmenter ou non, le volume des rapports que les bureaux d'enregistrement normalement reçoivent, donc cela s'applique aux plaintes qui sont envoyées à l'ICANN.

Nous nous assurons de suivre cela de très près pour avoir des niveaux suffisants de qualité et de quantité vis-à-vis de tout cela.

Sam l'a dit également dans ses diapositives, nous permettons aux bureaux d'enregistrement de nous envoyer des plaintes d'une autre manière,

puisque jusqu'à très récemment seulement les mails étaient disponibles pour envoyer un rapport d'utilisation malveillante du DNS. Mais le fait d'avoir déplacé cela sur un site web nous permet vraiment de pouvoir les classifier, les catégoriser et c'est vraiment essentiel pour un grand fournisseur de services internet, surtout lorsqu'ils reçoivent beaucoup de plaintes.

Voilà donc jusque-là. Nous appelons désormais NetBeacon qui permet aux bureaux d'enregistrement et opérateurs de registre d'avoir des rapports et des mesures de performance. Cela nous permet d'avoir aperçu de l'état de l'utilisation malveillante du DNS avant ce contrat et cela nous permettra d'évaluer, depuis la mise en œuvre de ces amendements, pour voir ce qui a évolué.

Nous pourrons ainsi identifier quelles parties contractantes le font de bon cœur et lesquelles ne respectent pas vraiment ces obligations. Et ça, c'est très important, je crois que c'est Sam qui l'a dit, ce n'est pas une solution unique pour la lutte contre l'utilisation malveillante du DNS. Il y a énormément de choses à faire.

Il est peut-être intéressant de différencier les différentes manières d'utilisation malveillante du DNS, parce qu'il y a une grande différence entre l'utilisation malveillante du DNS avec de nouveaux noms de domaine créés de manière malveillante ou des noms de domaine qui sont détournés après création et qui sont désormais utilisés pour une utilisation malveillante.

Donc ça, c'est un point très intéressant pour nous et je pense que cet outil va être très intéressant et utile. Je pense qu'il y a encore beaucoup à

apprendre en ce qui concerne la manière dont l'ICANN va répondre aux nouvelles règles.

Comme je le disais, nous avons reçu le rapport qui a posté sur le blog vendredi, le volume a l'air d'être plus élevé, mais l'ICANN évalue également certains de ces rapports pour savoir s'ils sont appropriés, s'ils peuvent être envoyés aux bureaux d'enregistrement.

Quelque chose que l'on voit ici c'est que certaines plaintes qui rapportent une utilisation malveillante du DNS sont faites à l'ICANN et aux bureaux d'enregistrement. Ce n'est pas utile, le but de l'ICANN n'est pas d'être le gardien de ce processus. Ils sont ici au cas où le bureau d'enregistrement ne réponde pas ou ne prenne pas les bonnes actions. Donc envoyer les rapports aux deux n'est pas utile, c'est peut-être une mauvaise compréhension des rôles et responsabilités de chacun.

Par ailleurs, les informations sont parfois incomplètes, il manque des données, des informations, et on ne peut pas faire une enquête, par conséquent, ces rapports sont ensuite rejetés. L'ICANN se centre actuellement sur les problèmes systémiques et non pas sur les incidents individuels.

Je voudrais ajouter qu'actuellement il y a une séance qui a lieu avec les bureaux d'enregistrement, je pense qu'ils vont justement aborder ces questions et partager de nouvelles informations.

Finalement, je dirais que tout cela doit être considéré pour voir ce qui s'applique à chaque TLD. De toute façon, il nous faut aligner tout cela, ce

sera de toute façon un bénéfice pour les bureaux d'enregistrement et pour les opérateurs de registre.

Ces contrats vont permettre de garantir que les bureaux d'enregistrement respectent les nouvelles normes adoptées. On en a parlé, on a analysé tout cela, il n'est pas nécessaire de réinventer tout cela on peut l'utiliser.

Et nous invitons les ccNSO à utiliser ce travail, en ce qui concerne la terminologie, les définitions, de façon à ce que lorsque vous parlez avec votre bureau d'enregistrement vous parliez la même langue et que vous utilisiez la même terminologie. Vous devez aussi faire confiance dans les décisions des bureaux d'enregistrement. Il y a des politiques qui sont parfois trop prescriptives, qui ne vont qu'aider les acteurs malveillants. Donc il faut essayer d'éviter tous les mécanismes qui pourraient porter préjudice. Parfois il est bon de permettre un certain niveau de discrétionnaire pour que l'on puisse faire certaines enquêtes, voir quelles sont les mesures adéquates à mettre en œuvre ; et nous avons inclus tout cela dans les modifications des contrats.

Donc vous pouvez entrer avec vos bureaux d'enregistrement qui ont beaucoup d'expériences dans ce domaine. Sam l'a dit, ses collègues aussi, les bureaux d'enregistrement sont vraiment à la tête de ce mouvement, les opérateurs de registre un peu moins, je dirais qu'il y a beaucoup d'expérience et d'expertise qui peuvent être prises auprès des bureaux d'enregistrement pour lutter contre l'utilisation malveillante. On peut toujours en faire plus.

Les opérateurs de registre, les bureaux d'enregistrement veulent vraiment faire quelque chose ici. Parce que, de toute façon, même si on sait que

l'utilisation malveillante ne va pas disparaitre et qu'elle va se déplacer sur la partie la plus vulnérable de l'internet, on doit quand même essayer de réduire cette brèche de façon à ce que les espaces qui existent dans le domaine des ccTLD et des TLD en général soient plus fiables.

Voilà, j'en ai terminé et je vous remercie.

NICK WENBAN-SMITH: Merci, James. Votre présentation était très claire. Je vois qu'il y a une main levée et ensuite une autre sur Zoom. Allez-y Eberhard.

EBERHARD LISSE : Est-ce que vous avez eu des bureaux d'enregistrement qui étaient en conformité avec les nouveaux gTLD, mais pas avec le ccTLD ? Parce que nous, on accepte les titulaires qui sont en conformité et les ccTLD, dans ce cas-là, ne sont pas inquiets parce qu'ils sont sur la bonne voie.

JAMES BLADEL: Oui, je pense que c'est possible, je pense que c'est peut-être plus facile, moins cher aussi pour appliquer leurs pratiques de gTLD à tous les ccTLD dans leur secteur. Je ne pense pas que l'on doive penser que c'est le cas pour tous, mais je pense que ce serait logique de le penser.

En tout cas l'objectif est ici de continuer à appliquer cela dans l'ensemble du secteur et, s'il y a un changement de contrat ou de politique ou une communication des opérateurs de la ccNSO vers un bureau d'enregistrement en disant : on voudrait que vous appliquiez telle ou telle pratique dans l'espace des gTLD et que vous traitiez les ccTLD de la même manière, cela serait acceptable. Le message doit être clair, c'est tout.

NICK WENBAN-SMITH : Merci. Kristian ?

KRISTIAN ORMEN: Je suis de la fondation de l'internet de Suède. C'est un commentaire. Je voudrais dire qu'en tant que TLD, travailler avec un bureau d'enregistrement c'est beaucoup plus efficace que de le faire soi-même. Donc je suis tout à fait d'accord avec ce que James vient de dire.

NICK WENBAN-SMITH: Je ne vois pas de main levée. Pierre, allez-y.

PIERRE BONIS : Je peux parler en français ? Très bien, j'y vais. À cette occasion, je voulais vous interroger…. Je vais parler en anglais si vous n'avez pas la traduction.

Je voulais savoir, de votre point de vue, si les changements de contrat au niveau de l'ICANN vous donnent la possibilité de faire quelque chose ? Parce qu'on parle toujours des obligations, de nouvelles obligations qui figurent dans le contrat, mais des fois, quand on a cette relation avec les titulaires, on leur demande d'agir, ils nous répondent qu'ils n'ont pas ce pouvoir.

Donc c'est quelque chose qui est décrit dans le contrat qui vous permet de faire quelque chose que vous ne pouviez pas faire auparavant ou bien c'est une nouvelle conformité que vous souhaitez mettre en œuvre ? En tout cas c'est mon opinion, en tant qu'opérateur de registre, mais des fois les

opérateurs de registre n'ont pas la possibilité d'agir sur les noms de domaine.

JAMES BLADEL: Alors, le type d'utilisations malveillantes que nous utilisons dans le contrat interdit certaines conditions de service. Et les accords d'enregistrement des noms de domaine. Donc dans notre cas, je dirais que non. Nous avons toujours eu la possibilité et la capacité d'agir ici.

Ce qui, à mon avis, peut se passer, c'est que pour les bureaux d'enregistrement qui n'avaient pas la possibilité d'agir, maintenant ils peuvent faire ces choses, donc modifier les accords pour que les clients comprennent ou sachent que s'ils mettent en place des utilisations malveillantes, on va suspendre le service.

SAMATHA DEMETRIOU: Du côté des opérateurs de registre, je dirais que la situation est plus ou moins la même, les modifications ne donnent pas de permis aux opérateurs de registre. Mais il y a quelque chose ici d'important et c'est la réponse lorsqu'il y a une utilisation malveillante du DNS, comme par exemple lorsqu'on envoie un avis au bureau d'enregistrement. Et pour l'accréditation aussi, c'est pareil, il est plus sûr qu'on mette en œuvre des actions d'atténuation pour lutter contre l'utilisation malveillante du DNS.

NICK WENBAN-SMITH : Parfait. Nous allons continuer. En tant qu'avocat, je peux vous dire qu'il y a des questions qui sont contractuelles, mais des fois c'est difficile de les

appliquer. Donc ce qui est intéressant c'est qu'il y ait vraiment une obligation qui oblige le client à appliquer ce qu'il y a dans le contrat.

Par ailleurs, on sait qu'il y a une quantité importante d'utilisation malveillante qui se concentre dans des petites niches.

Donc nous sommes ici à Kigali, une belle ville, et je ne veux pas que vous partiez sans connaitre la perspective de la région, par conséquent, il est important de donner la parole à la personne qui me suit, Adéola.

ADEOLA RAJI: Bonjour, je travaille avec Upperlink du Nigéria. L'utilisation malveillante du DNS a été une question très importante.

En 2020, pendant la pandémie, nous avons constaté qu'il y avait beaucoup d'utilisations malveillantes du DNS qui étaient liées à la Covid. Nous avons reçu différents types de plaintes de la part des utilisateurs, mais les bureaux d'enregistrement n'étaient pas les seules personnes affectées. Les serveurs aussi étaient affectés. Et, lorsque nous avons constaté que l'on pouvait faire certaines modifications, nous n'avons pas douté, parce que tout cela permet de lutter, de contrôler cette utilisation malveillante pour que l'internet soit un écosystème plus sûr pour tous les usagers. Et, par ailleurs, nous voulons lutter contre tous ceux qui veulent voler de l'argent ou avoir des activités malveillantes.

Donc on va parler de l'impact de l'utilisation malveillante du DNS du point de vue des bureaux d'enregistrement. Et je vous présenterai la situation en Afrique.

Mes diapositives parlent de l'amendement de 2013 et ensuite je parlerai de l'amendement de 2023. Alors 2013, c'était sur les politiques et 2023 c'était sur les contrats. Je ne rentrerai pas dans le détail pour une question de temps.

D'abord, pourquoi nous parlons de cela ? Notre objectif est de combattre l'utilisation malveillante du DNS, comme par exemple le hameçonnage, la distribution malveillante de virus, les botnets, tout ce qui est lié aussi aux cryptomonnaies. Nous allons parler de l'impact de ces modifications sur les entreprises qui sont les bureaux d'enregistrement et tous les défis que cela peut présenter.

Du point de vue des bureaux d'enregistrement, ils sont obligés de faire un suivi. Et dans les accords d'accréditation des bureaux d'enregistrement, il est dit qu'ils doivent présenter toutes les plaintes et faire un suivi des plaintes. Donc il est important de tenir compte de ces modifications parce que cela permet d'avoir accès aux plaintes. On peut faire un site internet sur lequel les gens peuvent envoyer leurs plaintes. Si les gens n'ont pas cette possibilité, à ce moment-là il faut envoyer un email à une adresse spécifique et en ayant un formulaire web sur la plateforme, ce sera plus facile à utiliser. Les utilisateurs pourront le faire. Et ceux qui veulent dénoncer une utilisation malveillante du DNS pourront le faire.

On sait qu'il y a beaucoup de délits sur l'espace d'internet. Donc il est clair dans ces accords, lorsqu'on a une plainte d'utilisation malveillante, le bureau d'enregistrement doit agir.

Alors, s'il y a des problèmes de hameçonnage, il faut retirer ce contenu. Il y a des clients qui ont eu des problèmes liés aux contenus et on a établi qu'il

s'agissait d'une affaire illégitime au Nigéria et à ce moment-là on a fait la suspension de ce domaine.

Et avec ce système, on facilite pour l'utilisateur final, la possibilité de fournir des preuves sur l'utilisation malveillante.

Ce message a été partagé à toutes les parties prenantes et tous les acteurs. Nous avons aussi partagé les informations sur les actions qu'ils devaient mettre en œuvre. Et ces amendements proposent aussi des éléments pour éviter les conflits juridiques. Donc nous pouvons prendre connaissance ensuite et agir de façon adéquate.

Et, parfois, nous avons des réunions sur ce fait. Si vous avez des informations, et bien communiquez, et si vous avez des exemples, vous pouvez partager tout cela, nous pouvons faire le suivi. Et cela, vraiment, nous aide à rentrer dans la conformité. Et cela pourra réduire, justement, ces conflits juridiques.

Voilà donc ce que seraient les impacts possibles de ces amendements.

Alors, nos ccTLD, comment pouvons-nous aider dans la lutte des abus malveillants ?

Il y a eu des moments où nous avions des problèmes avec les forces de l'ordre et il y avait un cas d'utilisation malveillante et nous avons, dans ce cas, contacté nos supérieurs, NIRA est intervenu, a fait un rapport et l'idée était justement de donner des informations aux forces de l'ordre dans le cas et commencer une investigation. Dans ce cas nous avons résolu le problème et le harcèlement s'est arrêté.

[L'interprète s'excuse, il y a une interférence sur la ligne avec un micro ouvert]

L'ICANN a donc rendu les choses plus claires pour pouvoir arrêter cette utilisation malveillante et pour donner des informations sur ce qui doit être fait.

Pour les bureaux d'enregistrement, les extensions géographiques, les CCT aident à surveiller les enregistrements et les vérifier. Donc beaucoup de personnes, lorsqu'il y a un problème, au lieu d'aller vers les bureaux d'enregistrement, vont directement vers les opérateurs de registre. Maintenant il y a donc des conseils qui sont mis en œuvre pour trouver des solutions. Et il y a de meilleures solutions mises en œuvre.

S'ils reçoivent un courriel, par exemple quand un email malveillant est envoyé et que quelqu'un clique sur cet email et qu'il s'agit d'une utilisation malveillante, cela pose toujours des problèmes. Beaucoup de bureaux d'enregistrement utilisent une base de données. Par exemple, pour .BANQUE.COM ils avaient BANQUE.AUTRE CHOSE. Si on ne fait pas attention quand on ouvre un tel document, on perd ses informations. Ou, on sait très bien que beaucoup de personnes ne sont pas au courant. Les bureaux d'enregistrement peuvent commencer à essayer d'aider les utilisateurs finaux pour éviter cette utilisation malveillante.

Il s'agit de collaborer aussi avec les forces de l'ordre et faire l'éducation nécessaire pour qu'ils puissent faire les investigations nécessaires, encore une fois. Et, quand on reçoit un email lié aux utilisations malveillantes du DNS, et bien on peut fournir les informations.

[L'interprète s'excuse, cette intervenante parle très vite et il est très difficile de la suivre]

Encore une fois, on est là pour éduquer, lorsque nous avons de tels cas. Par exemple on vous dit : si vous faites face à un cas comme celui-ci, voilà ce que vous devez faire et l'information doit être partagée. Il faut absolument faire une vérification des processus et cela est quelque chose que les opérateurs de registre doivent mettre en œuvre.

Et les extensions géographiques doivent exécuter les politiques liées aux bureaux d'enregistrement.

Alors, les politiques d'extension géographiques sont importantes, il y a d'autres politiques qu'on peut aussi consulter lorsqu'il s'agit d'utilisation malveillante du DNS. Les deux côtés, que ce soit opérateur de registre et bureau d'enregistrement peuvent ainsi obtenir du soutien.

Merci.

NICK WENBAN-SMITH : Merci beaucoup, des conseils très pratiques. Souvent, les opérateurs de registre et les bureaux d'enregistrement peuvent travailler ensemble, car il y a des choses qui sont mieux faites par une entité ou l'autre, ça dépend du contexte. C'est un bon passage vers le côté des règlements.

Alors, voilà, la raison pour laquelle on doit avoir un modèle de règlementation c'est qu'on puisse être plus flexible, mettre en place un système qui soit bon pour l'industrie et le secteur.

Alors moi, ce qui m'intéresse, c'est l'avis des régulateurs. Alors, jusqu'à quel point doit arriver le problème pour qu'il y ait des actions ? À quel niveau doit-on arriver pour pouvoir agir ?

ENGR BABAGANA DIGIMA: Je suis de la Commission de la Communication du Nigéria. On l'a dit tout à l'heure, on ne doit pas forcément redéfinir ce qu'est l'utilisation malveillante du DNS, mais ce que je voulais dire, c'est qu'on va parler du point de vue gouvernement et des unités régulatrices.

Dans ce contexte, ces modifications apportées aux accords gTLD apportent des moyens d'atténuation d'utilisations malveillantes. Ces amendements sont aussi critiques pour les ccTLD, car ce sont eux qui établissent une base de référence mondiale pour les efforts de lutte contre les abus qui sont directement appliqués ou servent de ligne directrice pour les opérations de ccTLD.

Alors ces récentes modifications apportées par l'ICANN en vue d'un internet plus sûr et plus résistant aux abus montrent la nécessité d'un alignement règlementaire et d'un engagement proactif.

Alors, à notre avis, on peut voir quel genre d'impact cela aura sur les citoyens lambdas et nous voulons améliorer la sécurité en ligne. Bien sûr, nous avons beaucoup d'inquiétudes par rapport à ce rapport, surtout lorsqu'il s'agit de l'utilisation malveillante à travers des emails qui ont pour origine le Nigéria.

Nous voulons absolument arrêter ce genre d'abus, améliorer aussi notre infrastructure en ligne, surtout pour .NG, nous allons donc vraiment tirer

avantage de ces nouvelles mesures et nous devons dans ce sens améliorer le soutien local pour les entreprises locales qui s'appuient sur le DNS.

Nous voulons aussi parler de l'utilisation malveillante du DNS en elle-même. On l'a dit, on n'a pas besoin de redéfinir cela, mais nous sentons, au Nigéria, en tant que régulateur ou de gouvernement, nous sentons tout de même qu'il s'agit d'abus ou d'utilisations malveillantes du DNS qui devraient être défini en tant que tel. Par exemple, nous avons beaucoup de défis avec certains sites web qui sont actifs au Nigéria. Et nous avons des problèmes avec certaines plateformes qui sont utilisées au Nigéria. Et, dans ce sens, aussi, nous aimerions que l'ICANN examine cela, à savoir si c'est vraiment un cas d'utilisation malveillante du DNS, est-ce que c'est une activité au Nigéria qui est considérée comme un abus du DNS ? S'il s'agit d'un site au Nigéria qui n'a pas de licence, est-ce que c'est considéré comme abus ou non ? Mais on va laisser ça sur la table pour une prochaine discussion, on en apprendra plus quand le prochain amendement rentrera en compte.

Ensuite, quels sont les défis auxquels font face les régulateurs ? Bien sûr, ces changements vont nous apporter aussi d'autres défis.

Alors, bien sûr, comment peut-on sensibiliser la population sur ces changements ? Et aussi pour les gestionnaires de ccTLD.

On doit pousser cela devant le public et on doit discuter de cela, de ce que l'on fait. Et on doit s'aligner avec les unités régulatrices, on doit parler de sensibilisation et de renforcement de capacité. Et, bien sûr, il y a aussi des éléments techniques qui doivent être pris en compte, surtout pour le bureau d'enregistrement, quand il s'agit du RDAP.

Pour les ccTLD, nous voyons qu'il nous faut équilibrer les standards internationaux.

Alors, quelles sont nos réalités locales aussi ? Et comment peut-on mettre en œuvre le renforcement de capacité ?

Nous voyons, au Nigéria comme dans beaucoup d'autres pays, des défis, surtout lorsqu'il s'agit des talents, des compétences des travailleurs.

Et, il y a un terme qu'on appelle « japa ». Alors on sait très bien que nos talents, nos employés dans le secteur IT, nos ingénieurs au Nigéria, ce genre de personnes, pour obtenir leurs compétences, il leur faut 3 ans. Ils obtiennent des compétences dans tout ce qui est du domaine des réseaux. Quand il s'agit par exemple de la mise en œuvre du DNSSEC, cela prend du temps, il leur faut l'expertise. Donc souvent les défis correspondent plus à l'expertise qu'à la mise en œuvre.

Il y a des personnes qui travaillent dans une entreprise pendant un ou deux ans, puis ils passent à une autre entreprise. Donc ils doivent réapprendre toutes les complexités, tous les problèmes qui vont avec. Voilà, cela représente tout de même un défi.

Donc ces changements ne sont pas liés seulement au DNSSEC, mais aussi dans tout le secteur. Nous devons étudier cette réalité, mettre cela en perspective.

Il y a une banque au Nigéria qui a par exemple perdu plus de 80 % de ses données et informations. Et c'est similaire à travers tout le secteur au Nigéria, donc nous pensons que le conseil d'administration de l'ICANN devrait étudier la question de renforcement de capacité, de

développement de compétence. Et, ensuite, nous voulons compenser, pour tout ce qui a déjà été perdu dans ce secteur. Donc nous pensons qu'ICANN peut aider dans ce sens et nous devons ainsi continuer tout ce qui est la formation au Nigéria et même en Afrique en général.

Nous allons aussi parler de notre rôle en tant que corps régulateur. En tant que régulateur, nous avons des règles, des lignes directrices qui nous permettent de voir comment nous évoluons. Donc une des clefs pour cela c'est de savoir comment on peut créer des lignes directrices sur la gouvernance de l'internet et la sécurité.

La question est de savoir quelles sont les normes de l'industrie, d'évaluer quels changements ont été adoptés récemment ou mis en œuvre dans d'autres scénarios.

Donc nous sommes en phase de révision, nous passerons bientôt dans une phase de consultation et puis nous aurons un document préliminaire d'ici à la fin de cette année ou au début de l'année prochaine. Donc nous verrons, l'important sera de s'aligner avec les standards de l'ICANN et de répondre aux demandes des ccTLD.

Donc la collaboration est encore quelque chose dont nous parlons, je voulais vraiment insister là-dessus. Nous sommes également dans une situation similaire, nous travaillons avec les gouvernements, les institutions en charge de l'application de la loi, des institutions de la société civile, du secteur privé, et cela nous permet vraiment d'améliorer notre stratégie.

Cependant, certaines institutions n'ont pas suffisamment de contexte sur ce qu'il se passe. Et cela, encore une fois, nous ramène à ce niveau.

Nous avons des parties prenantes qui ne font pas partie du secteur de l'internet et c'est quelque chose que nous regardons toujours en tant que régulateur, de s'assurer prendre tout le monde en compte.

Pour le Nigéria, bien sûr, à l'avenir, nous regarderons et évaluerons la possibilité de développer des lignes directrices qui s'alignent avec les politiques de l'ICANN pour améliorer l'engagement, la participation des parties prenantes.

Nous ferons un suivi, en particulier, des provisions que nous mettrons en œuvre pour lutter contre l'utilisation malveillante du DNS.

Pour conclure, en tant que régulateurs, nous sommes engagés à suivre ces normes mondiales, en particulier sur ces domaines et le domaine NG et nous assurer que nous soyons un phare de confiance dans la sécurité.

NICK WENBAN-SMITH: Merci beaucoup. C'est la fin de la présentation, vous serez heureux de l'entendre, nous avons désormais un petit peu de temps pour une discussion entre nos panélistes et je vais donner la parole à Barrack pour modérer cette discussion. S'il y a des choses que vous voulez demander à nos panélistes ou si vous avez des commentaires à faire. Je crois qu'il nous reste 10 minutes, seulement 10 minutes parce que nous avons la visite du mémorial du génocide à 15 h 10, il faudra être à l'heure.

BARRACK OTIENO: Merci, avons-nous des questions pour les membres du panel ? Une question ?

IRINA DANELIA: Bonjour, ce n'est pas qu'une question, c'est plus un commentaire, si c'est possible. Je fais partie du .RU pour la Russie. Cela fait 10 ans que je gère un projet qui nous demande de détecter des noms de domaine suspicieux.

[L'interprète s'excuse, mais il y a une interférence sur la ligne, un micro est ouvert, il y a un écho]

Il n'est pas possible de garantir à 100 % des situations sans erreur. C'est statistiquement un faux positif. Les noms de domaine légitimes, sur 50 000, sont à presque zéro. Mais, en pratique, lorsque l'on prend cette chaine d'erreurs humaines, ces processus parfois peuvent entrainer des noms de domaine suspendus par erreur.

Et si ces noms de domaine appartiennent à une grande chaine de marché, par exemple, un espace de marché, cela pourrait un grand problème pour le bureau d'enregistrement, cela pourrait leur causer préjudice. Donc je voulais vraiment avoir une discussion sur les garde-fous qui peuvent être mis en place pour réduire le risque de telles situations.

Peut-être que ce n'est pas une question pour aujourd'hui, mais quelque chose sur lequel il faudrait nous pencher à l'avenir.

BARRACK OTIENO: Merci beaucoup, Irina. Y a-t-il d'autres commentaires ? Il y a une question en ligne.

ALAN WOODS: Bonjour à tout le monde, juste pour répondre à ce que l'oratrice précédente disait, je pense qu'on pourrait trouver une réponse commune entre la GNSO et la ccNSO sur ces enjeux.

Il y a eu une déclaration très claire qui a été faite, en particulier sur les normes de preuve et sur des attentes minimums parce que d'avoir ces normes bien définies est vraiment clef pour notre travail et ce serait une bonne chose de commencer à réfléchir par ces normes.

Cela nous permettrait également de nous assurer que nous fassions le travail d'une bonne manière. Donc je suggèrerais de commencer par ce côté-là.

BARRACK OTIENO: Merci. Je ne sais pas si des membres du panel veulent répondre au commentaire ?

SAMANTHA DEMETRIOU: Merci beaucoup, merci pour la contribution, Alan. Je voulais juste vous donner un petit point sur le programme. Jeudi, à Kigali, ici, il y aura un atelier sur l'utilisation malveillante du DNS avec les opérateurs de registre et les bureaux d'enregistrement. Et ce donc nous parlerons c'est quelque chose qu'Alan vient de mentionner, garantir de bons rapports. Donc si on veut avoir des normes qui s'appliquent à toute l'industrie, j'encourage toutes les personnes qui peuvent être intéressées par cette discussion à participer à cet atelier.

BARRACK OTIENO: Merci beaucoup. Des membres du panel veulent répondre aux questions posées avant que je me tourne encore une fois vers nos modérateurs ? Y a-t-il des questions en ligne ou en présence ? Très bien, donc j'attends que les questions viennent.

Mais je voulais vous dire que lorsque nous avons préparé cette séance, nous avons fait une enquête, ce qui en est ressorti, nous avons fait cette enquête pour 12 ccTLD au niveau de l'AFTLD, donc en Afrique, certaines formes les plus fréquentes de l'utilisation malveillante du DNS qui ont été rencontrées venaient en majorité d'attaques de fishing.

Une autre question qui était posée est de savoir si l'utilisation malveillante du DNS était un problème important et les 12 ont répondu que oui, c'était un vrai enjeu.

Voilà, je vous ramène ces résultats, je ne sais pas si on a plus d'inquiétudes, de commentaire ? Joke ?

JOKE BRAEKEN : Une question dans le chat : les statistiques et les rapports de conformité en 2024 vont être mis en œuvre en 2024, est-ce que cela veut dire que l'ICANN va supprimer ces 2500 noms de domaine malveillants ?

BARRACK OTIENO: Merci. Est-ce que quelqu'un dans le panel voudrait répondre à cette question ? James ?

JAMES BLADEL: Je suis désolé, je n'ai pas compris la question.

JOKE BRAEKEN : Les statistiques données le 5 avril 2024 veulent-elles dire que la conformité de l'ICANN a demandé aux bureaux d'enregistrement de suspendre 2528 noms de domaines malveillants ?

JAMES BLADEL: Le mot n'est pas juste, l'ICANN ne requiert pas d'action de la part des bureaux d'enregistrement. Donc je ne sais pas j'y réponds bien, mais ce n'est pas la responsabilité de l'ICANN de demander aux bureaux d'enregistrement de prendre des actions, de faire action. Leur responsabilité est de vérifier qu'ils répondent aux requêtes.

BARRACK OTIENO: Merci beaucoup. Je pense que je vais demander aux panélistes pour clore cette séance.

JAMES BLADEL : Rien à dire, merci beaucoup pour cette séance, merci de penser à nous et de penser qu'il y a des choses à apprendre les uns des autres en ce qui concerne les ccTLD. Je pense que plus on s'aligne sur nos travaux plus on pourra lutter contre l'utilisation malveillante du DNS. Parce que les personnes qui utilisent de manière malveillante du DNS ne s'intéressent

pas au fait que ce soit un ccTLD ou un gTLD, donc il faut que nous travaillions ensemble pour lutter contre ça.

ENGR BABAGANA DIGIMA : Merci, je suis tout à fait d'accord avec mon collègue, je crois que les utilisations malveillantes doivent être prises en compte, nous en tant que gouvernements en tout cas, nous avons cette responsabilité de faire quelque chose pour atténuer cette utilisation malveillante. Nous voulons être sûrs que la communauté mondiale fasse sa part également.

SAMANTHA DEMETRIOU: Merci, je voulais dire que le travail concernant l'utilisation malveillante continue au-delà de ces amendements et nous comptons sur l'aide de la communauté dans ce sens.

ADEOLA RAJI: Merci à tous, je dirais que ça a été une séance très intéressante. Donc nous allons vous envoyer le matériel, nous allons continuer à travailler sur les questions liées à l'utilisation malveillante du DNS et à l'atténuation de celles-ci.

BARRACK OTIENO: Nick, vous avez la parole.

NICK WENBAN-SMITH: Bien, je dirais que cette séance a été très intéressante. Je remercie tous les participants pour leur participation. C'est un thème de grande importance

pour nous tous. Et on s'en rend compte, les discussions étaient très intéressantes, avec la participation des gouvernements, des ccTLD, des représentants des ccTLD. Tout ce qui concerne le hameçonnage est un point important. Et les contrats dont on a parlé, les clauses de contrat qui tiennent compte de ces aspects sont aussi très importants. Nous vous remercions et nous vous applaudissons. Merci.

[FIN DE LA TRANSCRIPTION]