MONTREAL – Utilisation malveillante du DNS
Mercredi 6 novembre 2019 – 10h30 à 12h00 EDT
ICANN66 | Montréal, Canada

BRUCE TONKIN : Nous vous demandons s'il vous plaît de bien vouloir prendre place. Nous allons commencer la séance. Je sais qu'il y a beaucoup de personnes qui s'intéressent à ce sujet, donc nous souhaitons vraiment bien exploiter le temps qui nous est imparti ce matin.

On a l'impression d'être là depuis deux semaines pour certaines d'entre nous mais l'objectif de cette séance, c'est de rassembler un petit peu toutes les discussions qui ont déjà eu lieu pendant la semaine par rapport au sujet de l'utilisation malveillante du DNS.

Le contexte de ce sujet, c'est qu'il y a un certain nombre de références à l'utilisation malveillante du DNS, à la collecte d'informations, il y a également la question des contrats, des opérateurs de registre et bureaux d'enregistrement, il y a également la question de la confiance, du choix des consommateurs et de la concurrence. ICANN Org, l'organisation, collecte et publie des données, des statistiques sur le nombre de noms de domaine qui ont été signalés dans différents registres et domaines de premier niveau. Et il y a certaines pratiques qui ne sont pas très connues. Et je crois que du point de vue de la communauté, les obligations ne sont pas très connues en termes

d'investigations des bureaux d'enregistrement et des opérateurs de registre. Et surtout lorsqu'un signalement a été fait, que se passe-t-il ? C'est vraiment un des domaines qui est le moins bien compris.

L'objectif de cette séance, c'est de vous présenter d'une manière générale le sujet. Nous avons un panel d'experts de différentes parties de la communauté de l'ICANN qui pourront faire des commentaires sur les différentes thématiques. Et ensuite, je passerai la parole à la salle pour poser des questions, pour avancer des suggestions de manière à faire des progrès dans ce domaine et finalement de manière à protéger l'utilisateur final.

Pour commencer, je vais rapidement présenter les membres du panel. Si chacun des membres du panel pouvait dire son nom, de quelle partie de la structure de l'ICANN ils font partie, simplement en une phrase. Et ensuite, on présentera de manière assez générale le sujet. En fait, c'est un petit peu la version écourtée d'un webinaire qui a eu lieu récemment sur ce sujet.

On va commencer par vous.

GABRIEL ANDREWS : Bonjour. Je m'appelle Gabriel Andrews. Je suis ici au nom du groupe de travail pour la sécurité publique, le PSWG. Et je suis dans l'investigation de la cybercriminalité aux États-Unis.

FARZANEH BADII : Bonjour. Je suis Farzaneh Badii. Je suis là pour représenter le groupe des parties prenantes non commerciales.

BRIAN CIMBOLIC : Bonjour. Je suis Brian Cimbolic, je suis là avec le groupe des parties prenantes des opérateurs de registre et je travaille avec le .org.

GRAEME BUNTON : Bonjour. Je m'appelle Graeme Bunton. Je travaille pour Tucows, bureau d'enregistrement canadien, et je suis là au nom du groupe des parties prenantes des bureaux d'enregistrement.

MASON COLE : Bonjour. Je m'appelle Mason Cole. Je travaille pour des avocats et je suis là au nom de l'unité constitutive commerciale.

JEFF BEDSER : Je suis Jeff Bedser. Je suis là au nom du SSAC.

BRUNCE TONKIN : Merci. Alors je vais passer la parole à Gabriel qui va nous donner une version rapide des diapositives qui ont été présentées lors du webinaire il y a quelques semaines de cela.

GABRIEL ANDREWS : On va tester le son. Ça fonctionne.

Pour commencer, je sais qu'il y a eu beaucoup de discussions qui ont eu lieu sur la définition de l'utilisation malveillante du DNS et le désir d'une bonne définition.

Du point de vue du PSWG, il y a déjà d'excellentes tentatives pour définir cet espace. Et en particulier, je crois que souvent, on se réfère à l'avis que le GAC a émis en 2013, donc l'avis de Pékin ; vous le voyez ici en haut. Je ne vais pas vous lire toute la diapositive mais vous avez là certaines des recommandations initiales par rapport à ce que l'on pense qu'est l'utilisation malveillante du DNS. Il y a la question dans contrats, il y a spécification 11.3b. Pour nous, ceci est ce que les parties contractantes doivent considérer comme leur responsabilité en cas d'utilisation malveillante dans l'écosystème de l'internet.

Et depuis lors, nous savons qu'il y a eu beaucoup de discussions très intéressantes, beaucoup de suggestions par différentes parties de bonne foi pour adapter la compréhension que nous avons de la sécurité et de l'utilisation malveillante du DNS.

Nous savons qu'il y a le DAAR qui essaie de quantifier certaines choses, le signalement des cas d'utilisation malveillante des noms de domaine. Il y a différentes méthodologies qui ont été suggérées pour améliorer ceci. Et nous savons également que le cadre pour s'occuper de ces mauvaises utilisations est le résultat d'un effort collaboratif de différentes parties contractantes, de différentes unités constitutives pour aller un petit peu plus loin pour décrire les lieux où les utilisations malveillantes doivent être traitées. Donc nous apprécions

énormément les efforts de collaboration pour essayer de trouver des solutions à tout ceci.

Ceci étant, je souhaite m'assurer qu'on ne perde pas de vue ce qui se passe dans la réalité. Très souvent, dans la réalité, on parle de cybercriminalité plutôt que d'utilisation malveillante du DNS. Et donc dans la réalité, les exemples qui se manifestent, on peut les définir, il faudrait une parfaite définition. Je vous donne trois exemples de ce que l'on peut voir dans la réalité.

Premier exemple, il s'agit des courriels professionnels compromis. Et ceci peut être très simple mais vraiment causer d'énormes dommages. Donc ce sont des mauvais acteurs qui convainquent des gens d'envoyer de l'argent. Je crois que c'était un exemple où on demandait à la victime d'envoyer 250 000 $.

Les domaines que vous voyez ici en fait sont vrais. J'ai demandé la permission des victimes, je n'ai pas demandé la permission du mauvais acteur. Nous n'avons pas mis le nom à l'écran mais vous voyez, c'est très simple finalement. Il n'y a pas vraiment besoin de compétences techniques. Et vous voyez que les caractères changés, il n'y en a que quelques-uns qui ont été changés, donc entre « iet » et « jet ». Donc vous voyez, un seul caractère entre les deux domaines permet cette manipulation. Le budget de BEC a été mis en danger. Cela aurait pu éliminer cette entreprise du monde entier. Et cela nous a coûté 26 millions de dollars.

Cela a un impact sur 177 pays dans le monde. Il n'y en a que 195 sur Wikipédia. Je ne sais pas quels sont les quelques unes de ces nations

qui ne sont pas affectées, mais vous voyez à quel point ce problème est important.

Cette diapositive par rapport aux réseaux zombie, je sais que ce n'est pas très clair mais vous voyez que les réseaux zombie affectent énormément d'ordinateurs. Vous avez par exemple votre père qui vous dit que vraiment, son ordinateur ne fonctionne pas bien, il est lent. Et en fait, c'est un contrôle par un réseau zombie et donc l'utilisation des algorithmes d'enregistrement de domaines permettent à ces réseaux zombie d'opérer.

Vous voyez ce qui est en rouge, ce qui est surligné, ce sont des domaines qui sont générés par un algorithme. Donc le mauvais acteur utilise ceci pour contrôler les différentes machines du monde entier. Et ce qui est intéressant, c'est que les DGA, ces algorithmes d'enregistrement de domaines, utilisent le spam. Donc je vous invite à venir m'en parler dans le couloir. Il n'y a pas d'utilisation légitime. Si vous les connaissez, n'hésitez pas à me le dire. Mais parfois, les DGA font partie du processus d'enregistrement, je ne vois pas pourquoi.

Troisième catégorie, les rançonlogiciels. Ce sont des attaques qui sont vraiment dommageables. Si vous êtes à une conférence de l'ICANN, quand vous vous réveillez le matin en général, si vous êtes comme moi, vous allumez votre téléphone. Vous avez peut-être vu cela un matin, c'est donc apparemment selon la police canadienne une petite ville, et vous voyez dans l'intitulé qu'ils ont été attaqués par un rançonlogiciel. En fait, c'est un logiciel malveillant qui arrive sur votre ordinateur et qui chiffre tous vos fichiers de manière à ce que vous ne

puissiez plus y avoir accès. Vous ne pouvez plus voir ce qu'il y a sur votre ordinateur. Et au-delà de cela, cela infectera tous les ordinateurs qui sont sur le réseau. On vous demande de payer une rançon. Si vous payez la rançon, vous aurez peut-être accès à votre ordinateur ou non.

Alors vous voyez, cette attaque est venue d'un pourriel, d'une adresse spam. Les gens du Nunavut sont en train de se préparer pour l'hiver. Alors eux, ils sont en train d'essayer de mettre en marche leurs chasse-neiges. À votre avis, est-ce qu'ils se préoccupent de l'utilisation malveillante du DNS ? Non.

BRUCE TONKIN : Merci Gabriel.

Un petit point sur les bureaux d'enregistrement et les opérateurs de registre s'il vous plaît.

BRIAN CIMBOLIC : Oui, nous allons les présenter ensemble. Nous allons parler des obligations des bureaux d'enregistrement et des opérateurs de registre tous les deux.

GRAEME BUNTON : Nous allons donc commencer par les obligations contractuelles des bureaux d'enregistrement qui sont relativement claires.

Il y a trois dispositions dans nos contrats : s'occuper des utilisations malveillantes ; i faut qu'il y ait toujours un contact qui soit entretenu ;

et il faut investiguer de manière appropriée à tout signalement d'utilisation malveillante. Nous devons avoir les coordonnées d'un agent d'application de la loi 24/24 et nous devons publier nos procédures sur notre site web.

BRIAN CIMBOLIC : Du côté des opérateurs de registre, la plus grande obligation est dans la spécification 11.3b. Cela veut dire que les registres doivent effectuer des analyses techniques régulières pour identifier les menaces de sécurité, Dave en a parlé un petit peu, tout ce qui est phishing, malwares, réseau zombie. Et nous devons maintenir des rapports statistiques sur les menaces qui sont identifiées et les actions que nous engageons à la suite de ces menaces.

Ensuite, il faut reconnaître dans le cadre de ces conversations ce que peuvent faire les bureaux d'enregistrement et ce qu'ils ne peuvent pas faire. Même chose pour les opérateurs de registre. Nous n'avons qu'une option pratique pour nous occuper des utilisations malveillantes, c'est en fait la suspension du nom de domaine. Cela se fait du côté du registre par le *server hold* et du côté du bureau d'enregistrement par le *client hold*. Il y a aussi redirection et transfert, c'est un remède assez extrême. Effacement : ce n'est pas efficace parce que si le domaine a été utilisé à mauvais escient, une fois qu'il est effacé, il peut être réenregistré et de nouveau utilisé à mauvais escient. Donc la suspension du domaine est finalement la solution la plus efficace et le réel outil que nous avons à notre disposition des

bureaux d'enregistrement et opérateurs de registre pour nous occuper de l'utilisation malveillante.

Donc n'oubliez pas que nous agissons au niveau du nom de domaine. Donc s'il y a un problème de contenu, une plainte, nous ne pouvons pas agir à ce niveau-là. Peut-être que l'hébergeur pourra éliminer une partie du contenu ; nous ne pouvons pas le faire. Nous ne pouvons agir qu'au niveau du nom de domaine.

GRAEME BUNTON : Autre petit ajout. Agir au niveau du nom de domaine s'il y a un problème de courriel, en fait c'est compliqué parce que nous ne voulons pas avoir d'impact sur des adresses courriels au niveau du nom de domaine.

Et il y a aussi autre chose sur les domaines non enregistrés, surtout par rapport aux DGA. Il n'y a pas beaucoup de bureaux d'enregistrement qui ont des outils qui permettent d'éviter les enregistrements qui n'existent pas encore ; cela, c'est un problème assez intéressant.

BRIAN CIMBOLIC : Les DGA, les algorithmes d'enregistrement de domaines, c'est un domaine de travail dans lequel nous travaillons avec le PSWG et plusieurs agences d'application de la loi. Nous découvrons l'algorithme, nous travaillons avec le registre de manière à enregistrer ou à bloquer les noms de domaine avant même qu'ils soient utilisés.

Donc ces deux diapositives étaient importantes pour d'une part reconnaître ce que nous sommes forcés de faire de par le contrat et une fois que nous avons identifié une mauvaise utilisation, que pouvons-nous faire du point de vue technique. Cela, c'est vraiment la référence. Mais il faut également reconnaître que les opérateurs de registre et les bureaux d'enregistrement régulièrement dépassent ce qui est indiqué dans les contrats. Donc nous avons des politiques d'utilisations qui justement s'occupent des questions relatives au contenu dans les sites web.

Il y a, comme Gabe l'a mentionné, un certain nombre de bureaux d'enregistrement et d'opérateurs de registre qui ont ensemble publié un cadre pour s'occuper de l'utilisation malveillante. Il faut savoir que c'est simplement un ensemble de pratiques recommandées que nous suggérons à l'adoption.

Les parties contractantes travaillent souvent avec des notifiants de confiance. Nous travaillons par exemple avec l'Internet Watch Foundation pour tout ce qui est pornographie infantile dans le .org et il y a beaucoup d'autres opérateurs et bureaux d'enregistrement qui font des coopérations et ont des initiatives du même type.

Et il y a récompense des bons comportements. Donc au PIR, nous avons un indice de bonne performance ou performance adéquate qui permet de mesurer tout ce qui est utilisation malveillante et qui récompense en fait tout ce qui est une bonne utilisation de qualité. Donc lorsque les enregistrements sont de qualité, nous avons ce programme. Dans le SIND, le .nl a quelque chose se similaire.

GRAEME BUNTON : Je ne vais pas parler au nom des opérateurs de registre mais pour les bureaux d'enregistrement, en général, on n'explique pas bien le travail que nous faisons dans cet espace. Donc la réalité, c'est que les bureaux d'enregistrement agissent toute la journée et tous les jours dans le domaine des utilisations malveillantes. Nous éliminons 100 domaines par jour. On ne le dit pas, on n'en fait pas la publicité mais je vous garantis que ceci existe dans tout le secteur. Il y a énormément d'activités, c'est vraiment un travail important. Et en fait, on ne dit tout simplement pas aux gens à quel point cela fait partie de notre.

Et enfin, par rapport à la définition de l'utilisation malveillante du DNS, c'est une des raisons pour lesquelles ce cadre de travail a été publié. On souhaitait en fait par défaut agir parce que c'est bien beau parler de cette définition, etc. mais nous souhaitions quand même publier ce que nous faisions et ensuite avancer et nous attaquer à certains de ces problèmes plutôt que d'en discuter à l'infini.

BRIAN CIMBOLIC : Justement par rapport à ce que vient de dire Graeme, ce n'est pas uniquement une discussion académique. Les bureaux d'enregistrement, les opérateurs de registre agissent. Nous avons commencé à PIR à faire la liste de nos statistiques et au troisième trimestre de 2019, nous avons suspendu 28 000 noms de domaine. Donc on le fait au jour le jour. On ne fait que commencer de parler des résultats. C'est simplement cela.

BRUCE TONKIN : Je crois que c'est important. Nous avons entendu un bureau d'enregistrement et un opérateur de registre de gTLD et je crois que c'est important pour les opérateurs d'extensions géographiques de savoir ce qui se fait. Il y a le .eu, il y a un certain nombre de cc qui ont des programmes financiers pour motiver un bon comportement. Il y a également les notifiants de confiance. C'est quelque chose qui existe dans l'espace des extensions géographiques.

Nous avons parlé de la définition de l'utilisation malveillante, Gabriel dans sa première diapositive a parlé du phishing, du pharming, du malware, du réseau zombie.

Le rapport de l'ICANN parle du spam, le pourriel. Parfois, le spam, c'est simplement du marketing. Cela prend différentes formes. Il y a le marketing, on essaie en fait de vendre des produits. Les pays ont des lois parfois où on a le droit de le faire une fois et après, les gens peuvent se désabonner. Mais le spam, c'est aussi un mécanisme pour lancer des attaques de hameçonnage ou de phishing. Donc une des clarifications dans le document, c'est que parfois, les attaques peuvent venir de ces spams.

Mais je voudrais revenir aux autres membres du panel et j'aimerais qu'on parle de cette définition dont on a parlé jusqu'à maintenant. Est-ce qu'elle est trop étroite ? Est-ce qu'elle est trop large ? À votre avis, que devrait-être cette définition de l'utilisation malveillante du DNS ?

On va commencer par Farzaneh. À votre avis, quelle devrait être la définition de l'utilisation malveillante du DNS ?

FARZANEH BADII : Merci.

Au NCSG, nous pensons que l'utilisation malveillante du DNS à l'ICANN devrait être définie de manière technique et limitée. L'ICANN ne devrait pas s'engager vis-à-vis de programmes non techniques qui luttent contre l'utilisation malveillante du DNS.

Et moi, ce qui me surprend, c'est que nous avons une définition. Et la définition n'a pas forcément à être parfaite mais elle doit être limitée et technique. En fait, on ne peut pas lutter contre toute sorte d'utilisation malveillante du DNS qui se produit de par le monde tout simplement parce que le DNS a été utilisé à des fins délictueuses. Il faut voir si c'est stipulé, si cela relève du mandat de l'ICANN de lutter contre ce genre d'utilisation malveillante. Et jusqu'à présent, je n'ai vu nulle part dans aucun document que l'on puisse me démontrer une nouveauté en termes d'utilisation malveillante. Outre les exemples qu'ont donnés les bureaux d'enregistrement et opérateurs de registre, je n'ai vu aucune autre utilisation malveillante technique du DNS qui existe et qu'on n'ait pas prise en considération.

Donc je pense que le problème auquel on est confronté, ce n'est pas celui de la définition puisqu'on a une série de solutions ici et là, mais on n'a pas de mécanisme cohésif de gouvernance, on n'a pas de

politiques mises en place qu'on puisse mettre en œuvre pour régler tel et tel problème. Pour moi, c'est cela le problème à mes yeux.

BRUCE : Oui, Mason.

MASON COLE : J'aimerais saluer les opérateurs de registre et bureaux d'enregistrement puisqu'ils ont dit que par défaut, ils avaient agi et c'est une très bonne chose. L'utilisation malveillante du DNS, c'est une réalité et il le faut le régler aujourd'hui et pas demain. Donc on peut tourner autour du pot par rapport à la définition.

Mais par rapport à la déclaration du BC de la semaine dernière par rapport à l'utilisation malveillante du DNS, la définition, c'est une action qui entraîne des dommages significatifs et qui vont à l'encontre des objectifs légitimes.

Au-delà de cela, vous avez fait un excellent travail pour vous rapprocher d'une définition technique lorsqu'il est question de la distribution de programmes malveillants, de hameçonnage, de réseaux zombie, d'infractions au droit de propriété intellectuelle, de pratiques illicites et de contrefaçons. Cela, c'est une excellente classification et c'est un excellent point de départ pour commencer cette discussion.

La définition de l'utilisation malveillante du DNS a été reprise et pendant la transition, le BC a fait son possible avec le Conseil

d'Administration pour nous protéger de cela. Et on a appris au début de la semaine qu'il y a eu certaines difficultés au sein de l'ICANN pour appliquer ou plutôt pour voir ce que le service de conformité peut faire pour améliorer cela.

BRUCE TONKIN : Jeff ?

JEFF BEDSER : Merci Bruce.

Moi, je travaille dans une société et je suis très fier de ce que fait le PIR. Et j'ai quelques expériences en termes d'utilisation malveillante de DNS.

Pour moi, la définition de l'utilisation malveillante renvoie au fait qu'en fin de compte, il y a une victime dès qu'il y a utilisation malveillante, une victime qui a des problèmes en termes financiers. Voilà le type d'utilisation malveillante auquel on fait face.

Donc c'est un problème éthique finalement. On parle d'un écosystème qui a environ 200 ou 250 opérateurs de registre, plus de 2 000 bureaux d'enregistrement mais lorsqu'il s'agit d'hébergement, vous avez plus d'un millier d'entreprises d'hébergement et pour le reste, une centaine de milliers d'entreprises.

Et il y a de plus en plus de victimes et cela ne cesse de croître. Donc si on ne prend pas de mesures, les gens continuent de tomber dans ce problème. Et je pense que lorsque vous allez vers l'opérateur de

registre, il faut absolument lutter contre ce genre de problèmes pour qu'il n'y ait plus de victimes. Et c'est très souvent au niveau de l'hébergement qu'il faut agir.

Donc si on réunit toutes ces compétences entre bureaux d'enregistrement, opérateurs de registre et hébergement, on va pouvoir régler le problème.

BRUCE TONKIN : Merci Jeff.

Graeme.

GRAEME BUNTON : Très brièvement.

Vous savez à ce niveau-là, par rapport à la définition – et bien sûr, je ne veux pas continuer à discuter de cette question de la définition – mais vous savez, j'ai entendu beaucoup cette semaine que certaines personnes disaient qu'on allait bien trop loin, que c'était une erreur. D'autres disaient qu'on n'allait pas suffisamment loin. Et pour moi, c'est un débat classique à l'ICANN ; on n'est pas d'accord.

Mais très brièvement, par rapport à ce qu'a dit le BC, ce qui est légitime à mes yeux – et j'ai du mal à voir ici ce qui est légitime aux yeux des uns et des autres – pour moi, ce qui est légitime, c'est de prendre une action.

BRUCE TONKIN : Ce qui a été dit auparavant, c'est que la question générale, c'est la proportionnalité. Donc que faites-vous lorsqu'il y a un nom de domaine qui cause des problèmes ? Si vous avez un spam avec une adresse courriel, le nom de la personne gmail.com, la plupart des gens pensent que le fait de supprimer gmail.com va régler le problème. Ou pour YouTube, la plupart des gens disent qu'il vous mieux ne pas retirer le .com parce que c'est un mauvais contenu.

Donc cette question de proportionnalité, à savoir que la solution qui est proposée consiste à dire que les opérateurs de registre et bureaux d'enregistrement peuvent agir à ce niveau-là ou doivent s'adresser aux titulaires de nom de domaine ou à l'hébergeur. Et dans les présentations, on a bien vu qu'il y a des conditions de la part des bureaux d'enregistrement pour fournir un contenu en termes d'abus ainsi que du côté des autorités chargées de l'application de la loi.

Mais il faut également ce qu'il se passe du côté du titulaire de nom de domaine. Traditionnellement, il y avait un service WHOIS pour voir quels étaient les détails des contacts pour connaître quelle était l'entreprise qui gérait. Mais or cette information disparaît pour être en conformité avec des lois concernant la vie privée. Donc s'adresser à l'hébergeur, oui d'accord, mais comment suggérez-vous qu'on trouve les coordonnées des personnes pertinentes ? Cela peut être un problème actuellement.

BRIAN CIMBOLIC : Merci Bruce.

Par rapport à la question, il y a toujours une question de proportionnalité lorsque vous parlez de l'utilisation du système des noms de domaine pour traiter la question du contenu de l'utilisation malveillante des noms de domaine.

Ce n'est pas aussi simple que cela. D'un autre côté, vous avez le niveau de dommages. Il est disproportionné d'agir sur le contenu pour ce genre de choses.

Mais lorsqu'il s'agit de distribution de pornographie infantile en ligne, alors là, oui, vous avez un dommage physique et humain qui justifie que l'on intervienne et que cette réponse soit celle-ci et qu'on prenne les choses très au sérieux. Donc cela dépend de ce à quoi vous avez affaires. Bien entendu, il faut essayer d'agir de cette manière et il faut essayer d'agir en montant les échelons petit à petit, mais tout dépend de la gravité des choses.

BRUCE TONKIN : Une question spécifique.

Lorsque vous pensez que vous ne pouvez pas entreprendre d'action et que vous pensez que c'est au bureau d'enregistrement d'agir, comment est-ce que vous pensez que la communauté peut agir ? Quels sont les outils à sa disposition ? Parce que je peux appeler le bureau d'enregistrement mais qu'est-ce qui se passe après ?

GRAEME BUNTON : Je pense que Jeff est plus à même de répondre à cela.

Mais je pense qu'il y a une différence importante ici entre l'hébergeur et le titulaire du nom de domaine. Et on peut avoir une conversation pour savoir comment faire en sorte que ce soit plus transparent et quels sont les outils qui existent et qui sont à la disposition de la communauté. Peut-être que Jeff les connaît.

JEFF BEDSER : Oui. Cela implique d'enquêter un petit peu, de faire des recherches. Il y a beaucoup de changements ces dernières années. Par exemple, si vous utilisez un fournisseur DNS comme Cloudflare, le système est le suivant. Vous avez en cache l'hébergeur, donc il faut les contacter pour trouver les coordonnées de l'hébergeur. Et il y a *bulletproof hosting* qui vous permet d'éviter les dénis de service distribués. Et si quelqu'un arrive à votre porte avec un badge et vous dit : « On ne peut pas entreprendre aucune action. », dans ce processus, comment passer entre le premier contact, deuxième contact, troisième contact avant que vous puissiez entreprendre quelque action que ce soit si tant est que vous puissiez en entreprendre une. Qui est responsable de ce contenu ? Il faut qu'il y ait une méthodologie qui fasse en sorte qu'on puisse trouver plus facilement ces personnes à contacter.

BRUCE TONKIN : Gabriel ?

GABRIEL ANDREWS : S'agissant des lacunes et du rapport d'utilisation malveillante, je pense qu'il est important d'avoir une conversation honnête par

rapport au fait de faire rapport sur la conformité. Et quand on nous dit : « Oui, je sais que ce domaine a beaucoup de rapports d'utilisation malveillante. », il faut aussi que ces abus soient notifiés au sein de l'ICANN et que ce cercle soit complet et qu'on puisse faire plus au niveau de la conformité.

Si on n'a pas de suivi obligatoire du nombre de réclamations et de notifications d'utilisation malveillante, cela va être très difficile d'avancer. Il faut pouvoir assurer un suivi spécifique de ces notifications. Sinon, toutes ces notifications ne servent à rien finalement.

BRUCE TONKIN : D'après ce que je comprends, on n'a pas de bonne solution encore. Et plus cela va, plus les choses se compliquent. Donc il faut se protéger par rapport aux attaques de déni de service, par rapport à l'infrastructure de l'internet qui veut que typiquement, entre l'opérateur de registre et l'utilisateur, l'opérateur de registre soumet des choses au bureau d'enregistrement, puis le revendeur peut utiliser un fournisseur de DNS qui peut utiliser un pare-feu. Donc il y a toute une série d'entreprises. Il y a 10 ou 15 organisations qui interviennent pour fournir un service.

Donc essayer de trouver la bonne personne pour appliquer certaines actions, cela peut s'avérer vraiment difficile. Et ce genre d'informations n'est tout simplement pas disponible. Donc peut-être que les bureaux d'enregistrement pourraient agir davantage pour ce qui est des informations pour contacter l'hébergeur ou autres.

Oui, Farzaneh.

FARZABEH BADII : Je voulais dire clairement que lorsqu'on parle de contenu, on ne parle absolument pas de quoi que ce soit qui soit lié à l'ICANN parce que pour ceux qui ne le savent pas, dans nos statuts constitutifs, il y a des dispositions qui empêchent l'ICANN de règlementer quelque partie du contenu que ce soit. Donc mélanger le niveau contenu avec le niveau technique, c'est extrêmement dangereux. Donc il faut être clairs par rapport à ce que l'on entend par réglementation du contenu.

Et par rapport aux opérateurs de registre et bureaux d'enregistrement et des actions qu'ils peuvent entreprendre en dehors de l'ICANN, je pense qu'ils doivent être à même de prendre des actions – cela ne fait aucun doute. Et s'ils veulent que ces actions soient davantage légitimes, peut-être qu'il faudrait qu'ils soient plus transparents par rapport aux politiques qu'ils mettent en œuvre, par rapport à la manière dont ils les mettent en œuvre et avoir également en place des processus de diligence raisonnable qui feraient que s'ils appliquent ces processus, l'utilisateur pourrait effectivement en bénéficier.

BRUCE TONKIN : Oui, c'est une bonne question Farzaneh. Effectivement, quels sont les recours que peuvent appliquer les bureaux d'enregistrement et opérateurs de registre ?

BRIAN CIMBOLIC : Oui, c'est une bonne question et c'est une question sur laquelle on continue de travailler et on essaie de mettre en place des processus de recours pour les PIR. Donc ce serait un processus où le titulaire de nom de domaine a un domaine qui a été suspendu et qui pourrait faire appel auprès d'un tiers. En attendant, cela passe par un courriel auquel on peut s'adresser pour dire : « Mon domaine a été suspendu. » Et si on peut démontrer que c'est un cas de compromis, on entreprendra des actions. Donc si un titulaire de nom de domaine vient nous voir et il nous prouve que son nom de domaine a été compromis, alors on reverrait cette décision de suspension.

BRUCE TONKIN : Merci.

L'une des choses qui a émané de la révision CCRT, c'est savoir s'il y a beaucoup d'utilisations malveillantes au niveau des opérateurs de registre et des bureaux d'enregistrement, comment mettre en place un processus pour surveiller les choses. Il y a également eu une suggestion d'amélioration de la part de l'équipe CCRT, voir quelles seraient les mesures d'encouragement financières qu'on pourrait mettre en place.

Est-ce que les membres du panel ont des suggestions ou des commentaires à faire sur ces deux aspects ?

GABRIEL ANDREWS : Ce que je veux dire, c'est que l'action qui est entreprise par le PIR devrait être analysée.

Lorsque vous parlez de mesures d'encouragement pour les opérateurs de registre, sachez que si vous prenez toutes ces mesures pour lutter contre cela, vous obtiendrez tel avantage. Et c'est une bonne chose parce que les délinquants ont une carotte qui les pousse à agir. Donc il faut mettre en place un bâton pour s'assurer que le délinquant se pose la question : « Est-ce que je suis en train d'agir de la bonne manière ? » Et on doit aussi se demander ce qu'on peut faire pour encourager les opérateurs de registre qui à leur tour vont encourager les bureaux d'enregistrement.

Dernier commentaire. Il y a l'histoire du bâton aussi. Quelles sont les mesures de découragement qui peuvent être employées ? Comment quantifier le nombre de bons et de mauvais ?

BRUCE TONKIN : Graeme.

GRAEME BUNTON : Merci.

Je pense qu'on n'a pas suffisamment parlé de programmes d'encouragement. C'est finalement une nouvelle idée, en tout cas à mes yeux. Et je pense qu'il faut être très prudents pour ce qui est de la définition de ce genre de programmes, les mesures qu'on pourrait utiliser pour mettre en place ces programmes.

Mais en général, nos marges sont très limitées. Donc peut-être qu'il faudrait l'analyser davantage.

BRUCE TONKIN : Mason ?

MASON COLE : J'étais à une époque avec les parties contractantes, donc je comprends bien qu'en termes d'incitations financières, cela peut être une solution attrayante. Moi, je pense qu'on devrait se pencher là-dessus.

Peut-être qu'on pourrait aussi revoir les contrats pour voir s'il y a des manières de travailler sur ces contrats et améliorer le texte de manière à avoir un impact sur l'utilisation malveillante du DNS. Parce qu'on s'est bien rendus compte cette semaine que les contrats ne sont pas aussi solides qu'on le pensait. On aurait peut-être une opportunité de justement renforcer ces outils.

BRUCE TONKIN : Les contrats finalement se limitent au signalement. C'est une question de collecte de statistiques. Les opérateurs de registre font un rapport aux bureaux d'enregistrement. Les bureaux d'enregistrement font leur rapport et ils font leur investigation. Mais je crois que le texte est assez vague. Donc effectivement, je pense qu'améliorer le texte dans les contrats, ce serait quelque chose de positif.

Y a-t-il d'autres choses à évoquer du point de vue du panel, des questions pratiques sur ce que pourrait faire ICANN Org ou la communauté ?

BRIAN CIMBOLIC : Par rapport à la question des programmes d'encouragement, c'est une petite anecdote mais avec notre programme QPI, nous avons vu des bureaux d'enregistrement qui ne reçoivent pas de programmes d'encouragement et qui ne sont pas aussi agressifs par rapport aux exploitations malveillantes. Donc ils nous disent : « Mais comment pouvons-nous nous améliorer ? » et tout est basé sur les fonds. Mais je pense que ce type de comportement pourrait s'adapter à l'ICANN. Si les différents acteurs étaient motivés financièrement, je pense que les choses seraient beaucoup plus efficaces.

BRUCE TONKIN : Du point de vue efficace, il y a les frais de l'opérateur de registre, il y a les frais de l'ICANN et il y a les frais du bureau d'enregistrement. Donc c'est quelque chose de très large et je pense que des programmes d'encouragement pourraient s'appliquer à différents niveaux.

FARZANEH BADII : Cette discussion sur les programmes d'encouragement, à mon avis, il faut faire attention parce qu'on parle d'encourager, on parle de motiver, des programmes d'incitation et le risque, c'est qu'ils soient remplis d'un zèle à éliminer tout un tas de domaines. Et cela n'est pas dans l'intérêt des titulaires de nom de domaine. On pourrait dire : « Oui, bravo. Lui, il a un résultat extraordinaire, il a éliminé 2 000 noms de domaine. » Je crois qu'il faut faire attention.

Il faut faire attention au processus. Nous avons les mécanismes en place qui existent, donc nous pouvons faire quelque chose par rapport à l'exploitation malveillante du DNS lorsqu'elle se produit. Et je pense que c'est cela, l'objectif.

Par ailleurs, pour parler de manière peut-être plus agréable, le DNS dans le cadre de l'internet a pour objectif de connecter le monde entier et de nous faire prospérer au jour le jour. Ce n'est pas uniquement un moyen de commettre des crimes. C'est important de se le rappeler.

BRUCE TONKIN : Oui, effectivement. L'internet est une force pour le bien.

BRIAN CIMBOLIC : Oui, tout à fait. Je pense que Farzaneh a raison. Mais je parlais uniquement de l'utilisation abusive du DNS. Et on parle uniquement du petit nombre de mauvais acteurs, pas du reste.

Nous avons suspendu 28 600 et quelque domaines et c'est un petit nombre parce qu'il y en a également plusieurs qui étaient liés au CSAM. Donc nous avons également une remédiation. C'est ce que nous souhaitons observer. Nous ne souhaitons pas agir au niveau du nom de domaine. Donc nous nous occupons du problème. Le contenu, c'est vraiment un tout petit chiffre dans un espace beaucoup plus large d'abus du DNS. Il s'agissait de seulement huit domaines.

BRUCE TONKIN : CSAM, pour ceux qui ne le savent pas, c'est le code qui est utilisé chez nous pour parler de pornographie infantile.

GABRIEL ANDREWS : Votre commentaire par rapport au processus est effectivement excellent. Il y a beaucoup de choses que l'on peut faire à ce niveau-là. Et personnellement, j'aimerais bien collecter différentes bonnes pratiques qu'on a pu voir dans l'espace des ccTLD. Je ne sais pas si vous l'avez déjà entendu mais nous avons pu observer que votre idée, en particulier, essaie de bloquer les domaines qui se ressemblent. Parfois, les domaines sont très similaires, le domaine victime et le domaine du mauvais acteur.

Par ailleurs, il y a un autre processus utilisé pour utiliser les anciens signalements d'abus pour identifier les abus en temps réel. Le meilleur prédicteur des comportements futurs, c'est le comportement passé. N'est-ce pas ? Et donc ce type de travail, c'est quelque chose qu'il faut applaudir et peut-être même récompenser. Moi, je pense que c'est logique de récompenser.

BRUCE TONKIN : Graeme.

GRAEME BUNTON : Très brièvement, je voulais remercier Farzaneh pour ce qu'elle a dit. Je crois que c'est très important, surtout si on réfléchit à des programmes d'encouragement. Il ne faut pas le faire dans le vide. Il

faut avoir des mécanismes de recours, il faut que la transparence fasse partie du processus, il faut que le processus soit vraiment solide de manière à ce que cela ne devienne pas problématique.

JEFF BEDSER : Et je crois qu'une des incitations principales, c'est que cela permet de se différencier du point de vue du marché, d'avoir un bon écosystème propre, on est un bon voisin et on n'est pas associé avec tout ce qui est utilisation malveillante.

Comme Graeme l'a dit, on n'en fait pas assez pour montrer le travail qui est effectué parce que les bons acteurs, les bonnes organisations en fait devraient bénéficier de leur travail et obtenir davantage de clients. Certaines incitations pourraient simplement de faire le bien, c'est sa propre récompense et cela est bénéfique pour vous.

BRUCE TONKIN : Voilà, nous en sommes à la moitié de la séance. Nous allons commencer par le premier intervenant.

MARK SEIDEN : Nous avons vraiment un marteau contondant et nous sommes vraiment dans la chaîne alimentaire en haut. Donc nous pouvons finalement gérer le contenu aussi.

Et je crois qu'il est pratiquement impossible pour nous en tant qu'opérateurs de registre et bureaux d'enregistrement de faire des investigations sur certains de ces rapports parce que nous n'avons pas

accès au contenu. Et parfois, on n'arrive même pas à reproduire le problème qui nous a été signalé. Donc je comprends, oui il faut aller à la machine way-back, aller voir l'enregistrement des domaines, vous avez parlé d'essayer de comprendre ce qui se passe, etc. On invente des systèmes qui finalement sont défaillants et qui, à mon avis, sont un petit peu comme un objet contondant.

Et puis il ne faut pas non plus former l'adversaire. Par exemple en termes d'actions par rapport à l'algorithme d'enregistrement de domaines, les empêcher d'enregistrer tout autre domaine avec un DGA, il serait bien mieux de prendre leur argent et de leur refuser le service. Ce qui veut directeur qu'il y aurait en fait une sanction financière. En plus, on aurait un peu d'argent. Donc ne formez pas l'adversaire, il va aller autre part. Ou alors, changez le DGA. Ils pourraient le faire très facilement.

BRUCE TONKIN : Excellentes suggestions.

ELLIOT NOSS : Merci Bruce.

Je travaille avec Tucows.

Nous parlons depuis 45 minutes et même depuis 20 ans de ce sujet. Il y a eu d'excellents progrès puisque nous avons six panelistes qui ont en fait six points de vue et vous êtes tous d'accord à mon avis, selon ce que j'entends. Mais il y a quelque chose qui est enfoui dans la

discussion qu'on a eue depuis 45 minutes et qui à mon avis est extrêmement important pour faire des progrès en 2019 et en 2020. C'est ce qu'a dit Mason, la conformité a des problèmes par rapport au PIC spec.

Et dès le début de ce panel, ce qui m'a frappé, c'est les trois exemples de Gabriel, les trois exemples monstrueux d'utilisation malveillante du DNS. Chacun de ces exemples fait l'objet d'une action par des bureaux d'enregistrement responsables. Je crois, je le crois depuis dix ans, j'ai vérifié avec la conformité avant d'arriver ici. Donc maintenant, on en est aux bons bureaux d'enregistrement/mauvais bureaux d'enregistrement. Il y a des gens qui sont là, il y a des gens qui ne sont pas là.

Je suis fatigué de cela depuis des années, je le dis au forum public depuis des années. Il nous faut maintenant passer à l'action.

Le membre les plus important de ce panel qui pourrait contribuer à faire avancer les choses ne fait pas partie du panel. C'est soit Jamie, soit John Jeffrey, soit les deux. Parce qu'ils pourraient nous expliquer pourquoi la conformité n'est pas en mesure de faire appliquer ce qui à mon avis fait partie des quatre coins du contrat tel qu'il existe actuellement.

J'ai une certaine empathie par rapport à eux, par rapport à la position dans laquelle ils se trouvent. Et je crois qu'il nous faut rassembler tout le travail de la communauté ensemble parce que vous êtes tous d'accord. Vous êtes tous d'accord, pour le meilleur et pour le pire. Donc je pense que c'est là-dessus que tous, nous devons travailler.

C’est dans ceci que nous devons investir notre énergie dans l’immédiat.

Nous avons un cadre qui nous vient de la communauté et ce que je souhaite savoir – et d’ailleurs, j’en ai parlé brièvement hier lors de la séance entre le Conseil d'Administration et les parties contractantes –, c’est pas simplement de parler des personnes qui sont là et des personnes qui ne sont pas là. On parle d’incitations, d’encouragements. Aujourd’hui, il y a de claires motivations financières qui sont avancées par les opérateurs de registre mais avec une bonne intention et qui poussent aux mauvaises actions. Cela existe dans la communauté. Ce sont des personnes qui sont présentes et qui viennent régulièrement aux réunions de l’ICANN. Ceci n’est pas quelque chose dont on est inconscients. Il nous faut absolument traiter les problèmes auxquels nous sommes confrontés. Si la conformité pouvait identifier de manière efficace certains éléments spécifiques du contrat qui pourraient les aider à appliquer les règles aux mauvais acteurs, cela serait positif.

Donc parlons de ceci de manière très spécifique. La conformité doit s’occuper des mauvaises actions que nous connaissons. Et nous sommes tous d’accord pour dire qu’il faut absolument s’en occuper.

BRUCE TONKIN : Merci Elliot.

Je vais prendre un commentaire ou une suggestion en ligne.

PARTICIPATION EN LIGNE : Nous avons quatre commentaires et deux questions.

Les deux premiers commentaires sont de Maxim Alzoba : « DAAR a des faux positifs, des preuves connues, mais ne donne pas d'information utiles pour les opérateurs de registre.

Deuxièmement, il faut savoir que l'élimination sans diligence raisonnable sera utilisée par les criminels pour faire du chantage et encouragera la criminalité. »

Deuxième commentaire de Andrew Campling : « Il ne faut pas que les définitions et les petites luttes empêchent de lutter contre l'utilisation malveillante du DNS. »

Michele Neylon : « Il ne faut aucun doute que le secteur est mieux positionné pour résoudre et ajouter de nouvelles obligations aux contrats. »

Et nous avons une question de Sivasubramanian Muthusamy qui est en Inde : « Comment se fait-il qu'il y ait des limites artificielles à la mission de l'ICANN ? Si l'ICANN se limite aux abus dans l'espace des noms de domaine, il y a également des abus dans l'espace des numéros, et cela veut dire qu'il y a une grande proportion d'utilisation malveillante dont on ne s'occupe pas. Comment se fait-il que ceci soit en dehors de la mission de l'ICANN ? L'ICANN est la seule organisation qui ait les capacités techniques pour s'occuper des utilisations malveillantes qui se passent en dehors de l'espace des noms et de ce qui se passe dans le darkweb ? Comment se fait-il que l'ICANN soit réticente ? »

Dernière question de Andrew Campling : « L'écosystème du DNS a été décentralisé et collaboratif. Avec des protocoles tel que le DoH, est-ce que les opérateurs tel que Cloudflare devront scanner ou alors est-ce qu'ils exploiteront ces informations ? »

BRUCE TONKIN : Première question. Par rapport à la mission, il y a d'abord les statuts et ensuite l'ICANN qui une organisation du secteur privé et ensuite, les contrats avec les bureaux d'enregistrement et les opérateurs de registre et ensuite, il y a les contrats avec les utilisateurs finaux. Donc ce dont on parlait tout à l'heure, ce sont les limites dans les statuts et le fait que cela découle dans le reste de la hiérarchie.

FARZANEH BADII : Lorsqu'on parle de cybercriminalité en général, en partie, la criminalité existe par l'utilisation du DNS. Alors cela ne veut pas dire que toute ce qui est lié à cette criminalité doit être résolu par une organisation telle que l'ICANN. Et il est très risqué de suggérer qu'on utilise ce forum – qui est en fait une organisation centralisée – pour tout les problèmes relatifs au DNS, pour tous les abus qui ont lieu parce qu'à ce moment-là, on peut en danger l'internet ouvert, global et interconnecté.

BRUCE TONKIN : Par rapport à la deuxième question, on mentionnait un fournisseur de service spécifique et est-ce qu'ils doivent contribuer à signaler des abus. Alors il faut savoir que la chaîne d'approvisionnement est très

longue et il faut arriver à la partie de la chaîne qui cause le problème. L'idée, c'est de savoir contacter les bonnes parties en fait ; c'est cela.

Je ne vais pas parler de manière très longue sur chaque point parce que j'aimerais donner la parole à d'autres personnes. Monsieur.

ALAN GREENBERG : Bonjour.

Mon commentaire est relatif à ce qu'a dit Elliot avec une petite perspective différente.

Donc ce dont on entend parler maintenant de Graeme et de Brian, ce type de travail est vraiment encourageant. Ce n'est pas qu'il n'y avait pas des choses qui étaient faites avant mais le fait que ce soit fait en public, le fait d'encourager d'autres bureaux d'enregistrement et opérateurs de registre à le faire, c'est vraiment quelque chose de positif.

Par rapport au commentaire de Mason sur les PIC, on en entend parler depuis des décennies. Oui, on sait qu'il y a un problème mais on n'a pas les outils, la conformité n'a pas les outils. Et dans certains cas, je pense qu'Elliot a raison, il y a des clauses dans le contrat qui pourraient être interprétées comme contraignantes. Mais souvent, on nous dit : « Oui, ce n'est pas possible de vraiment les appliquer. Ce n'est pas aussi facile d'éliminer quelqu'un de cette clause parce qu'il n'a pas payé sa facture. » J'ai entendu des commentaires comme quoi le rapport DAAR est utile et important mais c'est l'OCTO, ce n'est pas la conformité.

Alors ce que je souhaite voir maintenant, c'est toutes les parties se rassembler autour de la même table. Et si la conformité a besoin de changements dans les contrats, et bien mettons-nous d'accord là-dessus et allons-y. Assurons-nous que la séparation artificielle entre le bureau technologie et la conformité ne nous empêche pas d'utiliser des informations qui sont utiles et importantes.

Comme Elliot l'a dit, il est très facile de dire que les mauvais acteurs ne sont pas à l'ICANN. Certains sont là. Donc arrêtons de faire semblant et agissons sur ce que nous pouvons faire.

BRUCE TONKIN : Merci Alan.

BRIAN CIMBOLIC : J'aimerais mettre l'accent sur quelque chose par rapport à la sensibilisation des autres bureaux d'enregistrement et opérateurs de registre et puis le cadre de travail sur l'utilisation malveillante.

C'est un appel ouvert. Si vous pensez que ce cadre de travail est quelque chose que vous pensez que vous pouvez mettre en œuvre, nous souhaitons ajouter des signataires, des personnes qui s'engagent par rapport à ce qui existe dans ce document. Donc plus on est nombreux, plus on rit. Donc nous avons un certain nombre d'acteurs qui sont engagés, des opérateurs de registre et des bureaux d'enregistrement qui sont engagés. Donc allez-y, signez.

Stéphanie ?

STÉPHANIE PERRIN : Stéphanie Perrin du NCSG. Et je suis venue au micro pour reprendre à mon compte ce que disait Farzaneh.

Mais il y a un terme qu'elle n'a pas utilisé et c'est un terme qui nous tient très à cœur, c'est la réglementation. Tout mouvement que fait l'ICANN pour encourager d'un point de vue financier ce qu'elle considère être de bonnes actions, c'est une réglementation parallèle. C'est-à-dire qu'il faut faire la différence entre les abus d'un point de vue technique et les abus d'un point de vue du contenu. Et on sait qu'il y a toute une palette d'abus en termes de contenu. Mais s'il vous plaît, je vous demande, tenez-vous-en aux abus d'un point de vue technique parce que là, vous avez suffisamment à faire. Et je pense que je peux reprendre à mon compte que ce disait à l'instant Elliot. Tant que cela est protégé et que l'ICANN ne se lance pas dans les encouragements financiers de ce qui est l'application des contrats, on ne s'en sortira pas.

BRUCE TONKIN : On ne va pas faire des commentaires sur chacune des interventions. Je veux être sûr d'écouter toutes les personnes qui viennent au micro et ensuite, je me tournerai vers les membres du panel pouvoir si vous avez des commentaires ou des réflexions.

DIRK KRISCHENOWSKI : J'aimerais faire un commentaire au nom du groupe de travail que je préside sur les géoTLD.

Par rapport aux obligations d'intérêt public y compris l'abus tel que défini par la loi nationale, l'année dernière, nous avons vu que les géoTLD gèrent quelques requêtes et de très bonne manière. J'aimerais faire part de ce sondage pour les géoTLD ; 22 ces derniers mois. Oui, il y a des abus par rapport aux géoTLD mais très peu. Seuls trois membres ont plus de 10 cas au cours de la dernière année. Nous allons publier les résultats de cette étude d'ici peu. Mais j'aimerais dire que par rapport à la discussion actuelle, on ne pense pas qu'il soit nécessaire d'appliquer d'autres mesures en termes d'obligations contractuelles et qu'il n'est pas nécessaire d'appliquer un modèle unifié d'accès.

BRUCE TONKIN : J'aimerais revenir aux questions à distance.

PARTICIPATION À DISTANCE : Question d'Andrew Campling : « Ma question quant à l'impact du DNS crypté a été mal comprise. Le système DNS a été hautement décentralisé et coopératif. Avec les protocoles tel que DoH et les résolveurs opérationnels, on peut partager les renseignements et utiliser ces renseignements à des fins commerciales. Comment est-ce que les opérateurs de registre et bureaux d'enregistrement savent là où se produisent les délits ?

BRUCE TONKIN : Il s'agit d'une question. Qui veut y répondre ?

JEFF BEDSER : Il faudrait que je réfléchisse à cela. Je n'ai pas de réponse toute faite pour l'instant.

BRUCE TONKIN : Non, on ne peut rien obliger ici mais clairement, j'ai bien compris la question. C'est une question qui porte sur les résolveurs.

BYRON HOLLAND : Byron Holland, opérateur de ccTLD pour .ca.

Merci de cette discussion, j'apprécie. Mais j'entends beaucoup de discussions un peu houleuses et j'aimerais faire quelques commentaires.

Je sais qu'il y a des gens qui ont des points de vue politiques très tranchés. Mais éloignons-nous ici de cette discussion.

La définition est importante. Les termes sont importants. Et tant que juristes, on sait que les termes sont importants. Sinon, on va partir dans tous les sens. Donc assurons-nous de bien définir les choses.

De mon point de vue, opérateur, la notion dont vient de parler Stéphanie, les abus en termes techniques et en termes de contenu, c'est important. Et la manière dont on va le définir, cela va définir la réussite d'un espace propre. Et c'est ce que l'on veut tous.

Et par rapport aux définitions des statuts constitutifs de l'ICANN qui sont très clairs par rapport à la mission, où commence la mission et où

finit la mission et par rapport à l'abus en termes de contenu, cela va au-delà de cela.

Ensuite, voyons où se trouvent les problèmes et quelles sont les règles en termes de réglementations et quelles sont les actions qu'on peut prendre. Là, le fonctionnement du DNS, cela vient ensuite et le contenu vient en troisième. Donc il faut prioriser les choses. Pour nous qui suivons les batailles de la gouvernance, beaucoup de ces batailles se livrent au niveau de la réglementation et de la législation et cela se trouve à des niveaux différents. Donc il faut s'assurer qu'on définisse bien ce dont on parle.

Et enfin, beaucoup des commentaires faits autour des acteurs individuels qui agissent, je pense qu'effectivement, il y a un espace pour cela. Mais souvenons-nous que la supervision judiciaire, ce n'est pas une mauvaise chose. Et dans les états de droit où il y a une supervision judiciaire indépendante qui donne une permission pour agir de cette manière, la supervision judiciaire, ce n'est pas un gros mot, ce n'est pas un mauvais mot, donc utilisons-le.

BRUCE TONKIN : Merci Byron.

Bill.

BILL JOURIS : Je suis membre du groupe des parties prenantes At-Large.

Les opérateurs de registre et bureaux d'enregistrement parlaient de ce qu'ils faisaient pour régler les problèmes lorsqu'ils sont identifiés. Je me demande si vous envisagez ce que vous pouvez faire pour éviter que les problèmes ne se posent.

Pour prendre l'exemple qui vient d'être donné, si vous saviez que [EZIAET] allait se poser, pourquoi est-ce que vous avez laissé ce problème se poser ? La bonne nouvelle, c'est que l'ICANN avec l'effort sur les noms internationalisés a compilé une longue liste des caractères qui peuvent prêter à confusion. Donc vous pourriez utiliser cela pour vos travaux. Ce n'est pas une liste exhaustive probablement mais en tout cas, cela va vous aider. La mauvaise nouvelle, c'est de savoir si l'ICANN publie cette liste. Et publier cette liste, cela va permettre d'éviter de semer le doute.

Je pense qu'il faudrait rendre obligatoire la publication de cette liste conformément à ce qui est stipulé dans le contrat mais pour ce faire, il faut que les opérateurs de registre et bureaux d'enregistrement s'en servent à titre de prévention.

BRUCE TONKIN : Qui souhaite intervenir ?

GRAEME BUNTON : Vous savez que je pense que le problème, c'est quand on rentre trop dans le détail. Et un système qui empêcherait l'enregistrement, cela engendrerait des problèmes qui iraient au-delà de ce à quoi on peut s'attendre. Et on rentre dans le même genre de problèmes que ce dont

il était question à l'instant avec les programmes d'encouragement. Donc il faut y réfléchir davantage.

BRUCE TONKIN : Oui. Je pense que ce que font les CC, c'est qu'ils utilisent des logiciels prédictifs pour identifier des choses qui méritent d'être examinées plus avant. Donc je pense qu'il ne s'agit pas simplement d'arrêter un enregistrement mais de voir quels sont les indicateurs qui nous poussent à enquêter.

NEIL SCHWARTZMAN : Monsieur Schwartzman.

Je trouve que cette discussion est intéressante. Bienvenue à Montréal. C'est ma ville natale. On entend une discussion qu'on connaît bien et j'aimerais donner un peu de contexte de mon point de vue.

Jusqu'à la fin août, j'étais très occupé par l'utilisation malveillante du DNS avec le DNS et dans le DNS. Et en tant que fabriquant de logiciel, nous avons vu 30 000 attaques d'hameçonnage par mois impliquant 90 000 actifs. Personnellement, j'en ai retiré 50 000 en un mois.

Donc lorsqu'on parle d'efforts – et peut-être qu'effectivement, on a besoin d'une meilleure définition puisque l'internet existe depuis 50 ans –, qu'est-ce qui fait qu'on ne peut pas définir les choses ? Il est temps d'avancer. Je ne dis pas d'avancer dans n'importe quel sens ou de manière chaotique, je comprends bien le processus, mais je pense qu'il est temps de concerter nos efforts parce qu'il y a crise. Lorsqu'il y

a anonymisation d'IP à IP, lorsqu'il y a anonymisation de savoir qui détient un actif comme un domaine, vous parlez là de personnes qui agissent à leur guise et on ne peut absolument pas imaginer le nombre d'attaques d'hameçonnage. Et toutes ces attaques ne sont pas notifiées parce qu'on n'a pas le temps de le faire. Donc tout le monde, opérateurs de registre et bureaux d'enregistrement, est finalement encouragé à ne pas investir pour lutter contre cela. En fait, c'est ce qui se passe actuellement, des noms de domaine qui sont là pour ensuite être victimes d'utilisation malveillante et il n'y a pas un système de notifications précis et correct.

Je pense que l'un des principaux bureaux d'enregistrement qui a beaucoup à voir avec le problème d'hameçonnage a trois personnes qui travaillent sur le hameçonnage. L'un d'entre eux vient d'avoir un bébé, donc ce sont deux personnes à plein temps ; ce n'est pas suffisant, clairement. Et là, je parle uniquement de hameçonnage. Je ne parle pas de dénis de service, de spam.

Mais comme vous l'avez dit à juste titre, le spam, le marketing, c'est un peu la même chose. Je ne rentrerai pas là-dedans. Mais il s'agit de renforcer la confiance des consommateurs sur l'internet. Et c'est ce pourquoi on est ici, protéger les utilisateurs finaux.

PIERRE BONIS : Bonjour, Pierre Bonis, AFNIC, ccTLD .fr.

J'aimerais reprendre ce qu'a dit Byron qui vous invitait à vous poser la question : « Pourquoi est-ce qu'on parle de cela aujourd'hui ? » Parce

que l'utilisation malveillante, ce n'est pas une nouveauté. Les abus techniques, ce n'est pas nouveau non plus et d'ailleurs, c'est dans le contrat.

Je pense qu'on parle de cela aujourd'hui parce qu'il y a de plus en plus de pression – à juste titre – de la part de bon nombre des parties prenantes en dehors de l'ICANN, à savoir les gouvernements, des organisations de la société civile, qui en ont tout simplement marre des acteurs numériques qui leurs disent : « Non, on ne peut rien faire. »

Donc il y a des plateformes énormes, des moteurs de recherche énormes et très importants qui ont dit cela aux gouvernements et à toute une série d'acteurs pendant des années. Et lorsqu'on essaie de dire qu'il y a une couche technique dont on est chargée et il y a une couche contenu dont on n'est pas chargé, plus personne ne nous écoute parce qu'ils ont entendu ce genre d'argument depuis des années maintenant de la bouche des gens qui étaient chargés du contenu.

Donc je pense qu'il est très important d'éviter de transférer les responsabilités des hébergeurs et des plateformes d'hébergement à l'industrie du DNS tout simplement parce que les gens en ont assez des explications techniques.

Et d'ailleurs, si on continue à essayer de faire quelque chose par rapport au contenu pour que les gens voient que nous sommes des acteurs responsables, en fin de compte, on ne sera pas responsables parce qu'on agira comme un gendarme. Or, ce n'est pas notre travail,

non pas parce qu'on ne veuille pas le faire mais parce que ce n'est pas démocratique.

Donc cet appel à agir, c'est bien beau mais je pense que dans un intérêt général et dans l'intérêt de tous, on doit être très prudents et dire : « Oui, on peut faire quelque chose au niveau technique mais il y a un grand risque à nous positionner d'une manière où on dit : « Celui-ci est bon, celui-ci est mauvais. » Et c'est encore plus vrai au niveau mondial pour une organisation comme l'ICANN parce que bien sûr, personne ne pense que dans une organisation mondiale et multipartite comme l'ICANN, on puisse avoir une définition de mauvais contenu qui puisse s'appliquer à toutes les juridictions internationales et à toutes les cultures aussi.

Merci.

BRUCE TONKIN : Merci.

On n'a plus beaucoup de temps. Est-ce que je peux vous demander d'être brefs dans vos interventions parce qu'on a encore beaucoup de demandes d'intervention ? Allez-y.

TOM LAM : Bonjour. Tom Lam de Cloudflare. J'ai une question et quelques commentaires puisqu'on a été ici à deux reprises déjà, nous Cloudflare.

Par rapport aux programmes d'encouragement, est-ce que les opérateurs de registre donnent aux bureaux d'enregistrement une liste de domaines qui ont été enregistrés puis effacés dans un délai de quelques jours en utilisant cette liste ? Et est-ce que les bureaux d'enregistrement décident de blacklister ces enregistrements ? Parce qu'alors, les opérateurs de registre pourraient encourager les bureaux d'enregistrement d'une certaine manière à choisir les bons domaines et développer une sorte de clients légitimes qui sont pris dans ce genre de processus.

Mon commentaire concernant Cloudflare, il a été dit que nous sommes hébergeur bulletproof. Or, nous ne sommes pas hébergeur bulletproof. Nous avons un programme pour cela. D'ailleurs, si cela vous intéresse, n'hésitez pas à nous contacter, nous vous donnerons plus de détails. On ne partage pas vos informations donc ne vous inquiétez pas, on ne partage absolument pas vos données, ce n'est pas le cas. Et nous travaillons pour traiter la question des programmes malveillants et autres.

BRUCE TONKIN : Merci.

Personne suivante s'il vous plaît.

DEAN MARKS : Dean Marks, je travaille avec la coalition sur la responsabilité à l'IPC. Je suis également avocat. Et j'aimerais répondre à certains des commentaires par rapport à la réglementation parallèle, par rapport

au rôle très important d'ajuster le système et d'une révision indépendant.

Lorsqu'il y a contrat entre le titulaire du nom de domaine et le bureau d'enregistrement et que ce contrat stipule qu'il y a des obligations qui relèvent aussi bien du titulaire du nom de domaine que du bureau d'enregistrement, donc au titre de ce contrat, le bureau d'enregistrement est autorisé d'un point de vue juridique à entreprendre des actions en justice pour des actions pour suspendre le nom de domaine. Donc je ne vois pas pourquoi il faudrait qu'il y ait une réglementation parallèle.

Je suis d'accord avec vous, je pense que s'il y a des cadres en place pour que les opérateurs de registre et bureaux d'enregistrement puissent suspendre un nom de domaine, de la même manière, il faudrait qu'il y ait en place un système facile pour qu'un titulaire de nom de domaine puisse aller voir son bureau d'enregistrement ou opérateur de registre pour dire : « Je pense que vous avez fait une erreur en suspendant mon nom de domaine. » Je pense qu'il est important d'avoir ce cadre en place pour lutter contre l'utilisation malveillante. C'est important effectivement. C'est une excellente mesure, un excellent pas en avant et j'aimerais dire merci, merci au nom de l'IPC.

Et enfin, par rapport aux notifiants fiables ou de confiance, c'est très important effectivement. Et j'aimerais inviter toute personne intéressée par cela à venir me voir pour me poser des questions. J'en serais ravi.

BRUCE TONKIN : Milton.

MILTON MUELLER : Milton Mueller de Georgia Tech.

J'ai vraiment envie de faire ce commentaire parce que j'ai le sentiment que le réel problème n'est pas identifié de manière adéquate. Je pense qu'il faut cadrer la question différemment.

Donc la question de départ, c'était que devons-nous faire par rapport à l'utilisation malveillante du DNS ? Donc bien sûr, la question suivante, c'est que veut-on dire par utilisation malveillante du DNS ? Et ensuite, on commence à parler du contenu, à savoir si oui ou non c'est inclus dans notre définition.

Mais je pense que c'est une mauvaise perspective parce que les personnes qui souhaitent avoir une définition plus élargie de l'utilisation malveillante du DNS prétendent que si on ne le définit pas, rien ne serait fait.

Donc en termes de tout ce qui relatif au contenu, prenons la pornographie infantile comme exemple, c'est quelque chose d'illégal dans toutes les juridictions du monde. Il n'y a pas d'exception. Il y a des mécanismes extraordinaires pour signaler, pour éliminer tout ce qui est pornographie infantile.

Même chose pour l'infraction aux marques de commerce. Nous avons des traités internationaux. Regardez un petit peu ce que faite ICE, tout

ce qui est l'application des lois relatives à l'immigration aux États-Unis, je ne sais pas pourquoi mais ils éliminent tout ce qui est relatif aux marques de commerces mal utilisées dans le monde entier.

Donc la définition de l'utilisation malveillante ne veut pas dire qu'il n'y aura pas des attaques politiques. Alors la bonne question à se poser, c'est lorsqu'il y a un problème avec le DNS, un problème immédiat, un problème urgent, lorsqu'il faut en fait contourner la diligence raisonnable, il faut qu'il y ait un processus pour les bureaux d'enregistrement et les opérateurs de registre. C'est cela la question. Quand est-ce que les bureaux d'enregistrement et opérateurs de registre sont les juges et les exécutants de la politique ?

Il y a certaines justifications dans certains domaines. Mais par rapport au contenu, je pense qu'il n'y a pas de justification.

Merci.

BRUCE TONKIN : Merci.

James.

JAMES BLADEL : James Bladel de GoDaddy. Je suis une des 11 sociétés qui a participé à la mise en place du cadre sur l'utilisation malveillante du DNS. Alors je voudrais répondre à plusieurs choses.

Vous savez, le cadre, ce n'est pas quelque chose de nouveau. En grande partie, les pratiques qui sont décrites existent depuis des années, des décennies même et elles représentent un petit peu un dévoilement de ce qui se passe déjà dans les opérateurs de registre et les bureaux d'enregistrement. Et l'idée, c'est vraiment d'éduquer le reste de la communauté, d'informer sur ce qui se passe déjà.

Mais je voulais mettre l'accent sur quelque chose que vous avez dit, Bruce. Il y a beaucoup de choses dont nous avons débattues mais je pense que tout à l'heure, vous avez mentionné quelque chose d'important.

Si l'hébergeur est l'entité la plus appropriée pour s'occuper de l'utilisation malveillante du contenu –normalement, le contenu, c'est le problème –, alors que font les bureaux d'enregistrement pour s'assurer que ces coordonnées sont mises à disposition pour les plaintes ? Parfois, c'est très facile parce qu'on est hébergeur et bureau d'enregistrement donc on peut agir dans le cadre de notre accord sur l'hébergement beaucoup plus facilement, avec beaucoup plus de souplesse qu'avec nos accords et contrats avec l'ICANN. En plus, nous savons qui est l'hébergeur, donc nous pouvons envoyer les gens au bon endroit.

Mais au-delà de cela, il ne faut pas faire l'hypothèse que les bureaux d'enregistrement ne connaissent pas les hébergeurs, qu'ils ne connaissent pas les coordonnées. Il y a toujours un transfert d'un réseau à un autre, donc ce n'est pas qu'on n'est absolument pas au courant. L'idée, c'est de faire des recherches et de trouver comment

joindre ces personnes. Et je pense qu'il y a des ressources qui existent, il y a l'ASO, il y a différents outils, même ici, qui nous permettraient de combler ces lacunes.

Mais partir du principe que nous avons des informations et que nous ne souhaitons pas les divulguer, je pense que ce n'est absolument pas une hypothèse qui tient la route. Donc je voulais la remettre en question.

BRUCE TONKIN : Je ne mentionnais pas que vous aviez les informations mais je disais simplement qu'elles n'étaient pas disponibles.

Ensuite ?

LUTZ DONNERHACKE : Lutz Donnerhacke, EURALO, At-Large.

Ce dont on parle ici, c'est de ce qui fait partie de la mission de l'ICANN. Et si j'ai bien compris, la plupart des thématiques dont on parle ici sont relatives aux contrats. Donc s'il est possible de voir avec quels contrats l'enregistrement a été effectué, il sera plus facile pour les agences d'application de la loi de savoir qui est responsable sans demander trop d'efforts de la part des bureaux d'enregistrement en termes de collecte des donnés ou d'utilisation des bases de données. On peut simplement suivre la chaîne contractuelle parce qu'en fait, le contrat doit être bien entretenu. Pas l'enregistrement ; l'enregistrement, c'est un travail de masse, automatique.

Mais je crois qu'il faut vraiment se préoccuper des contrats au niveau du détail. Les contrats entre les bureaux d'enregistrement et les opérateurs de registre, ces contrats sont toujours en vigueur et ils ont les bonnes données. Donc ma question, c'est pourquoi est-ce qu'on ne publie pas la chaîne de contrats à chaque enregistrement ? Par exemple, en utilisant un service WHOIS, un WHOIS résumé et on oublie le RGPD.

BRUCE TONKIN : Merci.

KATE PEARCE : Je parle en mon propre nom. Je suis responsable de sécurité aussi, donc je comprends bien tout ceci. Je suis également au conseil de différents groupes de confiance des consommateurs.

Alors plusieurs choses. Je vais effectivement ralentir. Il y a l'accent de Nouvelle-Zélande aussi. Donc quelques points rapidement.

Premièrement, l'âge du domaine est important. La majorité des abus que l'on voit, c'est dans des domaines enregistrés récemment. Et la plupart des problèmes se produisent dans des domaines d'un certain âge. Et en général, l'impact n'est pas le même en fait au premier jour de l'enregistrement. Il faut s'en rappeler quoi qu'on fasse à n'importe quel niveau.

Mais il y a également autre chose. On parle de règlements parallèles. C'est quelque chose qui se produit au niveau des résolveurs,

beaucoup d'ailleurs, surtout dans l'espace gouvernemental et l'espace des entreprises. Et je ne sais pas si on considère que ceci est une protection ou une censure mais c'est quelque chose qui se produit. Et c'est peut-être quelque chose qui fonctionne mais le résultat, c'est que beaucoup des organismes qui ont moins de ressources, les personnes de ce monde qui n'ont pas de ressources n'obtiennent pas le même niveau de censure et de protection. Donc pour beaucoup d'entre eux, ce sera peut-être le seul point de contact, surtout lorsque l'hébergement est difficile à cibler.

BRUCE TONKIN : Merci.

David.

DAVID CANE : Je fais partie de l'unité constitutive des entités non commerciales et je travaille également dans la sécurité.

Mon problème avec le terme utilisation malveillante du DNS, c'est qu'on se pose toujours cette question, mais qu'est-ce que c'est ? Quelle est la définition ? En gros, c'est quelque chose qui est relatif au DNS et qui est mauvais. Mais je sais que débattre de la définition finalement, c'est bien, mais on en revient toujours à la même chose. Donc il y a tout un tas de choses qui sont disparates et que l'on regroupe dans cette définition et certaines choses font partie de la mission de l'ICANN telles que la sécurité et la stabilité. Mais lorsqu'on rassemble tout ceci, finalement, on n'a pas forcément le meilleur

résultat Par exemple pour les réseaux zombie, on ne va pas éliminer tous les domaines possibles qu'un réseau zombie pourrait cibler ; il vaut mieux carrément éliminer le réseau zombie par un commandement contrôle.

Donc même si tout ceci fait partie de la mission de l'ICANN, je pense que tout rassembler ne permet pas d'arriver au meilleur résultat possible.

Il y a également un problème de contenu et le fait que le contenu soit quelque chose de parfois très illégal et d'affreux, on ne peut pas défendre ce type de contenu mais cela ne fait pas partie de la mission de l'ICANN. Maintenant, le fait que cela ne fasse pas partie de la mission de l'ICANN ne veut pas dire que l'on ne doit rien faire. Il y a des questions vitales dont il faut qu'on s'occupe. La question, c'est de savoir comment. Et je crois que les points de vue sont déjà bien établis. Il y a des efforts coordonnés pour avoir une réponse coordonnée à ces questions.

Mais n'oublions pas ce que nous avons appris de l'ICANN, à savoir que pour certaines de ces questions, il y a beaucoup de subtilités en matière de politiques, même lorsque le contenu semble vraiment monstrueux. Il y a des détails et je crois parfois que même lorsqu'on se dit : « Oui, vraiment il faut absolument réagir par rapport à ce contenu. »... Parce que c'est un problème qui demande une réponse, on doit le faire à l'extérieur de l'ICANN et voilà ce qu'on fait. Mais je pense qu'il ne faut pas oublier ce que l'on a appris à l'ICANN, à savoir que souvent, les questions de politiques sont complexes, les gens ont

des perspectives très différentes. Et peut-être faudrait-il réfléchir à utiliser les leçons de l'ICANN lorsqu'on apporte une réponse concertée à ces questions. On pourrait peut-être réfléchir à comment élaborer les politiques multipartites et comment utiliser ce modèle en dehors de l'écosystème complexe de l'ICANN.

Merci.

BRUCE TONKIN : Merci David.

Donc nous avons deux intervenants pour terminer. S'il vous plaît, rapidement.

WERNER STAUB : Je parle en mon propre nom.

On parlait des mauvais noms de domaine et de ce qu'il faut faire pour les pourchasser. Imaginons qu'on parle de contrefaçon de billets de banque. Imaginons qu'on parlait d'accréditer des imprimeurs de billets de banque contrefaits. Si on réfléchit de cette manière, j'imagine qu'on trouverait un second moyen. Cela ne veut pas dire que le premier moyen ne serait pas quelque chose auquel on réfléchirait mais on pourrait peut-être améliorer les billets. On pourrait améliorer les caractéristiques qui nous permettent de reconnaître un bon billet de banque et non pas un mauvais billet de banque. C'est cela notre industrie, c'est là-dessus qu'on devrait travailler, c'est-à-dire ajouter de la valeur.

Donc ce qui me frappe, c'est qu'on fait un peu la course vers le bas en termes de qualité d'enregistrement, tout le monde veut avoir une approche moins chère. Personne ne souhaite avoir quelque chose de cher. On se dit chez les clients : « Mais ce n'est pas forcément le cas. » Les gens veulent pouvoir montrer aux gens et aux machines que cet enregistrement est vérifié. C'est donc une opportunité pour les bureaux d'enregistrement, pour les opérateurs de registre, c'est un moyen pour les nouveaux TLD de se distinguer et je crois que ce serait une approche positive, une approche de cercle vertueux, une approche qui motiverait, qui encouragerait les bons TLD.

BRUCE TONKIN : Merci Werner.

Dernier intervenant.

ROB HALL : Je m'appelle Rob. Cela fait longtemps que je n'étais pas venu mais me revoici.

Je suis un petit peu frustré parce qu'on parle du DNS et on couvre beaucoup de choses avec cet acronyme. Mais dans l'acronyme, on parle d'un système. Mais en fait, on parle surtout de l'abus de noms de domaine et non pas de tout l'écosystème.

N'oublions pas qu'il y a d'autres systèmes à l'intérieur de tout ceci. Lorsque l'on parle d'utilisation malveillante du DNS, il faut bien définir ce dont on parle.

Question pour le panel. Certaines des utilisations malveillantes que nous avons pu observer, c'est le minage de notre système WHOIS. Donc nous allons lancer ce nouveau RDAP. Et pourquoi n'avons-nous pas parlé de l'interruption de l'utilisation malveillante de cela ? Il y a donc le problème de la protection de la vie privée de nos clients. Donc ne nous concentrons pas simplement sur l'abus des noms de domaine. Commençons à parler de tout l'écosystème et des systèmes que l'on oublie parfois parce qu'en fait, ce ne sont pas les sujets brûlants d'actualité.

BRUCE TONKIN : Alors pour terminer, j'aimerais que chacun des panelistes nous fasse un commentaire très général, un message général pour conclure.

GABRIEL ANDREWS : J'aimerais remercier les gens pour les différents commentaires. C'est vraiment très intéressant d'écouter les différents points de vue. C'est très éducatif et très utile pour l'ICANN. Donc merci.

Et pour conclure, je crois que d'une manière générale, nous sommes conscients qu'il y a le potentiel de trouver vraiment un point commun pour nous occuper des comportements néfastes. On peut parler de définition, on peut parler d'essayer de trouver les termes exacts mais je vous demande de faire attention parce que les mauvais acteurs sont créatifs. Et si on est trop prescriptifs, si on essaie d'identifier tous les moyens d'utilisation malveillante qui existent, on pourrait

potentiellement être trompés par ceux que nous n'avons pas réussi à identifier.

Puis il y a vraiment de bons conducteurs sur la route, mais il faut quand même que les règles soient suivies.

BRUCE TONKIN : Farzaneh.

FARZANEH BADII : Deux points.

Je crois que par rapport à Cloudflare qui cacherait l'hébergeur, etc., en termes d'anonymité et de personnes en mesure d'effectuer certaines actions et d'avoir des sites web sur l'internet, je ne pense pas que ce soit nécessairement des activités criminelles. Tout le monde ne veut pas nécessairement être anonyme ou agir de manière délictueuse. On ne peut pas dire tout simplement : « On va mettre toute la chaîne de contrats sur intérêt pour identifier le titulaire du nom de domaine. » Il y a des libertés qui sont en jeu.

Je crois que je n'ai pas été claire au début donc je souhaitais rectifier certaines choses que j'ai dites.

À l'ICANN, l'utilisation malveillante du DNS que vous avez mentionnée dans le cadre de travail, vous avez mentionné le cadre de travail mais nous ne sommes pas d'accord sur le reste des questions, à savoir éliminer le contenu à cause des opioïdes, etc. Donc je voulais simplement clarifier ceci.

BRIAN CIMBOLIC : Ce que je retire de tout ceci, c'est qu'il y a beaucoup de bureaux d'enregistrement et d'opérateurs de registre qui font de leur mieux, qui font certaines choses même lorsque les contrats ne leur demandent pas pour traiter ces problèmes d'utilisation malveillante du DNS.

Mais éliminer les mauvais acteurs simplement pour dire qu'on l'a fait, ce n'est pas nécessairement la bonne approche. Il faut le faire de manière réfléchie et transparente.

GRAEME BUNTON : Merci. Quatre petites choses rapidement.

On a beaucoup parlé des bureaux d'enregistrement qui permettent ces abus et je crois qu'on est toujours à la merci d'une attaque DDoS en tant que bureaux d'enregistrement. Et je crois que c'est important de le reconnaître pour bien dire les choses. Je suis d'accord avec Elliot, il y a des outils, il y a des choses dans nos contrats. Il faut être un peu plus créatifs et mieux utiliser ces outils.

En ce qui concerne ce qu'ont dit Milton et Farzi, le cadre et le fait qu'il aille au-delà de l'utilisation malveillante du DNS, je crois qu'on pourrait dire que nous agissons dans ces cas très spécifiques à cause des échecs des gouvernements et de la réglementation internationale. Et c'est là qu'on voit qu'il y a des dommages. Et à notre avis, il n'y a pas d'outils externes qui entrent en jeu au niveau international.

Et dernière chose, je suis en train de réfléchir à une métaphore comme quoi l'utilisation malveillante du DNS telle qu'elle est définie dans le document, c'est un peu la pollution, le produit dérivé de notre secteur. Donc faire comme si c'est quelque chose d'externe, je pense que ce n'est pas bon. Il faut absolument faire le nettoyage. Merci.

BRUCE TONKIN : Merci.

MASON COLE : Merci Bruce.

Je crois qu'il y a un manque de confiance sur internet étant donné cette utilisation malveillante. Et si l'ICANN ne s'occupe pas de ce manque de confiance, je crois que ceci porte atteinte à la légitimité de l'ICANN

Nous sommes d'accord par rapport à ce que font les bureaux d'enregistrement et les opérateurs de registre par rapport aux outils, par rapport aux programmes d'encouragement qui ont été suggérés. Je suis tout à fait d'accord par rapport à ce qu'a dit Elliot. Nous devons travailler la conformité de manière à ce qu'ils aient les moyens d'éliminer les mauvais acteurs. Je pense que nous avons tous appris quelque chose aujourd'hui. Nous pouvons rassembler nos efforts pour améliorer ce que fait l'ICANN.

JEFF BEDSER : J'ai beaucoup entendu parlé de ce dont on parle depuis longtemps d'ailleurs, c'est un sujet qui est à l'ordre du jour cette semaine et depuis quelques mois en particulier. Et je crois que ce dont il faut tous se rappeler, c'est que les mauvais acteurs ne voient pas les lignes entre le contenu, l'infrastructure du DNS, peu importe les limites : « Oui, cela, c'est votre problème. Cela, c'est le vôtre, etc. » Ils utilisent l'écosystème pour attaquer les gens et ils vont continuer de le faire.

Il nous faut avoir un espace dans lequel on a cette conversation. Je ne fais pas partie des politiques, donc je pense que cela fait partie du travail de l'ICANN. Et je crois que c'est dans cette communauté qu'on peut faire avancer les choses et améliorer l'écosystème pour avoir moins d'utilisations malveillantes et améliorer la réputation du modèle pour permettre la croissance capitaliste du commerce grâce à un modèle de confiance.

Si ce n'est pas nous qui le faisons, je ne sais pas qui le fera. Merci.

BRUCE TONKIN : Merci.

Alors pour résumer, on a entendu une discussion sur les définitions et Byron a bien dit que les mots sont importants. Et on a été très clairs par rapport à la ligne entre l'abus d'un point de vue technique et l'abus du point de vue du contenu. On voit qu'il y a une frontière entre les deux ; cela a été clair.

Il y a des suggestions pour améliorer plus avant. On l'a entendu. Les gens qui identifient le contenu, des gens qui sont physiquement responsables d'héberger continuent de trouver des moyens appropriés de contacter le titulaire de nom de domaine. Également une méthode pour faire recours ; cela également, c'est important. Il y a eu beaucoup de discussions aussi sur les différentes mesures d'encouragement ; cela, c'est important pour pouvoir examiner si ces mesures d'encouragement peuvent être sous forme tarifaire ou autres, faire connaître ces mesures pour qu'on sache ce qui est bon et ce qui l'est moins.

Et il y a un mélange dans cet environnement. Il est important dans cet environnement de partager les bonnes pratiques. Clairement, le contrat doit relever de la mission de l'ICANN et également aider l'équipe de conformité à être plus efficace.

Je vais remercier chacun des intervenants au panel, les personnes dans la salle aussi. Je pense que les membres du panel nous ont invités à réfléchir. Et cela a été très intéressant. Merci.

[FIN DE LA TRANSCRIPTION]