MONTREAL – Séance relative aux politiques d'At-Large : Utilisation malveillante du DNS - Inquiétudes de l'utilisateur final
Dimanche 3 novembre 2019 – 13h30 à 15h EDT
ICANN66 | Montréal, Canada

ORATRICE NON-IDENTIFIÉE : ... et veuillez s'il vous plaît vous asseoir. Nous allons commencer notre travail. La réunion est maintenant enregistrée.

JONATHAN ZUCK : Je pense qu'avec ma voix, vous m'entendez.

Bienvenue à toutes et à tous. Nous sommes très contents de cette séance qui pourrait avoir un sous-titre. Vous voyez, si vous allez voir un film, il y a un sous-titre très souvent, « On revient avec un esprit de vengeance », par exemple. Cela, c'est la 75ème édition d'ICANN au cinéma : « ICANN66, l'utilisation malveillante du DNS ». C'est un thème véritablement pour notre réunion de l'ICANN à Montréal, les abus du DNS.

Donc durant cette séance, nous allons, en tant qu'At-Large, essayer de couvrir cette thématique de l'utilisation malveillante du DNS avec des recommandations qui sont nombreuses, dont on entend beaucoup parler. Il y a des activités qui se déroulent en ce qui concerne les abus du DNS. Donc on va essayer d'avoir une discussion très ouverte sur ce

thème, comment le définir, qu'est-ce qu'on peut prendre comme mesures pour y pallier et quelle est la perspective de l'At-Large là-dessus

Pour nous aider avec ce débat, nous avons trois invités, deux sont arrivés déjà. Nous avons Drew Bagley qui a travaillé à la révision du CCT avec moi et qui a fait beaucoup de recommandations. Je pense qu'il va nous parler un petit peu de ces recommandations. Nous avons Graeme Bunton qui est à la tête de ces efforts des registres et des bureaux d'enregistrement pour véritablement définir un cadre de référence pour améliorer les réponses à l'abus du DNS. Donc je lui ai demandé de venir nous voir pour partager un petit peu ses points de vue. Et enfin nous avons Jamie Hedlund, qui s'occupe du département de conformité de l'ICANN et qui était un lobbyiste avant. Et Fadi lui a demandé de faire partie du CCTRT, de l'équipe de révision CCT avec moi, Drew et Kali également.

Plutôt que d'attendre que la bureaucratie fasse son travail, il y a des initiatives qui ont été prises par le département de conformité pour faire des réformes pour gérer certains de ces problèmes provenant des utilisations malveillantes du DNS. Donc on apprécie beaucoup sa présence et son point de vue et on va lui donner la possibilité de s'exprimer pour mettre en contexte tout cela.

Ce n'est pas une surprise, c'est quelque chose qui nous intéresse beaucoup à At-Large parce que nous représentons les intérêts des utilisateurs individuels de l'internet, les utilisateurs finaux. Et nous avons les bureaux d'enregistrement et d'un autre côté, c'est

4 milliards de personnes qui essaient d'utiliser l'internet et qui sont préoccupées par ce qui se passe, par les abus du DNS.

Donc sans plus attendre, je crois que nous allons pouvoir donner la parole à Graeme s'il est prêt. On va donner la parole à Graeme Bunton... Non, commençons plutôt avec Jamie si cela ne vous dérange pas parce que c'est quelque chose qui s'est déjà passé. Ensuite, on va donner la parole à Graeme et ensuite, on débattra. Donc merci Jamie de prendre la parole.

JAMIE HEDLUND : Merci Jonathan. Je m'appelle Jamie, j'étais lobbyiste mais je suis toujours lobbyiste. Je suis du comté de Cook dans l'Illinois bien connu pour la politique. Je suis donc habitué aux questions de politiques. Mais là, je travaille à la tête de la conformité et des protections que l'on pourrait apporter aux consommateurs par rapport à l'utilisation malveillante du DNS.

Il y a eu cette révision du CCT dont vous avez parlée, il y a eu des délibérations de l'équipe de révision et on a beaucoup parlé de données, des rapports sur les données, des abus qui existaient au niveau des données. On a été très contents de mettre en place un grand nombre de recommandations avant même qu'elles aillent pour approbation auprès du Conseil d'Administration parce que nous travaillons en pleine transparence.

Et la conformité a des rapports qui sont publiés, donc je vais vous référer à ces rapports. Et nous faisons beaucoup de travail dans ces

rapports sur les différents types de plaines, les types d'abus. On a listé ce type d'abus, les résultats qu'on peut obtenir pour lutter contre cela mais on n'a pas beaucoup de visiteurs sur ce site web. Donc on veut vraiment reporter des informations parce que c'est important d'être transparent, mais on a besoin de données que les gens ont envi de voir.

Je le répèterai aujourd'hui, s'il y a des données que vous ne voyez pas et si vous voulez qu'on fasse des rapports sur ces données, dites-le-nous. Nous pouvons continuer à préparer des rapports. Il y a un projet séparé de plateforme de données ouvertes et toutes les données de conformité seront tout à fait disponibles, donc vous pourrez personnaliser vos rapports. Mais on va continuer à créer nos propres rapports, mais on espère que vous vous intéressez à ces rapports, que vous allez les visiter et les télécharger.

JONATHAN ZUCK : Vous nous dites que ce que vous avez mis en œuvre jusqu'à présent, c'était principalement de mettre à disposition des données. Ce n'est pas les autres aspects, vous n'avez pas changé beaucoup les pratiques, donc ce n'est pas directement en rapport avec les recommandations.

JAMIE HEDLUND : Pas directement en rapport avec les recommandations. Nous avons eu un audit des registres, je pourrais vous en parlez. Il y a une relation indirecte entre ceci et le rapport du CCT, l'utilisation malveillante du

DNS. On parle beaucoup de l'utilisation malveillante comme étant un problème sérieux. Donc nous nous sommes concentrés sur ces abus du DNS étant donné que cela a un impact sur les contrats également.

JONATHAN ZUCK : J'ai oublié de me présenter. Il n'y a pas assez d'outils pour la conformité pour travailler à un niveau holistique. Vous, vous travaillez plutôt au niveau des plaintes qui vous arrivent et vous étiez dans une position difficile dans votre travail. C'est toujours le cas je crois. Vous gérez plus des plaintes et vous n'êtes pas toujours en mesure d'être proactif et de trouver un .science par exemple qui avait un taux d'enregistrement avec 50 % d'utilisation malveillante du DNS.

JAMIE HEDLUND : Nous faisons respecter les contrats tel qu'ils existent. Nous n'avons pas la capacité et le personnel suffisant pour faire plus. Notre cadre de référence, c'est la conformité contractuelle. Donc on a beaucoup de débats avec la communauté sur ces utilisations malveillantes, nous avons le groupe des parties prenantes des bureaux d'enregistrement et des registres et opérateurs de registre, nous avons des audits qui sont réalisés. Cela vient d'être le cas. C'était limité néanmoins aux contrats.

JONATHAN ZUCK : Graeme, dites-nous en plus sur ce groupe des...

GRAEME BUNTON : Je travaille pour Tucows et je suis président du groupe des parties prenantes des bureaux d'enregistrement. Je ne veux pas parler d'initiatives directement de ce groupe, mais j'aimerais d'abord vous remercier de m'avoir invité. Je n'ai jamais parlé à un panel de l'ALAC, donc c'est très agréable de le faire.

Je crois que beaucoup de bureaux d'enregistrement et de registres ont entendu parlé dans la communauté ces mois derniers de beaucoup d'abus. On en a parlé entre nous et il y a une certaine frustration : on n'a pas progressé beaucoup parce qu'on n'avait pas une définition de l'utilisation malveillante du DNS, une définition solide et claire. Il y a des gens qui veulent que la définition soit étroite et il y en a d'autres qui veulent y mettre toutes les activités désagréables de l'humanité. Donc on avait besoin d'une expertise. On était à Washington pour une réunion séparée et on s'est retrouvés et on a essayé de définir un cadre de référence pour les utilisations malveillantes du DNS et pour une définition sur laquelle on tomberait tous d'accord donc qui nous permettrait d'agir.

Nous avons publié un cadre de référence sur les utilisations malveillantes du DNS. C'est ironique en tant que bureaux d'enregistrement, je n'ai pas exactement l'adresse pour l'obtenir. En tout cas, ce que ce document effectue, et ce n'est pas un secret, nous avons des mesures pour lutter contre les abus dans notre secteur. Ces mesures pourraient être adoptées par d'autres entités également.

En ce qui concerne l'utilisation malveillante du DNS, ce que nous pensons, c'est que nous avons les pourriels, les botnet, le

hameçonnage, le spam également – cela, c'est quelque chose d'un petit peu séparé – cela représente des utilisation malveillantes du DNS et on a besoin d'actions à ce niveau.

Donc j'ai demandé à la personne qui est à la tête du département de conformité. Il y a 100 domaines par jour qui sont affectés et donc qu'on retire, donc beaucoup de travail qui est effectué pour lutter contre ces abus.

On est passé à ce que l'on doit faire à ce que l'on devrait faire. Il y a des abus au niveau du contenu qui sont très graves, donc il faut agir à ce niveau. Cela, est-ce que c'est étroit ou pas ? Pour nous, en tant qu'infrastructure de l'internet, on prend notre travail au sérieux et on veut s'assurer que toutes les couches soient bien gérées, d'une manière très réfléchie. Les actions que nous prenons au niveau du DNS, on n'a pas beaucoup de régularité, sont importantes.

Et sur la liste de ce que nous devrions faire, il y a les abus sur le trafic d'êtres humains, vente d'opioïdes et l'incitation à la violence. Cela, ce sont des abus du DNS qui demandent des actions selon nous. On pense que c'est une étape très positive qui montre bien ce qui est déjà fait aujourd'hui et qui donne, je pense, une possibilité à se retrouver de manière plus nombreuse pour prendre des mesures. Si vous n'étiez pas dans la salle lors de la réunion que nous avions auparavant, on savait que Montréal allait arriver très vite et on n'est pas encore tout à fait prêt. On veut s'assurer que d'autres personnes qui adopter ce cadre de référence, que d'autres personnes se joignent à nous pour

s'attaquer à ces problèmes. Je serais très heureux de cela. Et on a encore quelques petites modifications à effectuer.

Donc c'est à peu près tout ce que je voulais dire sur notre initiative. Donc je vous propose de prendre connaissance plus avant de ce programme.

JONATHAN ZUCK : Merci. On vous posera des questions un petit peu plus tard.

Drew, allez-y, parlez-nous un petit peu du CCT et des recommandations que l'on a effectuées.

DREW BAGLEY : Oui, merci beaucoup Jonathan de m'avoir invité. Je suis Drew Bagley. Et comme Jamie l'a dit un petit peu et je vous l'ai dit de par le passé, l'équipe de révision de CCT a travaillé sur le nouveau programme des gTLD –et cela, c'est notre travail que nous effectuons – avec une analyse proche et sérieuse des procédures de sauvegarde et protections que nous avons par rapport aux abus qui ont été identifiés par la communauté.

Donc l'équipe de révision CCT s'est basée sur les données, a analysé les mesures de protection et s'est penchée sur une étude qui montre bien des degrés d'abus qui sont définis de manière très similaire par rapport à ce qu'a dit Graeme dans son cadre de référence. C'était des problèmes de sécurité qui se posaient.

Donc une nouvelle fois, on s'est penché sur les données et l'étude a montré que malgré les mesures de protection qui existaient, il y a toujours beaucoup d'utilisation malveillante du DNS, des gTLD, des nouveaux gTLD et que ce n'est pas par hasard. Les abus sont concentrés et sont en corrélation avec des actions que nous pouvons faire pour protéger les utilisateurs.

Donc notre équipe a proposé des recommandations ayant pour but de réparer le modèle qui est brisé, qui ne fonctionne plus à l'heure actuelle, et a défini trois catégories : premièrement basée sur les données, ensuite basée sur les incitatifs et basée également pour permettre à ICANN Organisation de prendre des mesures si nécessaire. Donc on recommande que l'ICANN publie régulièrement des données concernant les abus et la sécurité sur l'internet. Là, on peut vraiment voir où on en est au niveau de la sécurité et de la stabilité de l'intérêt.

De plus, nous recommandons qu'on explore des incitatifs pour être proactifs plutôt que réactifs, donc inciter les bureaux d'enregistrement à agir d'une manière proactive pour une meilleure sécurité de l'internet, pour qu'il y ait plus d'hygiène si vous voulez au niveau de l'internet à partir des bureaux d'enregistrement. Lorsque cela persiste sur une zone pendant longtemps, il faut vraiment agir.

Et nous proposons également que les accords soient amendés pour inclure des mécanismes où les prestataires d'infrastructures ne tolèrent pas certains niveaux d'abus et prennent véritablement des actions. On n'a pas indiqué exactement à quel niveau cela devrait se faire, mais nous avons pensé au vu des données que nous recevions

qu'il serait utile d'explorer cela. Donc la clé, c'était de donner aux outils de conformité la possibilité de lutter contre les abus systématiques.

Donc on a les résultats de la révision CCT, on a les données qui existent qui sont publiées mais en termes généraux, il y a toujours des abus mais ce ne sont pas les bureaux d'enregistrement que nous voyons à l'ICANN qui facilitent cela. Justement, ce sont les personnes qui ne sont pas dans les réunions de l'ICANN, que nous ne connaissons pas. Donc il y a un besoin au niveau des politiques de faire quelque chose.

Mais le bon exemple de ces recommandations, c'était altnames. On a vu des caractéristiques où il y avait des DGA ou des enregistrements en vrac qui étaient effectués. Cela, c'est le niveau systémique d'abus où il y a 50 % parfois pour certains domaines qui représente une utilisation malveillante. Donc il y a des zones, des TLD qui sont plus particulièrement propices aux abus et qui représentent une bonne partie des acteurs néfastes de l'industrie, du secteur. Donc il faut essayer de donner les moyens de gérer ces abus.

JONATHAN ZUCK : Bien, merci.

Dans l'intérêt d'avoir d'autres avis, nous allons passer à Graeme. Vous avez dit que le document était plutôt informatif et qu'il invitait à suivre l'exemple de ce qui était fait. Or, je dirais que vous n'avez pas compris les idées que vous êtes en train de considérer ou que vous trouviez

intéressantes quelles sont les mesures que vous auriez peut-être consultées lorsqu'elles était publiées mais que vous n'avez pas reprises ?

Je suis intéressé par cela puisque ce sont des aspects liés. Donc est-ce qu'il y a des recommandations spécifiques que vous avez appréciées et d'autres suggestions à adopter dans votre industrie par rapport à l'utilisation malveillante du DNS que vous ne faites pas en ce moment ?

GRAEME BUNTON : Merci Jonathan. Je vais passer la parole à ceux qui ont travaillé sur le CCT. Je vois James, il y a Brian également et d'autres gens qui s'étaient impliqués à ce travail. Pourtant, ce document est pour moi la base, pas la limite, c'est-à-dire que les bureaux d'enregistrement et les opérateurs de registre ont toute la marge de manœuvre qu'ils puissent avoir pour faire ce qu'ils veulent faire et pour encourager les autres à suivre leur exemple. Donc j'aimerais bien que tout le monde soit au même niveau et que tout le monde prenne cela comme le minimum. Comme cela, on pourra parler de ce qui est à venir. Mais espérons qu'il y ait un ensemble de principes de base. Peut-être que James aura plus d'informations à partager avec nous.

JAMES BLADEL : Merci. Je suis James de GoDaddy. Et effectivement, nous avons participé à l'élaboration d'un cadre de référence comme point de départ où on a vu des superpositions entre nos différentes pratiques.

Drew, vous l'avez signalé, c'est le fait que l'utilisation malveillante se concentre surtout sur les bureaux d'enregistrement et les opérateurs de registre qui ne viennent pas à l'ICANN ; ce sont les gens qui ne participent pas à notre communauté.

Par rapport au CCT, il m'a semblé que le rapport était très informatif, peut-être un peu tardif, mais je ne suis pas aussi optimiste par rapport à la conclusion qu'il nous faille une nouvelle politique, surtout sachant que par exemple, les bureaux d'enregistrement en particulier comprennent que le RA a des dispositions qui demandent à ce que l'ICANN agisse contre les bureaux d'enregistrement qui s'impliquent à des activités illégales. Et je pense que cela pourra être appliqué de manière plus proactive. Je regarde James ici, je sais qu'il a d'autres limitations, je sais qu'il a d'autres responsabilités à répondre, mais il faudrait qu'il y ait une distinction un peu plus claire entre ceux qui agissent de bonne foi et les gens qui opèrent aux marges de notre système.

Et je dirais en même temps que la création d'obligations supplémentaires revient toujours au même parce qu'il nous faut un processus de PDP ouvert qui prendra des années et les mesures contre les pratiques illégales doivent être un peu moins transparentes de ce que la communauté de l'ICANN a l'habitude de voir, parce que les pratiques que nous avons, l'évasion de nos pratiques, le détournement de la protection, on n'a aucun intérêt à ce que tout le monde sache comment le faire.

Et peut-être que l'on pourrait également essayer d'impliquer davantage d'acteurs et de parties prenantes pour améliorer le système. Dans ce sens, peut-être que la non-normalisation serait positive. Donc il faudrait que les bureaux d'enregistrement et les opérateurs de registre travaillent sur l'élaboration de quelque chose de spécifique à leur modèle commercial, à leur région géographique ; cela pourrait être bien plus efficace que le modèle de l'ICANN. Encore une fois, je suis optimiste par rapport au CCT et aux recommandations mais il nous faudrait peut-être une politique.

JONATHAN ZUCK : Peut-être que vous voudrez répondre à tout cela. Alors, quel est votre avis concernant les définitions et pourquoi croyez-vous qu'il faudrait qu'il y ait de nouvelles politiques ? Qu'est-ce qu'il faudrait que l'on adresse de manière plus générale même si en général, ce sont les acteurs qui agissent en marge de l'ICANN qui sont les plus problématiques ?

DREW BAGLEY : Voilà ma précision, qui je suis.

Il n'y a rien de mutuellement exclusif par rapport aux recommandations des nouveaux régimes de la CCT et de la capacité des bureaux d'enregistrement et des opérateurs de registre de concevoir des mesures de lutte contre l'utilisation malveillante qui leur soient exclusives. En général, on évalue les moyens de l'organisation ICANN pour lutter contre l'utilisation malveillante de

manière systématique et pour les incitations à ce que les différents bureaux d'enregistrement adoptent des mesures de lutte contre ce fléau plutôt que d'être prescriptif. Donc il y a incompatibilité à ce niveau-là. Il se pourrait également que l'on travaille en parallèle pour lutter contre l'utilisation malveillante du DNS.

Or en ce moment, nous avons également identifié une lacune au niveau du concept sur le fait que notre univers et notre champ d'action est un peu trop réactif. Il faut que l'on attende à ce qu'il y ait une attaque et que la victime présente une plainte, soit dans le domaine des abus et de l'utilisation malveillante au niveau de la cybersécurité – et c'est des manquements que l'on peut identifier très rapidement – plutôt que d'avoir des politiques utilisées pour être plus proactifs.

Dans notre révision de la CCT, nous avons une définition différente de celle que vous avez, Graeme. Donc cela pourrait être problématique dans le sens où il y a des menaces cybernétiques. On voit les cyberdélits, on voit les rançon-logiciels qui sont utilisées pour le DNS et d'autres, bien sûr. Donc l'approche est un peu en retard, elle n'a pas suivi l'apparition de ces nouvelles catégories d'actions malveillantes mais en même temps, il faut que l'on adresse cette lacune et ce besoin de solution de politique nous-même. Si on a un abus systémique, ce que nous avons vu à partir des données était que les acteurs qui ne participent pas à l'ICANN sont généralement ceux qui sont responsables des cas d'utilisations malveillantes systémiques.

Mais cela ne veut pas dire qu'on n'a pas les moyens de travailler de manière proactive. On agit de manière réactive en ce moment et c'est ce que nous avons identifié. Cela ne nous permet pas de refléter le problème de pourcentage d'utilisation abusive élevé pour aller à l'encontre des responsables. Donc du point de vue de la politique, ce sont les outils qu'il faudrait que l'on développe davantage.

Puis Jonathan, vous me demandiez par rapport aux définitions. Et bien, la définition d'utilisation malveillante du DNS est bien sûr divisée en différentes catégories parce qu'il y a différents types d'utilisation malveillantes. Or, la bonne nouvelle est qu'au moins, on peut adresser le problème en différentes catégories et trouver des solutions à chacune de ces catégories pour lutter contre chacune d'entre elles alors qu'il y a quelques années, on se disait : « On ne peut pas définir tous les types d'utilisations abusives, donc on n'y peut rien. » Au moins maintenant, on peut commencer à essayer de dégager des consensus pour prendre des mesures.

Pour définir de notre part l'utilisation malveillante, on a essayé de parvenir à un consensus par rapport aux définitions de l'utilisation abusive plus orientée à la communauté. Avant le programme des nouveaux gTLD, la communauté avait travaillé pour créer des sauvegardes qui s'intègrent au programme des nouveaux gTLD. Cette inquiétude existe depuis longtemps et c'est positif de voir qu'il y a des petites mesures qui ont été prises ça et là.

JONATHAN ZUCK : Oui, pour répondre plus directement à la question, Drew, Graeme et peut-être que Jamie alors qu'il pourrait ne pas avoir un avis formé sur la question, mais croyez-vous que la définition de la révision CCT ou celle qui est compris ici dans le document – je ne connais pas le nom du groupe, donc on va parler du document Graeme – mais est-ce que vous croyez que la définition réussit à comprendre tout ce qui est inclus dans les contrats ? Autrement dit, Jamie disait que c'est les contrats qui nous restreignent. Donc est-ce que vous voyez des aspects de l'activité illégale ou de la définition de l'utilisation malveillante du DNS qui soient trop limités et qui ne comprennent pas toutes les dispositions contractuelles existantes ? C'est une question pour vous tous.

GRAEME BUNTON : Oui. Je ne dirais pas qu'il s'agit du document Graeme, c'est un document symbolique du groupe. C'est eux qui ont fait tout le travail. Moi, je n'ai que participé à la fin et j'ai mis ma signature. Mais je pense que c'est Brian qui a fait le gros du travail et qu'on a essayé de retenir tout ce qui apparaît dans le contrat.

Dans la définition, il y a des informations par rapport aux données de contact en cas d'abus, aux réponses aux plaintes d'utilisation malveillante et tout cela n'était pas défini. Au moment de recevoir des plaintes, on essaie de s'assurer que le bureau d'enregistrement fasse ce qu'il doit faire.

Dans l'accord de base des opérateurs de registre qui était conçu pour le programme des nouveaux gTLD, à partir des recommandations de Drew, il y a la spécification 11-3B qui exigeait que les opérateurs de registre créent leur propre système de suivi des menaces systémiques, d'hameçonnage, de pharming, de logiciels malveillants, de réseau zombie, et que tout cela soit informé à l'ICANN à travers des rapports comprenant les actions et les mesures prises par les bureaux d'enregistrement et les opérateurs de registre. Je pense que c'est cela le principal pour ce qu'est de l'utilisation malveillante telle qu'elle est considérée à l'heure actuelle. Et cela comprend toutes les obligations, dont la plupart des obligations qui sont incluses dans les contrats.

ORATEUR NON-IDENTIFIÉ : Je pense que c'est tout à fait compatible avec la rédaction de la spécification 11.

Et d'autre part, en ce concernant les mesures techniques et leur définition, selon l'opérateur de registre, on pourrait au-delà de la définition et interpréter différemment les spécifications. En tout cas, la définition semblerait être compatible alors que dans le contrat des bureaux d'enregistrement, en général, on a des politiques des titulaires de noms de domaine imposées par les bureaux d'enregistrement pour certaines activités qui sont en lien avec ce qui apparaît dans leur contrat d'accréditation, mais c'est un peu plus général. Je ne suis pas sûr que ce soit la même chose. Au moins, ce ne serait pas incompatible parce qu'il y a une rédaction différente entre

les deux. Mais l'identification d'une catégorie spécifique d'utilisation malveillante est quelque chose de tout à fait positif.

Donc à l'avenir, on aura la possibilité d'en discuter, de prendre des mesures là-dessus et d'évaluer les autres domaines d'utilisation malveillante pour nous assurer qu'il y ait également d'autres mesures à prendre à l'avenir et pour atténuer ces cas d'utilisation malveillante.

JONATHAN ZUCK : Dernière question du président de la séance. Une partie de la réponse du Conseil d'Administration aux recommandations de l'équipe CCT et aux données qui étaient informées était de parler du nom de domaine spécifique qui était impliqué, et puis ils disaient qu'ils étaient toujours en train de considérer la divulgation ou pas de ces données et parler du choix des utilisateurs en fonction du fournisseur utilisé. Donc Jamie, est-ce que vous avez des informations à partager par rapport aux progrès de cette ligne de considération ? Parce qu'on attend depuis un moment à avoir ces réponses.

JAMIE HEDLUND : C'est une des recommandations qui est en attente.

JONATHAN ZUCK : Oui mais on disait que cet élément de données particulier était toujours en cours de discussion. C'est pour cela que je voulais savoir si vous avez une mise à jour.

JAMIE HEDLUND : Non, on n'a pas beaucoup d'informations à partager. Je dirais que pour ce qui est de la transparence des plaintes en général, on voit une dynamique selon laquelle au moment de recevoir des plaintes, elles deviennent confidentielles lorsqu'elles sont traitées par le système et ce, pour deux raisons. D'une part, lorsqu'elles sont confidentielles et que l'on commence à signaler l'un ou l'autre, il est plus probable que le bureau d'enregistrement ou l'opérateur de registre déposant la plainte parvienne à résoudre le problème plus rapidement que s'il devait divulguer ces mesures à toutes la communauté.

Et 75 % des plaintes que nous recevons à peu près sont invalides ; elles ne sont pas fondées. Donc cela ne sert à rien de publier ce qui ne se fait pas puisqu'elles ne procèdent pas. Donc au moment de passer par l'étape d'enquête et de requête informelle et de décider de la validité ou pas d'une plainte, on a un avis de manquement qui est publié et qui comprendrait les noms de domaine en fonction du type de plaine spécifique, bien sûr. Mais nous sommes en train de considérer si on pouvait avoir ce compromis entre transparence et conformité. Donc on essaie de trouver un équilibre pour que ce soit disponible pour les utilisateurs, s'il est possible bien sûr de divulguer le nom.

JOANNA KULESZA : Vous attendez depuis un moment, monsieur. Allez-y.

MARK SEIDEN : Merci. Si j'ai bien compris, on parlait de divulgation de données illégitimes, ce qui n'est pas permis par les contrats signés avec l'ICANN. Or, l'ICANN est réticente à publier les publications illégitimes de données. Donc est-ce que vous l'avez considéré du point de vue de la transparence et est-ce que vous avez des suggestions à poser pour assurer la sécurité de la communauté de manière à ce que les autres bureaux d'enregistrement ne soient pas affectés de la même manière ?

JAMIE HEDLUND : Je ne pourrais parler des plaintes en instance mais c'est vrai qu'on a l'obligation d'informer les divulgations illégitimes de données liées au DNS qui en général passent d'abord par le GDD et qui sont reprises par l'équipe de conformité contractuelle pour application.

MARK SEIDEN : Mais ce n'est pas quelque chose dont vous informez à l'heure actuelle ?

JAMIE HEDLUND : Non, je ne suis pas sûr que l'on ait rapporté cette information auparavant.

MARK SEIDEN : Mais vous n'avez jamais informé de ces cas-là et vous avez même refusé de le faire disant que ces signalements étaient confidentiels et

qu'ils ne pouvaient pas être publiés. Et que je sache, tout dans les rapports d'infraction doit appartenir au domaine du public. Cela devrait être publié par les bureaux d'enregistrement et par l'ICANN pour protéger les titulaires de noms de domaine. Merci.

JAMIE HEDLUND : Merci.

JOANNA KULESZA : Merci. On passe au public et puis on vous donnera la parole. Mais j'ai un nombre de personnes qui sont debout. D'abord, le public ; Andrei, vous avez la parole.

ANDREI KOLESNIKOV : L'ICANN fournit le rapport DAAR aux opérateurs de registre où on comprend des mesures qualitatives et quantitatives du niveau d'utilisation malveillante des opérateurs de registre. Est-ce que vous voyez du feedback des parties contractantes, parce que ces rapports sont périodiquement disponibles à travers l'API ? Donc quelle est la réponse des opérateurs de registre à cela ? Le rapport ne fait pas partie des obligations contractuelles à ce que je sache ; c'est quelque chose de volontaire de la part de l'ICANN. Donc y a-t-il une réaction face à cela ? Est-ce que le service s'améliore à partir de la publication de ce rapport ?

JAMIE HEDLUND : Non, le DAAR n'est pas un programme de conformité. C'est une initiative de l'OCTO, responsable de la technologie de l'ICANN et il a commencé à informer de la sécurité et de la stabilité du DNS. Que je sache, il y aura une séance cette semaine et des réunions avec les parties contractantes et le bureau du responsable de la technologie de l'ICANN pour discuter du rapport DAAR et des manières de l'améliorer. En tout cas, le bureau du responsable de la technologie ne le fait pas comme obligation contractuelle. C'est quelque chose qui est fait dans le but de la recherche et d'améliorer la sécurité et la stabilité.

ANDREI KOLESNIKOV : Pas de réponse. Pas de réponse, c'est déjà une réponse.

JAMIE HEDLUND : Mais c'était quoi la question ?

ANDREI KOLESNIKOV : Une fois que le rapport a été publié, est-ce que la situation s'est améliorée ? Est-ce que les opérateurs de registre ont réagi de manière positive ?

JAMIE HEDLUND : C'est une question à poser aux opérateurs de registre.

JOANNA KULESZA : Une dernière question du public, puis nous allons faire un tour de table. Allez-y.

JEAN-PHILIPPE MÉTHOT : Je suis Jean-Philippe Méthot.

Si par exemple on avait un cas d'utilisation malveillante d'une entité puissante comme les milliardaires ou les gouvernements. Les bureaux d'enregistrement prendraient des mesures contre cette entité et cette entité à son tour prendrait des représailles. L'ICANN offrirait-elle du soutien aux bureaux d'enregistrement pour les aider à lutter contre ces représailles ?

JOANNA KULESZA : Est-ce que c'est une question adressée à un membre du panel spécifique ?

ORATEUR NON-IDENTIFIÉ : Non, à personne en particulier. Je voudrais simplement savoir quelle serait la politique de l'ICANN dans ce cas-là.

JOANNA KULESZA : Quelqu'un veut y répondre ? Graeme ?

GRAEME BUNTON : C'est un cas intéressant que vous proposez. Il faudrait qu'on en discute avec l'ICANN. Mais ma société fait l'objet d'attaques de DDoS

constamment pour différentes raisons et je dirais que c'est le cas des grands bureaux d'enregistrement et des grands opérateurs de registre. Et cela fait partie de notre activité commerciale. Si on leur demandait : « Est-ce que cela vous arrive de temps en temps ? »... Je ne pense que cela ait été abordé de la part de l'ICANN mais on en discute de la part des opérateurs.

JEAN-PHILIPPE MÉTHOT : Oui, pour que ce soit bien clair, je parlais par exemple de poursuites en justice.

JOANNA KULESZA : Oui, c'est une question intéressante. Merci monsieur. Nous en avons pris note, nous n'avons pas encore de solution mais on vous remercie de cette question intéressante.

Nous avons Seun, Tijani, Alan et Holly. Seun en premier, vous avez la parole avec une question. On a du temps, donc allez-y. Seun en premier.

SEUN OJEDEJI : Merci.

Je voulais simplement mentionner qu'autour de la table, nous avons des spécialistes et des non-spécialistes. Quelqu'un de GoDaddy est intervenu, a posé une question et lorsque l'on voit les rapports qui ont été mentionnés par Graeme, je crois que c'est important pour les

participants. Est-ce qu'il y a vraiment l'intention de résoudre le problème ou pas ? Est-ce que vous essayez, est-ce que vous voyez, vous observez actuellement un effort des bureaux d'enregistrement et des registres de lutter contre ces abus ? Parce qu'ils peuvent prendre en compte ces abus comme étant une opportunité commerciale de faire plus d'affaires. Est-ce que parfois cela ne montre pas dans leur modèle commercial justement ces abus ? Ou bien est-ce qu'ils essaient véritablement de trouver une solution ? Est-ce qu'il y a une intention forte ? Je ne parle pas de GoDaddy mais je crois que pour certains, ils ont l'intention de ne rien faire contre ces utilisations malveillantes parce qu'ils en tirent profit. Moi, je parle en tant qu'utilisateur final de l'internet.

GRAEME BUNTON : James de GoDaddy va répondre. Il faut être juste. Les abus du DNS, c'est mauvais au niveau commercial. Mais la réalité d'être un bureaux d'enregistrement, c'est qu'à chaque fois que vous avez un nom de domaine spécifique et que vous avez des problèmes, vous n'avez pas gagner beaucoup d'argent, vous allez gagner peut-être un ou deux dollars. Donc avoir une plateforme très propre, cela, c'est profitable. Il ne faut pas avoir de problèmes justement, il ne faut pas avoir d'abus, d'utilisation malveillante. Avoir des enregistrements abusifs, ce n'est pas quelque chose qui vaut la peine commercialement.

ORATEUR NON-IDENTIFIÉ : Une nouvelle fois, il y a un rapport d'une des organisations avec lesquelles je travaille qui date de plusieurs années, les coûts des abus des noms de domaine avec les bureaux d'enregistrement et les registres, avec tous les coûts associés aux utilisations malveillantes. Je crois que c'est très clair, c'est exactement ce que disait Graeme.

JAMES BLADEL : Donc pour répondre à cette question, je ne sais pas si vous avez eu l'impression lorsque je suis intervenu en premier que j'ai dit cela. Nous avons entre 20 et 40 personnes qui travaillent à plein temps pour lutter justement avec des outils contre ces abus. Nous avons véritablement une lutte très forte qui est effectuée contre ces problèmes de malveillance. Donc vraiment, on ne gagne absolument rien. C'est un coût, c'est une nécessité de lutter contre ces abus et cela nous coûte cher pour avoir une plateforme de haut niveau.

Si vous avez entendu quelque chose de ma part, c'est l'efficacité de l'ICANN pour lutter contre ces problèmes, telle était la question. Je crois qu'avec le cadre de référence dont parlait Graeme et que nous essayons de développer, c'est qu'il y a des domaines où l'ICANN peut être efficace pour la sécurité et la stabilité du DNS et pour les contenus tout à fait néfastes et malveillants par exemple. Mais je crois que nous devons observer d'autres domaines également, d'autres secteurs. Mais croyez-moi, ce n'est absolument pas profitable de se baser sur les abus. C'est un coût pour nous de lutter contre les abus pour avoir une plateforme de haut niveau et une bonne réputation dans ce secteur. J'espère avoir répondu à vos perceptions. Merci.

JOANNA KULESZA : Merci beaucoup, c'est un très bon débat.

Tijani, vous avez la parole.

TIJANI BEN JEMAA : Merci beaucoup. Merci de ces clarifications et merci Graeme d'avoir introduit ce document. Je l'ai lu avec attention et je suis d'accord avec votre définition. Néanmoins, étant donné que nous sommes à l'ICANN, nous sommes ALAC ici, en tant que parties prenantes, nous travaillons dans le cadre des statuts de l'ICANN qui clairement nous disent que le contenu n'est pas inclus dans notre mission.

Donc lorsque vous avez parlé d'un contenu néfaste et malveillant, même si on est tous d'accord là-dessus, cela ne peut pas être différent d'un pays à un autre. Donc je crois qu'en tant que registre ou bureau d'enregistrement, vous pouvez peut-être faire quelque chose au niveau du contenu, mais cela va être dans le cadre de vos lois nationales qui s'appliquent. L'ICANN ne peut pas faire cela parce que nous n'avons pas le droit juridiquement de juger ou d'évaluer un contenu.

GRAEME BUNTON : Merci Tijani, c'est un point intéressant. Je suis d'accord avec les statuts mais cela n'a jamais empêché qui que ce soit de parler de problèmes de contenu dans l'histoire de l'ICANN.

Mais vraiment, pour vous répondre, ce n'est pas une initiative formelle d'une partie prenante, c'est une action volontaire de quelques parties contractantes parce qu'en effet, cela dépasse les abus du DNS. Nous sommes une entreprise privée donc cela, on peut le faire. Nous avons choisi d'adopter cela et nous l'avons effectué. Mais ce document n'est pas une politique de l'ICANN, je suis d'accord. On n'a pas fait ce processus de développement de politique de l'ICANN. C'est pour cela qu'on a été très rapide aussi.

JOANNA KULESZA : Merci.

Je vais terminer le tour de la table. Nous avons un autre participant, Alan, Holly et ensuite, on passe le micro dans la salle.

ALAN GREENBERG : Merci beaucoup.

Graeme a parlé d'un projet tout à fait encourageant. Drew a fait le commentaire : « Une politique est nécessaire pour que l'ICANN puisse faire respecter certains points. » ; je ne suis pas d'accord avec cela.

Il y a deux manières de donner des outils à l'ICANN. Cela pourrait être par l'intermédiaire d'un développement de politique ou bien cela peut être par des négociations contractuelles. Donc ce que je vois manquant ici, c'est une véritable coopération entre tous les acteurs. Donc c'est très encourageant, ce que vous avez fait, Graeme. Vous

avez communiqué, vous avez quelque chose de viable, de pratique en tant que document.

Mais ce que j'entends également autour de la table, c'est que c'est un projet du bureau du directeur de la technologie, pas de la conformité. Donc moi, je crois que c'est bien d'entendre les registres. La conformité OCTO est toutes ces parties qui s'engagent se mettent ensemble pour, en groupe, dire ce qu'ils font pour régler ce problème des abus du DNS et ne pas avoir simplement un tout petit groupe qui ne communique pas avec d'autres.

Donc je crois qu'ensemble, nous avons les outils nécessaires pour mettre en place des mécanismes pour les bons bureaux d'enregistrement et registres pour avoir un outil de conformité de l'ICANN qui pourrait être respecté. Je crois qu'il faut bâtir ces outils pour que les personnes qui ne sont pas des personnes honorables puissent être attaquées par la conformité. Et l'OCTO peut développer des outils, l'OCTO devrait être présent également, ce bureau du directeur de la technologie. Moi, je crois que cela fonctionnerait mieux de cette manière plutôt que d'avoir un petit travail isolé d'un côté et d'un autre.

ORATEUR NON-IDENTIFIÉ : Pour clarifier les choses, lorsque j'ai dit que le DAAR était un projet OCTCO, clairement, cela ne provient pas du contrat. Mais récemment, nous avons eu un audit et en effet, la conformité récemment s'est

coordonnée étroitement avec OCTO pour les données utilisées pour l'audit.

ALAN GREENBERG : Donc je crois qu'on a besoin d'encore plus de collaboration entre toutes les entités.

DREW BAGLEY : Je voudrais clarifier également que la manière dont l'équipe de révision CCT a réfléchi, c'est par l'intermédiaire du contrat. En effet, inscrire cela dans le contrat pour que les services de conformité puissent faire respecter cela.

ALAN GREENBERG : Je sais que vous connaissez la réponse, mais je crois que ce n'est pas le développement de politiques uniquement qui va nous permettre de résoudre ces problèmes.

JOANNA KULESZA : Holly, vous aviez un commentaire ?

HOLLY RAICHE : Oui. Récemment, nous avons eu non pas un webinaire mais une téléconférence avec Dave Piscitello que vous devez connaître ou avec connu qui a fait beaucoup de travail dans ce domaine. Et les commentaires qu'il a effectués, c'est qu'on pourrait faire une grande

différence si ces enregistrements en vrac ne sont pas autorisés. C'est là où beaucoup de problèmes surviennent.

GRAEME BUNTON : Je ne crois pas qu'on ait beaucoup de enregistrements en vrac et je ne crois pas que cela soit très utile. Il y a beaucoup de raisons pour des enregistrements en vrac. Je crois que Telco en Amérique du Sud a acheté un domaine pour chaque tour je crois, et c'était des algorithmes. Cela, c'est un autre problème. Et cela, c'est un problème pour l'infrastructure.

DREW BAGLEY : Je suis au courant du travail de Dave et ce qui est intéressant dans sa proposition et dans le rapport, c'est qu'il a suggéré des changements pour les utilisations illégitimes que nous observons, ce n'est pas universel mais que nous voyons de la part des victimes. Oui, il y a ces enregistrements groupés, il y a des campagnes d'effectuées. Il y a eu là à ce moment-là une violation des données. Donc en général, Dave avec une dichotomie entre différentes catégories d'enregistrements. Il parle d'enregistrements non-groupés, en vrac, il parlait de processus pour ces enregistrements un peu par défaut. Il y a le problème des algorithmes en effet qui se pose. Cela, c'est cohérent par rapport aux attributs de la révision CCT. C'est au niveau systémique que nous voyons ces abus, c'est un problème de DNS. Il y a des opérateurs qui ont des pourcentages très élevés d'abus et il y a des acteurs qui, au niveau interne, ont une conformité très forte qui leur permet de faire

régner l'ordre de leur travail et dans leur entreprise. Mais il y a beaucoup de cas de figure en ce qui concerne ces abus.

JOANNA KULESZA : Très bien. Nous avons encore un peu de temps.

John, vous avez une question ?

JOHN LAPRISE : Oui, John Laprise de l'ALAC.

Je suis content que l'on débatte de cela mais j'encouragerais tout le monde à avancer encore parce que cela, c'est une possibilité de ne pas toujours se baser sur le juridique. On a déjà travaillé beaucoup sur le RGPD. Je crois qu'il faut vraiment que l'on fasse quelque chose, qu'on ne soit pas en retard. On était en retard avec le RGPD, on ne veut pas être en retard sur l'utilisation malveillante sinon d'ici quelques années, il y aura des textes de loi contre justement ces abus du DNS et des pays limiteront par exemple ces enregistrements groupés. Donc je crois qu'il faut que l'ICANN continue à travailler à cela.

JOANNA KULESZA : Je crois que vous avez raison, je suis d'accord. Nous avons besoin d'un cadre de référence plus solide.

Monsieur, vous avez la parole.

SIVASUBRAMANIAN MUTHUSAMY : Je suis participant à cette réunion.

Je crois que les autres abus du DNS, ce sont principalement pour les noms de domaine. Est-ce que cela dépasse les noms de domaine ? Est-ce que les abus proviennent d'en dehors parfois du DNS ou est-ce qu'ils sont uniquement limités au DNS ? Est-ce que c'est vraiment concentré sur les noms ou pas ? Les abus pour les noms de domaine légitimes, il faut également s'en préoccuper. En ce qui concerne le DNS, est-ce qu'il y a des abus avec d'autres DNS illégitimes, alternatifs dirons-nous ? Est-ce que l'ICANN se penche sur les autres systèmes de DNS ?

GRAEME BUNTON : Je vais essayer de répondre à votre question. En tant que bureau d'enregistrement qui vend des noms de domaine dans le cadre du DNS, je ne peux rien faire si on n'utilise pas le DNS. Et je dirais que les DNS alternatifs, ce n'est vraiment pas dans le cadre de l'ICANN, ce n'est pas régulé et il n'y a rien que l'on puisse faire à ce niveau.

DREW BAGLEY : Oui, c'est exact. Je parle de la révision du CCT, on a parlé de communication, de coordination du programme d'une éventuelle nouvelle série de nouveaux gTLD. On a parlé de ccTLD, on a parlé de ces contextes. Et comme l'a dit Graeme, on parle de ce qui rentre dans le cadre de la mission de l'ICANN. Au niveau de la sécurité, il y a le dark

web où il y a d'autres DNS, où il y a parfois en effet un aspect criminel. Cela, c'est un autre débat, c'est très difficile à gérer et à régler. Il y a une distinction entre ce que l'on peut régler à l'ICANN avec les prestataires de service internet, avec les identifiants uniques. C'est une envergure totalement différente. Et en effet, c'est un problème de cybersécurité, je suis d'accord. C'est un problème juridique également et cela dépend des entités juridiques.

JOANNA KULESZA : Pour clarification, qu'est-ce que c'est que ces DNS alternatifs dont vous nous parlez ? Quelle est cette notion ?

DREW BAGLEY : Ce qu'on appelle le dark web, c'est un réseau illégitime qui ne se base pas sur le DNS, qui n'utilise pas le même système d'identifiants. Il y a Tor par exemple qui est un exemple. On peut parler de DNS alternatif lorsqu'on n'utilise pas le DNS tel qu'on le connaît et lorsque l'on branche les ordinateurs de manière différente.

Là, vous avez un marché noir qui existe sur le dark web. Et ce que nous voyons, c'est un problème de violations de données, de protection de la propriété intellectuelle. Cela n'a pas un impact direct sur le DNS mais ce sont des outils de cybercriminalité. C'est un problème des forces de l'ordre. Les forces de l'ordre nous disent que ces DNS alternatifs sont là où se joue la criminalité principalement sur l'internet.

JOANNA KULESZA : Merci Drew, c'était très utile.

Maintenant, je recède la parole à Jonathan, le modérateur.

JONATHAN ZUCK : Merci Joanna. Je voulais intervenir en fait, ce n'est pas pour reprendre la parole.

Je voulais un peu participer à la conversation qui est venue et allée en raison de la structure. Il y avait quelqu'un de GoDaddy qui a pris la parole tout à l'heure. Il s'appelait comment ? James, oui, désolé. C'est horrible, on oublie tout ici.

INTERPRÈTE : On ne comprend pas ce qui est dit.

JONATHAN ZUCK : James, lorsque vous avez présenté vos objections aux recommandations de l'équipe CCT, vous avez soulevé deux aspects qui m'ont semblés intéressants. Vous souteniez l'adoption potentielle d'outils supplémentaires pour le département de conformité contractuelle pour soutenir sa mission existante. Et puis vous avez abordé le fait que les politiques étaient trop prescriptives, qu'elles avaient été adoptées il y a très longtemps.

Drew a dit que les recommandations de l'équipe CCT n'étaient en fait pas restrictives, qu'elles visaient d'une part à générer des incitations pour que les organes de réglementation prennent des mesures ; certaines le font, certaines ne le font pas. Puis il y avait d'autres recommandations pour fournir des outils supplémentaires au service de conformité contractuelle.

Ces deux déclarations que vous avez faites semblent être incompatibles entre elles. J'ai peut-être mal résumé ce que vous avez dit. J'espère que ce n'est pas le cas, mais ce que nous avons vu dans l'étude de CCT était qu'il y avait des domaines qui avaient 50 % d'utilisation malveillante. C'est-à-dire que le statu quo, quoi s'il en soit, ne suffit pas.

Donc le fait qu'ils soient volontaires de se conformer veut dire qu'il y a des gens qui ne font pas leur travail ou qu'alors ils leur manquent des outils pour affronter le problème. Du fait qu'il existe déjà, on voit que le statu quo actuel ne suffit pas.

JAMES BLADEL : Permettez-moi de répondre s'il vous plaît.

JONATHAN ZUCK : Ancien responsable de la GNSO.

JAMES BLADEL : Je suis à ma deuxième ou troisième réunion de l'ICANN peut-être.

JONATHAN ZUCK : Oui mais je pensais que vous étiez bien plus petit.

JAMES BLADEL : Oui, J'ai beaucoup grandi depuis que j'ai rejoint l'ICANN.

Permettez-moi de revenir sur ce que je disais tout à l'heure. Je ne disais pas que j'étais pour l'existence de nouveaux outils pour le service de conformité. Plutôt, je disais qu'il faudrait qu'on utilise pleinement les outils existants d'après les contrats actuels. L'ICANN peut prendre des mesures contre les bureaux d'enregistrement accrédités après les contrats qu'ils ont. C'est ce qui est dit dans les contrats actuels.

Donc je ne veux pas revenir sur pourquoi cela ne se fait pas s'ils ne peuvent pas le faire, s'ils ne veulent pas le faire. Mais il n'est pas clair comment la communauté pourrait soutenir une interprétation plus directe de tout cela alors qu'il y aurait des cas d'utilisation malveillante plus concentrés sur une des deux parties prenantes. On s'est dit qu'il faudrait évaluer les dispositions.

Nous, nous avons adopté ces dispositions sachant que notre contrat serait à risque si on agissait de mauvaise foi. Donc en fait il faudrait savoir ce que la communauté prévoit comme interprétation de ces dispositions, à quoi elle s'attend.

Vous avez dit que mes deux déclarations étaient incompatibles. Oui, elles pourraient l'être mais ce n'était pas le message que je voulais

transmettre. On ne croit pas que les outils supplémentaires soient nécessaires à moins que si l'on utilise les outils existants.

JONATHAN ZUCK : Non, désolé. Si vous sentez que le service de conformité a les outils nécessaires parce qu'il y a une disposition qui leur permet de prendre les mesures mais qui n'ont pas les mécanismes pour le faire, je ne sais pas comment répondre. Lorsque vous considérez le fait que tout cela existe et que cela n'a pas été abordé depuis très longtemps, il semblerait que cela suffit. Ce n'est pas pour vous dire que le service de conformité ne se conforme pas aux normes. Mais si c'est cela la question, il faut qu'on aborde ce problème-là.

Or, je pense que vous êtes en train de dire : « Nous sommes les héros, voilà ce que nous faisons, nous faisons ce qu'il faut faire. Il y a un régime d'autoréglementation et il faudrait continuer comme cela plutôt que d'avoir tout un processus d'élaboration de politiques pour avoir des réglementations externes. » Cela pourrait être raisonnable, oui, mais quelque part, la conversation omet de dire qu'il existe des bureaux d'enregistrement et des opérateurs de registre qui ne se bornent pas aux normes de notre système. Donc voilà ce que je voudrais que l'on aborde, que l'on discute de manière poussée.

Et je reviendrai sur ce qu'Alan disait, c'est très bien ce que vous faites, j'apprécie vos investissements et le fait que vos clients et vos utilisateurs puissent en bénéficier. Mais qu'en est-il du reste du marché ? Qu'est-ce qui vous inquiète ? Ne vous inquiétez-vous pas des

conséquences ? Comment aborder le problème auprès de personnes qui n'agissent pas de bonne foi ?

JAMES BLADEL : Il faudrait que l'on s'implique et que l'on aide Jamie et son organisation. Ce n'est pas nécessairement un problème. Ce l'était dans le passé mais cela a beaucoup changé grâce à des outils comme le rapport DAAR. Désormais, nous avons beaucoup d'outils à notre disposition. Lui, il travaille suivant différentes pressions dont on n'est pas toujours conscients à l'ICANN parce qu'on vient de l'extérieur, on ne voit pas tout ce qu'il y a derrière leur travail. Il faut qu'on les encourage à analyser les contrats en vigueur pour mettre en œuvre de manière plus proactive ces mesures.

Parce qu'il me semble que les outils existent, ils sont là. Jamie, est-ce que vous trouvez que les outils sont insuffisants ou inappropriés ? Vous pourriez prendre des mesures plus restrictives si vous vouliez et si vous aviez le soutien de la communauté pour ce faire.

JONATHAN ZUCK : Jamie, Drew, vous voulez répondre ?

JAMIE HEDLUND : Oui, on a de très bons outils, des outils qui ont fait un peu plus de sensibilisation. Le DAAR est efficace dans l'espace des opérateurs de registre. Mais il y a beaucoup de travail en cours pour résoudre cela également.

Vous savez, à partir de l'audit des opérateurs de registre, l'utilisation malveillante est un problème dont souffrent tous les opérateurs de registre et ils font énormément d'efforts pour atténuer les menaces à la cybersécurité. Nous continuons de travailler avec les opérateurs de registre, avec les bureaux d'enregistrement et avec les forces de l'ordre pour trouver des moyens plus créatifs de mettre à profit les outils que nous avons déjà. J'espère pourvoir suivre les discussions de la communauté pour pouvoir voir quels en sont les débouchés. Il pourrait y avoir des changements, soit à travers la politique, soit à travers des négociations contractuelles. Et le service de conformité contractuelle les mettra en œuvre si c'est le cas.

DREW BAGLEY : Au sein de l'équipe de révision de la CCT, nous avons vu qu'il y avait des dispositions existantes qui n'étaient pas suffisantes ou appropriées pour affronter le problème soulevé par les données. Mais la communauté a innové essayant de trouver de bonnes choses à faire par l'équipe et par la communauté. Donc on a essayé de trouver des moyens d'incitations économiques par exemple réduisant les frais des opérateurs de registre qui adoptaient certaines mesures anti-utilisation malveillante qui soit plus proactives. Mais l'encouragement du proactif plutôt que du réactif n'était pas tellement reflété dans les contrats actuels. On les a encouragés à ajouter ces dispositions dans les contrats actuels mais c'était en conflit avec les données existantes.

Pour ce qu'est de l'utilisation malveillante systémique, par exemple, on avait un opérateur de registre qui voyait sont nom associé à je ne

sais plus quel était le nom exact, mais la moitié de leurs enregistrements, même plus, faisaient une utilisation malveillante du DNS de cet opérateur de registre. Puisque le modèle était réactif, il fallait qu'à chaque fois l'on présente de nouvelles plaintes pour que des mesures soient prises. Et cela a pris presqu'un an pour le service de conformité de l'ICANN de prendre des mesures. Finalement, ils ont eu des problèmes parce qu'ils n'avaient pas payé leurs frais, ce n'était pas parce qu'ils facilitaient l'utilisation malveillante du DNS.

Et je pense que cela montre clairement le problème. Vous parliez de disposition d'illégalité, d'illégitimité, mais il manquerait davantage de fondements pour s'occuper de tout cela.

De toute façon, vous parliez des recommandations de l'équipe CCT et je dirais que ces recommandations n'étaient pas trop prescriptives dans le sens où il y a eu des choses qui ont été faites et de manière similaire, on n'avait même pas un seuil qui soit clairement établi. Et même si on l'avait eu, sans les données, l'entité qui participerait aux réunions de l'ICANN n'aurait rien à craindre dans ce sens parce qu'elle aurait été conforme à ces normes. Si toutes les recommandations étaient adoptées, il ne faudrait pas que l'on trouve des incitations en raison de leur bonne conduite, de leur bon comportement. Mais le système tel qu'il est en général génère davantage d'utilisations malveillantes.

JONATHAN ZUCK : Greg Shatan.

GREG SHATAN : Je suis d'accord avec ceux qui ont dit qu'il s'agissait d'un bon point de départ. Et l'article identifie ce premier pas en avant, bien qu'il y ait eu un peu plus de travail auparavant. Mais oui, en tout cas, c'est un bon point de départ de là où en est en ce moment.

De toute façon, je dirai et j'avoue que je sens qu'on n'a pas fait suffisamment parce qu'il y a des types très techniques d'utilisation malveillante du DNS et non pas des noms de domaine en eux-mêmes, ce qui inquiéterait davantage les utilisateurs finaux et qui pourrait connecter avec tout ce qui pourrait être fait autrement.

Par exemple, il y a des noms de domaine qui pourraient utiliser des marques commerciales de manière illégitime et qui pourraient donner aux consommateurs l'impression de, sans être nécessaire du spam, diffuser un logiciel malveillant ou autrement utiliser un nom de domaine pour obtenir la confiance du consommateur et puis par la suite générer des problèmes comme le hameçonnage ou autres types d'utilisations malveillantes qui font partie des discussions de l'ICANN mais qui ne sont pas nécessairement comprises dans la liste. Donc oui, il y avait des menaces de violence par exemple et d'autres cas qui étaient très inquiétants, mais ce qui m'inquiète est le résultat au-delà de l'enclos. Voilà ce que je voulais savoir, quel en est votre avis.

GRAEME BUNTON : Depuis la publication de ce cadre de référence, on m'a dit qu'on avait trop dit et d'autres m'avaient dit qu'il n'y avait pas suffisamment

d'information, et personne n'était content. Je dirais donc qu'on a fait un bon travail : si personne n'est bien content, c'est toujours le cas à l'ICANN, c'est qu'on fait un bon travail.

Et si j'ai bien compris, Greg, on en a discuté auparavant, donc on a cet ensemble limité de problèmes qui sont au niveau du contenu et non pas de l'utilisation malveillante du DNS en soi-même. Surtout, ce sont des problèmes liés à la propriété intellectuelle. Et il me semble qu'il ne faut pas qu'on s'en occupe au niveau du DNS, mais cela ne veut pas dire que les problèmes n'existent pas.

Cependant, si vous avez une plainte d'utilisation malveillante du DNS à nous présenter qui soit liée à un problème de propriété intellectuelle et à un cas d'utilisation malveillante qui soit clairement compréhensible, on pourrait prendre des mesures qui soient positives pour tout le monde.

Autrement, il est clair que la propriété intellectuelle n'entre pas dans notre cadre de référence.

JOANNA KULESZA : Une dernière question de la dame qui est devant le micro, puis Tijani et Olivier. Voilà la liste d'intervenants. Il nous reste 12 minutes. Allez-y.

KATE PEARCE : Je suis Kate Pearce de la Nouvelle-Zélande, responsable de la sécurité dans une grande société, mais je parle en mon propre nom.

Je vous encouragerais, si vous souhaitez entrer dans le domaine de la réglementation, de ne faire que mesurer le temps de réponse. Dans la cybersécurité, moi, cela ne m'intéresse pas si cela vous prend du temps, cinq ans, pour résoudre quelque chose. Mais il y a des choses à faire dans les quelques minutes. Il y a des mesures qui doivent être prises tout de suite. Donc suivant la jurisprudence, des fois, vous n'aurez pas de réponse.

Il y a des centaines de millions de personnes à risque si vous prenez trop de temps. Donc oui, il faut trouver un équilibre, il faut trouver un processus qui soit utile. Mais pour ce qui est des noms de domaine par exemple, si ce sont des contenus qui ne sont en ligne que pendant quelques minutes, le risque sera bien moins élevé que si le contenu est publié pendant quelques années. On parle d'audits, d'applications ; tout cela se fait déjà au-delà de l'ICANN. On a toute une industrie de la cybersécurité qui a cet ADN. Il y a des pays qui ont des pare-feu pour les DNS pour essayer de réduire les faiblesses de l'espace. Mais le marché ne pas résoudre certaines faiblesses. Il y a une faiblesse qui reste quand les utilisateurs finaux n'ont pas accès à ce recours. Et on ne peut pas l'oublier. Pour beaucoup d'utilisateurs individuels de l'internet, la réglementation, c'est tout ce qui les protège. Ne l'oubliez pas.

JOANNA KULESZA : Très bien, merci. Est-ce qu'il y a du feedback des membres du panel ? Non ? Merci de ce commentaire qui était très intéressant.

Tijani ?

TIJANI BEN JEMAA : Non, je cède ma place.

JOANNA KULESZA : Oui, Olivier ?

OLIVIER CRÉPIN-LEBLOND : Merci.

Je vais reprendre ce que disait mon ami et collègue Alan Greenberg tout à l'heure par rapport au fait qu'il semblerait effectivement qu'on est en ligne et qu'on a une collaboration inédite pour ce qu'est de la coopération entre bureaux d'enregistrement et opérateurs de registre, utilisateurs finaux et autres à l'ICANN. Or, pour ce qui est du service de conformité contractuelle de l'ICANN, je dirais que ce qui a été présenté aujourd'hui reflète clairement ce qu'ils disaient il y a quelques années. J'ai bien lu leur rapport et il est vrai que 99 % des mesures prises portent sur le non-paiement des frais.

Il y a quelques années, c'était exactement la même chose. Donc on dirait qu'on a fait des progrès et je félicite les parties contractantes, les bureaux d'enregistrement et les opérateurs de registre qui ont signé la lettre, le document dont on parlait tout à l'heure. Mais le service de conformité contractuelle, il semblerait, n'a pas avancé. Soit ils n'ont pas les bons outils pour faire autre chose que demander à ce que les

frais soient payés, donc Al Capone pourrait tuer, vendre, faire tout ce qu'il veut et puis être emprisonné en raison d'un manque de paiement de taxe, comme c'était le cas aux États-Unis, mais il y a des activités qui pourraient être traitées d'autres manières que tout simplement en raison des frais ou des taxes parce que la loi a évolué et on a maintenant des lois pour lutter contre les autres délits d'Al Capone. Donc l'ICANN devrait également évoluer et évaluer quels sont les outils et dispositions plutôt que d'utiliser les outils plus faciles à appliquer, à utiliser qu'est de prendre des mesures que lorsque quelqu'un n'a pas payé. Alors ce moment-là, de dire : « Ah ! On a eu beaucoup de personnes qui n'ont pas payé leurs frais cette année, il faut les suspendre. » Ce n'est pas cela. Il faut lutter contre les problèmes plus graves et cela m'inquiète de ne pas voir de progrès à ce niveau-là. Et j'espère que vous allez pouvoir le faire. Jamie, je sais que vous avez hérité d'une situation au service de conformité, mais cela dure depuis un bon moment et en ce moment, je ne vois pas qu'il y ait une volonté de changer la donne.

JAMES BLADEL : Moi, je voulais rebondir sur ce que vous dites et féliciter l'équipe de Jamie qui essaye de trouver une manière d'identifier les coupables. Moi aussi, j'allais reprendre l'exemple d'Al Capone. Si le seul moyen qu'il y a pour les emprisonner, c'est les taxes, tant pis mais au moins, ils arrivent à identifier quel est le coupable, ce qui n'était pas possible auparavant. Je ne vois que ce soit un problème. Ce que vous dites, ce n'est pas un problème, c'est une fonctionnalité. Cela montre que le

service de conformité contractuelle poursuit ceux qui ne se conforment pas ou qui agissent d'une mauvaise manière. Si quelqu'un ne répond pas à vos appels ou qu'ils envoient uniquement du pourriel ou qui sont coupables d'hameçonnage, on doit trouver un moyen pour les punir.

JAMIE HEDLUND : Merci Olivier, je prends note de votre commentaire. On est toujours ouvert à des suggestions pour améliorer notre travail. Il me semble que vous avez une vision un peu biaisée de ce que nous faisons parce que vous ne voyez que ce qui est publié et c'est ce qui correspond à des infractions. Et beaucoup de ce qui correspond à des infractions, c'est des manquements de paiement. Donc on a des programmes avec certains bureaux d'enregistrement également où nous traitons entre 40 000 et 50 000 plaintes par an, dont un petit pourcentage correspond à des problèmes de paiement. Est-ce qu'on pourrait faire un meilleur travail ? Oui, sans doute. On évaluera vos suggestions, on verra comment mieux faire. Merci.

JOANNA KULESZA : Merci.

On a Alan, puis Jonathan qui résumera.

ALAN GREENBERG : Je voudrais rebondir sur ces derniers commentaires. Je crois que si vous avez des problèmes de paiement, c'est très clair comme

situation. Mais on doit être en mesure de s'attaquer à ceux qui sont peut-être assez stupides pour payer leurs factures mais qui ne sont pas au niveau.

JONATHAN ZUCK : Est-ce que je peux résumer vraiment ce qui a été dit ? C'est un problème assez émotionnel parfois et c'est également des entreprises qui sont en jeu, donc il faut trouver le bon équilibre.

Je crois qu'il y a un consensus à At-Large : nous voulons prendre cela très au sérieux et nous engager de manière tout à fait spécifique. Vous allez continuer à entendre parler de nous au niveau du Conseil d'Administration et du département de conformité de l'ICANN pour trouver les meilleures manières de limiter ces problèmes. C'est important, nous devons en parler. C'est identifier les problèmes et surtout, identifier des solutions parce que comme je l'ai dit dès le départ, notre responsabilité c'est de représenter plus de 4 milliards d'utilisateurs finaux de l'internet qui connaissent très mal le système d'enregistrements ou qui ne connaissent pas l'ICANN et qui essaient de faire une réservation pour aller dîner, tout simplement. Que peut faire l'ICANN dans le cadre de sa mission ? C'est complexe.

J'aimerais qu'on remercie nos intervenants qui ont répondu à des questions parfois difficiles. Drew Bagley, Graeme Bunton, Jamie et James de GoDaddy et le public, merci beaucoup Andrei. Merci beaucoup à toutes et à tous.

Je crois que nous avons une pause.

[FIN DE LA TRANSCRIPTION]