ABOU DABI – Séance intercommunautaire : signalement des abus du DNS à des fins d'élaboration de politiques et d'atténuation desdits abus
Lundi 30 octobre 2017 – 13h30 à 15h00 GST
ICANN60 | Abou Dabi, Émirats arabes unis

IRANGA KAHANGAMA : Bonjour. Est-ce que vous pourriez prendre place, s'il vous plaît ? On va commencer d'ici une petite seconde.

Merci d'être venus à cette réunion sur la notification de l'utilisation malveillante du DNS – atténuation. Je suis l'un des coorganisateurs de cette réunion au nom du Bureau de recherche des États-Unis, du FBI.

CATHRIN BAUER-BULST : Bonjour. Cathrin Bauer-Bulst au nom du Groupe de travail sur la sécurité publique du GAC.

IRANGA KAHANGAMA : Merci Cathrin. J'aimerais vous donner un bref aperçu de l'histoire et de la logique de cette réunion, de ses problèmes. Et Cathrin nous donnera plus de détails d'ordre logistique sur cette question.

Donc du point de vue du Groupe de travail sur la sécurité publique, voilà le travail qu'on a essayé de mettre en œuvre pour la communauté ICANN au niveau de l'atténuation de l'utilisation malveillante du DNS après avoir posé plusieurs questions par rapport à cette thématique, à l'issue de différentes conversations qu'on a eues, qu'on a eu l'occasion d'avoir.

Lors de nos réunions, c'est quelque chose qui nous a beaucoup intéressés. Il s'est avéré qu'il y avait un net intérêt de la communauté par rapport à cette question et qu'il nous fallait donc aborder cette question avec sérieux. Pour vous donner quelques idées, on a eu trois appels à volontaires de la part des différentes parties prenantes de la communauté que vous voyez assises ici à cette table. Et ensemble, on a défini la manière de penser.

Ce groupe de travail a réuni les principes autour de l'atténuation de l'utilisation malveillante du DNS. Et après certaines propositions, il est apparu clairement qu'il y avait différents points de vue sur cette question. Et donc le résultat naturel de cela a été que l'on a débattu de cette question avec la communauté de manière ouverte, comme on le fait aujourd'hui.

Donc on a repris toutes ces discussions et toutes les questions liées à l'atténuation de l'utilisation malveillante du DNS avec trois grands chapeaux : la manière dont le DNS devrait être utilisé, les statistiques principales-

Donc on a encouragé la participation autour de ces grandes thématiques, et on va continuer donc nos travaux au sein de ce groupe de travail avec l'aide de la communauté autour de ces trois thématiques.

CATHRIN BAUER-BULST : Alors, vous allez entendre deux brèves présentations de David Conrad et Drew Bagley, qui sont assis à ma gauche. Et ensuite, on a un panel constitué de représentants des différents groupes qui ont également contribué à la préparation de cette réunion, donc Alan Woods de l'unité constitutive des bureaux d'enregistrement, Tania Tropina de NCUC, Denise Michel de l'unité constitutive commerciale, Jonathan Matkowsky d'IPC, le nouveau président du SSAC, et Jamie Hedlund, chargé des sauvegardes par rapport à la conformité contractuelle.

Donc comme Iranga l'a dit, on a essayé de structurer cette discussion. Donc voilà comment nous allons nous organiser. Nous allons commencer par deux brèves présentations et ensuite nous allons essayer de faire avancer la discussion en

passant par les trois catégories qui viennent d'être identifiées pour discuter des principes. Parce qu'on ne sait pas encore mis d'accord sur les principes qu'on devrait appliquer pour collecter les données et comment les utiliser par la suite. Il est apparu clairement que les principes qui allaient s'appliquer à ce processus devaient répondre à trois grandes questions. Ce sont les questions que vous voyez ici afficher à l'écran et auxquelles nous reviendrons lors de la discussion après les deux premières présentations. Ces questions sont d'abord : comment identifier l'utilisation malveillante du DNS de manière fiable et, à la lumière de cela, comment créer des rapports transparents et fiables pour rendre ces données accessibles ; ensuite, comment faisons-nous pour utiliser ces données. Voilà les trois catégories que nous espérons pouvoir débattre avec vous aujourd'hui, étant donné que nous avons des experts avec nous en la matière.

Nous aimerions vous inclure dans cette réunion. Donc après ces deux brèves présentations, on va lancer le débat où vous aurez l'occasion de poser des questions aux membres du panel. Et on va vous demander si vous voulez poser des questions sur une question générale ou sur une question spécifique aux membres du panel. On va vous demander de bien vouloir vous identifier, de lever la main pour que les personnes ici qui lèvent les

pancartes 1 et 2 dans la salle puissent vous voir, sachent que vous voulez intervenir et vous amène un micro. Et pour avoir autant d'interventions que possible, nous allons limiter à deux minutes le temps de réponse à chacune de ses interventions. Donc je vais demander aux membres du panel de bien vouloir respecter ces deux minutes de temps de réponse. Mais n'hésitez pas à intervenir et à nous faire connaître votre point de vue.

Donc sans plus attendre, nous allons commencer la première présentation qui va se concentrer sur le système de rapport des activités liées à l'utilisation malveillante du DNS.

DAVID CONRAD : Bonjour. David Conrad au micro, ICANN CTO.

Nous avons développé un système de rapport au sein de mon groupe sur les activités liées à l'utilisation malveillante du DNS.

Donc un petit peu de contexte. De quoi s'agit-il ? Ce DAAR en anglais, il s'agit de faire rapport sur les données liées à l'abus du DNS, par rapport aux données fournies par les bureaux d'enregistrement. Jusqu'à présent, on s'est concentré sur les gTLD parce que c'est ce sur quoi on dispose de données, mais ça ne se limite pas forcément au gTLD. Les ccTLDs qui souhaitent y

participer sont tout à fait les bienvenus pour en parler avec nous.

Donc comment fonctionne ce système de rapport ? Comme beaucoup d'entre vous le savent, il y a beaucoup de systèmes de rapport qui existent déjà. La plupart d'entre eux sont associées à des produits commerciaux ou des services commerciaux. Ce que nous faisons, nous, c'est d'étudier tous les détails des opérateurs de registres et des bureaux d'enregistrement, leurs données, et comme la plupart des analyses qu'on a menées, on essaie d'analyser un grand nombre de sources sous forme de RBL et on essaie de collecter ces données sur une période de temps afin de stocker suffisamment de données pour nous permettre d'effectuer des études.

Et on essaie d'analyser un certain nombre de menaces. Les menaces sur lesquels on s'est concentré se sont concentrées sur l'hameçonnage, les réseaux zombies et la distribution malveillante, également l'analyse de spam. On a inclus les spams à l'origine parce qu'ils sont un vecteur extrêmement efficace pour d'autres types d'abus. Et il y a également un indice et des informations qui nous sont fournies, parce que TLD qui est affecté par un logiciel malveillant ou une activité malveillante d'une manière ou d'une autre peut ensuite être impacté par le spam également.

On essaie aussi d'aborder les choses de manière scientifique en étant aussi transparent que possible. Et l'origine de notre projet remonte à un rapport de la part d'un fournisseur de sécurité qui a montré que le nombre de gTLD- il a démontré qu'il s'agissait d'un domaine de premier niveau qui correspondait à une chaîne spécifique que recherchait justement ce fournisseur – je crois qu'il s'agissait de .zip – ce qui a donné lieu au fait que ce domaine de premier niveau soit considéré comme malveillant.

Et lorsque cela a été publié, la presse a posé toute une série de questions adressées à l'ICANN et à la communauté dans son ensemble. Et un certain nombre de personnes de la communauté sont venues me voir, à l'ICANN, et nous ont demandés ou plutôt nous ont dit, « Il faudrait que quelqu'un ait une liste faisant autorité ; il faudrait qu'il y ait une méthodologie bien documentée sur laquelle tout le monde serait d'accord pour qu'on élabore par des rapports biaisés avec des intérêts commerciaux sous-jacents ». Donc c'est ce qui a donné lieu au DAAR.

C'est encore moi, donc je continue. Cela, c'est un problème technologique et ce n'est pas mon fort.

Donc le DAAR, je vous le disais, il s'agit de plusieurs menaces. Donc on collecte les mêmes données d'abus qui sont reportés

par les utilisateurs de l'industrie d'Internet. Et l'une des conditions principales du DAAR, c'est qu'il faut que l'on ne génère aucune donnée nous-mêmes. Ce qu'on fait, c'est qu'on prend des données disponibles au niveau du public et congénère ensuite des documents contenant des abus sous différentes formes, avec différentes catégories.

Les données en termes d'abus, qu'on collecte, sont utilisées par les systèmes de sécurité qui protège des millions d'utilisateurs au jour le jour. Le secteur académique et industriel est en train d'utiliser ces informations telles que nous le faisons et leur fait confiance. Les secteurs des universités et de l'industrie ont donné leur aval vis-à-vis de ces données, de la précision de ces données. Et il s'agit d'un cadre qu'on peut étendre afin de mieux comprendre ce qui se produit exactement.

Le point essentiel ici, c'est de savoir que le DAAR est un outil qui permet à la communauté ICANN de voir de quelle manière l'écosystème des noms de domaine est perçu à l'extérieur de notre communauté.

Voilà. J'aimerais afficher la prochaine diapo, s'il vous plaît. Voilà.

Alors une question était posée par rapport aux critères de sélection des séries de données du DAAR. Il s'agit de critères qu'on utilise avec la version courante du DAAR. L'une des

activités qu'on entreprend consiste à demander de la part du SSAC leurs contributions sur un critère. Et donc leurs contributions seront utilisées pour le DAAR. Et on développe aussi actuellement un RFP pour que des experts indépendants puissent contribuer sur notre méthodologie. Une fois que nous aurons reçu ces informations, nous élaborons un document pour décrire la méthodologie que nous proposons et nous la soumettrons pour commentaires publics. Et comme tout processus normal de l'ICANN, avec ses commentaires nous modifierons ce document en fonction des critères qui auront fait l'objet de commentaires. Mais pour lors, les conditions utilisées pour la sélection des critères sont les suivants : la confiance des communautés vis-à-vis des opérations de la sécurité aux fins d'exactitude, de clarté du processus. La liste de bloc doit fournir une claire classification, donc le réseau zombie, la distribution du courriel malveillant, l'hameçonnage etc. ; il s'agit de contributions qui sont introduites dans les opérations commerciales qui sont utilisées par les serveurs mail, et qui sont utilisés également par les fournisseurs de mail pour protéger leurs utilisateurs.

Un petit point de précision sur ces listes qu'on utilise. On les utilise pour tout, dans le cloud, dans les outils des réseaux sociaux, et très souvent dans le DNS. À Copenhague, on a eu une

présentation lors de la réunion du Groupe de travail technique faite par Paul Vixie pour le blocage des noms de domaine par l'intermédiaire d'une politique.

Donc on sait qu'il y a un certain nombre de fournisseurs de services Internet et de fournisseurs de mail qui bloquent des noms de domaine de premier niveau parce qu'ils pensent que ces noms de domaine sont remplis de noms de domaine malveillant et d'utilisation malveillante du DNS.

De plus, ils utilisent les RBL dans le système de messagerie commerciale et pour les fournisseurs tiers de service mail. Et dans le système DAAR, nous avons 7 RBL primaires, dont l'une à une liste constituée de toute une série d'éléments supplémentaires.

Donc pourquoi est-ce qu'il y a un système de rapport sur les noms de domaine malveillant ? Le GAC avait exprimé une certaine préoccupation à Hyderabad. Et de manière plus réaliste, le spam constitue une menace vis-à-vis de la sécurité. Le système DAAR mesure non pas les domaines de spam eux-mêmes, mais ce qui est affecté par le spam.

Donc je vais maintenant céder la parole à une autre personne.

CATHRIN BAUER-BULST : Merci, David. C'est à Drew maintenant.

DREW BAGLEY : Merci, Cathrin. Je m'appelle Drew Bagley. Je travaille avec la Fondation pour la sécurité des noms de domaine et CrowdStrike. Et j'aimerais parler avec vous de la manière dont on pourrait utiliser ces données au niveau opérationnel pour bloquer les TLD, plutôt que d'informer des politiques qui pourraient améliorer les efforts visant à maintenir un Internet libre et ouvert, et ne pas aller à l'encontre de l'idée de l'acceptation universelle.

Comme Dave l'a dit, il y a consensus au sein de la communauté concernant plusieurs formes d'abus, en particulier pour ce qui concerne l'hameçonnage et le courriel malveillant. Et également concernant les mécanismes utilisés pour faire face au spam.

Donc ce qui est important, au sein de la communauté, c'est de comprendre, c'est qu'il ne faut pas être pris par les différentes interprétations qu'on peut avoir du terme abus, qui peut nous empêcher d'agir. Il faut que la communauté commence à travailler sur des aspects politiques qui font l'objet de consensus et où il y a des mesures ou des données qui sont mesurables. Comme le disait l'orateur précédent, dans le cas de

l'hameçonnage, des contenus malveillants et du spam, c'est ce qu'on peut faire.

L'équipe de révision s'est penchée sur le problème que posent les abus du DNS par rapport aux sauvegardes mises en place pour prévenir l'abus vis-à-vis des nouveaux gTLD et pour le mesurer. Ce qu'on a examiné, ce sont l'hameçonnage, le contenu malveillant et le spam. Et on a travaillé sur différentes listes de manière macro pour pouvoir présenter des recommandations.

Et j'utilise là comme un exemple pour vous montrer la manière dont ces données peuvent être utilisées pour donner lieu à des politiques menées en fonction des intérêts de la communauté.

Donc ce dont on s'est rendu compte sur une analyse d'un an qui a pris en considération ces données, c'est que de fait l'abus est quelque chose qui en fait n'est pas du tout universel et qui s'applique à tous les TLD. Mais on a identifié certains facteurs qui étaient plus susceptibles d'être identifiés à certaines zones, à certains bureaux d'enregistrement ou à de bas niveau d'abus, surtout chez certains opérateurs de registres et bureaux d'enregistrement.

Donc il ne vous surprendra pas de savoir que lorsqu'il y a des restrictions importantes sur les enregistrements, lorsqu'il est

difficile d'enregistrer un nom de domaine, il y a peu d'abus. De la même manière, lorsque les bureaux d'enregistrement ou opérateurs de registres ont tendance à avoir de hauts niveaux d'abus, eh bien, il y a des prix inférieurs qui sont proposés avec des propositions d'enregistrement en gros également. Et j'en parlerai tout à l'heure.

Également, il y a une analyse à un microniveau de ces TLD que nous avons fait, et nous avons identifié un lien étroit entre les marques de commerce qui sont utilisées comme hameçon. Et justement, qui est souligné dans ce rapport, c'est qu'il y a 76 noms de domaine qui utilisent différentes versions de marque, tel qu'iPhone, pour essayer de faire une campagne d'hameçonnage contre les utilisateurs. Et d'autres noms de domaine, 76 noms de domaine, avec 83 instances d'abus dans ce TLD en un seul trimestre.

Et donc, d'une manière générale, ce que les données nous ont montré, c'est qu'il y a en fait une lacune en matière de politique. Voilà pourquoi il est très important de bien comprendre ce que fait le projet DAAR ainsi que d'autres communautés, donc de collecter, de rassembler ces ensembles de données très importants, surtout en s'appuyant sur les données du WHOIS pour voir les mécanismes qui existent et qui ne traite pas de

toutes les situations possibles qui pourront avoir un impact sur la stabilité et la résilience du DNS.

Donc je vais souligner deux bureaux d'enregistrement, en particulier, qui posent réellement problème dans le contexte de nos outils, et qui doivent donc donner lieu à de nouvelles politiques.

Premièrement, il s'agit d'un bureau d'enregistrement qui a été suspendu depuis l'étude, mais pendant 2016, pendant la majorité de l'année, il a pu fonctionner avec de très hauts niveaux d'abus. Et donc, c'est ce niveau très élevé d'abus qui a entre autres donné lieu à la suspension, mais pas seulement. En fin de compte, ils n'ont plus payé leurs factures. Si vous êtes dans la cybercriminalité, vous avez intérêt quand même à payer vos factures, sinon vous ne pourrez plus continuer. Donc c'est un petit peu la leçon à tirer de ça.

Mais ce qu'il faut souligner, c'est qu'en fait, à la base, le modèle était basé sur les plaintes. Et donc on s'attendait à ce qu'il y ait une approche réactive à l'abus du DNS. Mais si on procède de cette façon, l'intervention est plus lente au niveau de la communauté. Ce qui serait plus adapté c'est d'utiliser ces ensembles de données très larges, c'est justement à ça que correspond le projet DAAR, et cela nous permettra de détecter

les problèmes en amont et de réagir plus tôt, plutôt que d'attendre de voir ces infractions se produire après avoir déjà eu un certain nombre de victimes.

Alors, deuxième bureau d'enregistrement, AlpNames, qui est toujours en fonctionnement. Donc même niveau très élevé d'abus. Et lorsque la recherche CCT a été faite, ce bureau d'enregistrement proposait des enregistrements en gros. Un candidat pouvait enregistrer 2000 noms de domaine en une seule fois et créer un algorithme de génération de domaine pour un utilisateur. Donc 2000 noms de domaine qui, je suis sûr, étaient très intéressants. Et donc, vous avez votre domaine, vous l'enregistrez et il ne vous surprendra pas de savoir qu'il y avait un très haut niveau d'abus pour ce bureau d'enregistrement. Mais le nombre de plaintes n'a pas nécessairement donné lieu à des suspensions.

Grâce à ces données de gros, eh bien, il est facile de voir que cela représente une lacune en matière de politique pour la politique.

Je n'arrête pas d'appuyer sur le mauvais bouton. C'est sans doute parce que j'aime beaucoup ces deux bureaux d'enregistrement.

Alors où en sommes-nous ? Donc l'équipe de révisions CCT a pu mettre en place certaines recommandations en matière de

politiques qui seront publiées pour la communauté avec un chapitre sur l'abus du DNS qui sera donc disponible dans une semaine ou deux. Mais on ne va pas s'arrêter avec cette équipe de révisions CCT. En tant que communauté, au fur et à mesure que nous avons davantage de données, que ce soit par le projet DAAR ou par le travail de l'équipe cyber sécurité, l'APWG, Spamhaus, etc., tous ces différents groupes pour nous présenter des données. Et en tant que communauté, c'est non seulement l'approche opérationnelle, mais aussi les politiques, la définition des politiques, l'identification des lacunes, de manière à passer du modèle réactif au modèle proactif en matière d'abus du DNS pour que les bureaux d'enregistrement, les opérateurs de registres, puissent empêcher de plus en plus de voir des abus se produire par certaines entités. Et donc l'idée c'est vraiment d'atténuer les abus de manière très globale. Donc ça l'idée de ce panel d'aujourd'hui de voir les différentes perspectives, parce que ceci touche les différents groupes de notre communauté. Nous en sommes à un point où nous avons des données que nous pouvons exploiter, donc exploitons-les pour atténuer les risques et avoir un DNS plus sécurisé.

Je repasse maintenant la parole.

IRANGA KAHANGAMA : Merci, David, pour cette présentation. Je souhaite remettre l'accent sur la limite de deux minutes pour les réponses aux questions. Nous avons déjà un petit peu de retard, donc je souhaite m'assurer que tout le monde a le temps de participer.

Alors, en ce qui concerne les panélistes, donc vous serez limités aux deux minutes. Toutes les personnes qui sont dans la salle sont libres de prendre le micro si elle le souhaite. Nous allons d'abord commencer par Alan qui va, puisqu'il est temps pour le top de commencer, on a parlé de différentes choses jusqu'à maintenant.

Lorsqu'il y a vraiment un problème d'abus, quels sont les outils à la disposition du bureau d'enregistrement pour convertir ce type de tendance, pour en fait identifier certains de ces récidivistes.

ALAN WOODS : Merci. Je viens de Donuts. Alors pour répondre à la question, vous avez dit les personnes qui sont des récidivistes évidentes. C'est un petit peu compliqué. Les données nous arrivent par DAAR. Il y a d'autres sources de données avec des listes très utiles de choses qui sont sans doute abusives, mais nous ne pouvons pas dire que c'est évident d'identifier un contrevenant.

Donc nous devons faire remonter les informations à un bureau d'enregistrement, à la partie concernée. Mais la question à poser, c'est comment est-ce que l'on sait qu'il s'agit vraiment d'un abus. Lorsque nous obtenons des informations et des preuves de toute évidence, nous utilisons ces preuves. Nous les rassemblons, nous les analysons et ensuite nous les faisons passer à la partie appropriée. En général, c'est le bureau d'enregistrement. Et si le bureau d'enregistrement n'agit pas, eh bien c'est l'opérateur de registre qui va voir si on va envisager d'intervenir.

Donc certes, il y a des indicateurs que nous recevons, des listes de Spamhaus, etc., mais il nous faut également avoir d'autres informations, d'autres preuves pour faire le pont entre les statistiques, pour faire le lien entre les statistiques, le fait effectivement que l'abus est confirmé.

IRANGA KAHANGAMA : Merci Alan. Donc comme suivi, pourrait-on dire que minimum, ces statistiques sont quand même déjà en fait un premier pas dans le bon sens ?

ALAN WOODS : Oui. Alors peut-être que je vais vous contredire un petit peu. Souvent, les seules preuves que l'on trouve, c'est le fait que les gens sont présents sur les listes. Donc il faudrait avoir davantage de détails, voir un petit peu quelles sont les raisons pour lesquelles ces personnes sont placées sur ces listes ; parce que pour nous, le fait que ces personnes soient sur ces listes ne suffit pas. Donc c'est un petit peu plus compliqué pour nous. On fait tout ce qu'on peut. Dans ces cas-là, s'il y a vraiment un point qui pose problème, on essaie d'identifier la raison pour laquelle il y a un problème.

Mais c'est très compliqué en fait de tenir ces informations. Les gens qui rassemblent ces listes, qui composent ces listes, ont des secrets qu'ils ne nous livrent pas.

DAVID CONRAD : Une des raisons pour lesquelles DAAR inclut des informations historiques, c'est pour aider à identifier certaines tendances au fil du temps, y compris tout ce qui a informations abusives sur des périodes de temps prolongé. Donc tout à fait d'accord, à 100 %. Le concept d'évidence d'abus et le fait qu'il y ait simplement des informations ne permettent pas nécessairement d'identifier quelqu'un qui est réellement coupable d'abus.

Mais en partie, l'idée de notre travail dans la communauté c'est de fournir des informations sur de longues périodes de temps pour permettre une discussion en matière de politique qui puisse permettre d'identifier de manière très claire des tendances d'abus dans des espaces de noms déterminés.

IRANGA KAHANGAMA : Merci. Nous allons demander à Rod, et ensuite on passera au micro 2.

ROD RASMUSSEN : Rod Rasmussen au micro et je parle en mon propre nom. Je ne représente pas le SSAC ici.

Répondre assez directement à la question. Je pense que la réponse que nous avons entendue, c'est une réponse d'identification de la plupart d'une entité spécifique. Alors la partie fiable, cela veut dire politique, confiance, etc.

Dans notre industrie, nous existons depuis 10, 15 ans, et nous avons des méthodes très fiables d'identification des abus, de manière systémique.

Ensuite, tout ceci est renvoyé dans Internet Explorer, Google le navigateur sécurisé, les services Gmail, Hotmail, etc. Tout ceci

est automatique maintenant. Et de grande ampleur, de manière automatisée, sur des millions d'instances.

Alors la question de l'identification, il faut savoir que la technologie est fiable. Il y a beaucoup de méthodes pour établir des listes, pour réduire les faux positifs et arriver pratiquement à zéro. Donc la technologie existe. La clé c'est transformer ces informations en action. Et pour cela, il faut des contrats. Il faut de la confiance. Il faut tout un tas de détails ; un cadre qui permet aux gens d'agir dans le domaine, quel qu'il soit, que ce soit un fournisseur de services, un bureau d'enregistrement, un opérateur de registres, etc.

Donc pour moi, du point de vue technologique, le problème a été résolu. Par contre, du point de vue des politiques, non. Ce n'est pas le cas.

IRANGA KAHANGAMA : Merci Rod. On va demander maintenant à la personne micro de s'exprimer.

DAVE PISCITELLO : Dave Piscitello de l'ICANN au micro. Je n'aime pas la phrase ou plutôt l'expression « évidence d'abus ». C'est parce qu'on mesure avec le DAAR. Avec le DAAR, on mesurera les menaces à

la sécurité sur la base des listes de blocage et sur ce que nous percevons comme abus. Je crois que c'est complètement différent de l'obligation à un opérateur de registre ou un bureau d'enregistrement ou une société d'hébergement, un fournisseur d'hébergement, pardon, à considérer par rapport à ce qui leur a été présenté pour faire une investigation et pourrait effectivement confirmer cette plainte.

Moi, je vais chercher le mail. Si j'étais à votre place, j'irais chercher le mail avec l'URL. J'irai chercher la pièce jointe qui contient l'URL. J'irai sur le site, sur un Webget, quelque chose qui a été rejeté. Donc il y a beaucoup d'autres étapes qui représentent une diligence raisonnable du point de vue des bureaux d'enregistrement. Et je sais que ça coûte quelque chose.

Mais DAAR n'a pas pour objectif d'être le lieu où on se rend pour avoir toute la réponse. DAAR, c'est un mécanisme ; un mécanisme qui permet de faire un recensement de tous les espaces pour identifier là où les politiques fonctionnent, là où les politiques n'existent pas, et en fait, à la fin donc, de savoir comment créer une synthèse.

CATHRIN BAUER-BULST : Merci Dave.

Graeme, j'aimerais poser cette question bureau d'enregistrement. Nous avons maintenant parlé de tout ceci est des différents indicateurs que nous avons. Donc nous avons le DAAR qui est, en fait, une évaluation, une base. Mais il faut après faire davantage de choses du point de vue du bureau d'enregistrement pour que les informations soient utilisables, en fait, exploitables. Pour voir quels sont les clients qui ne sont pas conformes aux conditions.

Maintenant, ces conditions, comment les influencer, comment redéfinir vos politiques ? Donc est-ce que vous pourriez répondre à cette question ?

GRAEME BUNTON : Oui, merci Cathrin. Je suis avec Tucows, donc.

Il y a plusieurs points à mon avis qui sont intéressants. Alan a mentionné quelque chose de très intéressant tout à l'heure. C'est vrai que faire le lien entre les listes de blocage et les preuves, les preuves qu'on peut utiliser, ce n'est pas quelque chose de facile à faire.

Et Dave disait que les méthodes qu'on peut utiliser pour lutter contre l'abus sur les plates-formes, en fait, partent du principe qu'il y a une certaine sophistication du personnel de supervision

qui n'est pas forcément disponible, qui n'existe pas forcément chez les bureaux d'enregistrement. Donc pour réduire le nombre d'abus, il faut savoir qu'on n'a pas énormément de temps pour aller chercher toutes ces informations. Cela demande beaucoup de temps et de ressources.

Donc il faut savoir qu'il y a plusieurs utilisations qui sont faites de cette gestion des noms de domaine du point de vue des algorithmes. Donc encore une fois, en ce qui concerne les récidivistes et le suivi de ces récidivistes, je crois qu'il n'y a pas de réponse simple. En tout cas, ce n'est pas une réponse simple que nous avons trouvée. Cela nous permettrait de réduire les abus sur notre plate-forme, ce qui de toute évidence nous intéresse. Mais cela nécessite un point de vue très large par rapport à ce qui vous arrive listes d'abus. Et ça, nous ne l'avons pas.

CATHRIN BAUER-BULST : Merci Graeme. Je crois qu'Alan voulait dire quelque chose.

ALAN WOODS : Alan encore une fois. Je voulais simplement dire que ce que Dave Piscitello a dit tout à l'heure, moi j'aurais voulu lui serrer la main s'il était à côté de moi. Parce qu'en fait, c'est justement ce

que je voulais dire. DAAR est un projet qui donne des statistiques, mais il reste des choses à faire entre DAAR et l'intervention d'un bureau d'enregistrement ou d'un opérateur de registres. Donc merci Dave.

IRANGA KAHANGAMA : Merci Alan.

Alors rapidement, pour être plus spécifique, vous avez mentionné tout à l'heure, Monsieur, que, du point de vue technique, les choses étaient déjà faites. Donc quelles sont les données qui nous manquent encore ?

ROD RASMUSSEN : Alors il y a différentes méthodologies. Il y a des choses qui sont faciles à détecter, d'autres qui viennent des algorithmes, de la génération de noms de domaine. Donc il y a des séries de noms de domaines qui sont enregistrés peut-être à l'avenir, et donc vous avez des listes de domaines qui potentiellement seront utilisés ; vous devez surveiller l'enregistrement de ces domaines et agir en fonction. Parce que, vous savez, du point de vue de la sécurité, donc vous avez le spam qui est quelque chose qui existe depuis 10, 15 ans. Et du point de vue de l'analyse réglementaire, l'analyse est très sophistiquée. Il y a différentes

plates-formes, il y a Facebook. Les réseaux sociaux tous utilisent le programme. Les plates-formes e-mail, ils envisagent également l'utilisation du contenu par les utilisateurs. Et donc, il faut voir ces domaines. Et je crois qu'on peut utiliser ces informations pour établir le lien entre certaines métadonnées qu'on obtient des demandes, des requêtes WHOIS ou des requêtes du DNS. On peut également considérer les propres bases de données que l'on a avec différents objets. Il y a différentes formules qui existent pour cela. Et il y a aussi des outils supplémentaires qui existent sur les navigateurs, des dispositifs de sécurité de réseaux qui considèrent les flux de données entrants et sortants. Il y a des systèmes très sophistiqués de tunneling qui permette de superviser de contrôle les réseaux. Donc tout ceci peut être rassemblé pour former des listes des différents types d'abus.

IRANGA KAHANGAMA : Oui merci. J'ai cru que tu allais continuer toute la journée, mais effectivement cet élément est clé. Je crois qu'on a une question à distance. Non, on va prendre les questions à distance après.

CATHRIN BAUER-BULST : Oui. J'aimerais revenir aux différents types de données qu'il nous faut transmettre aux décideurs politiques ou à ceux qui

élaborent des politiques. Drew a dit clairement qu'il y avait des tendances générales et des développements pour informer les décideurs politiques de ce dont ils ont besoin pour prendre des actions individuelles. Ça ne dépend pas d'une enquête criminelle, mais ça va être en fonction des termes et conditions du fournisseur.

Donc peut-être qu'il faudrait fixer des normes pour les consommateurs. D'après vous, est-ce qu'il y aurait des enseignements attirés par rapport aux termes et conditions qui devraient être élaborées afin de permettre une réaction efficace vis-à-vis de cette utilisation malveillante ?

DENISE MICHEL : Denise Michel. Nous avons un système mondial très large d'atténuation de l'utilisation malveillante du DNS sur toutes nos plates-formes, qui sont surveillées et actualisées. Et nous coordonnons tout cela entre les différents secteurs pour partager, entre tous, les meilleures pratiques, que ce soit en termes de services ou en termes de partage de données et de sécurité aussi.

Je pense que si l'on regarde le contraste entre ce que l'on fait et ce que font les bureaux d'enregistrement et opérateur de registres, c'est un élément qui n'a pas été encore pris en

considération et qui devrait l'être. Et ça, c'est lié au commentaire qui a été fait par rapport à la révision ccTLD des abus et de la manière très spécifique dont cette étude pourrait être utilisée comme point de départ. La capacité de collecter des données visant à atténuer les utilisations malveillantes, les choses telles que les encouragements ou les frais que doivent payer les bureaux d'enregistrement et opérateur de registres, voir quelles sont les meilleures pratiques et ce genre de choses. S'assurer qu'il s'agit de la première étude relative aux abus et qu'on en fait une habitude. Et également, augmenter l'examen de la conformité pour s'assurer que l'on peut prendre des actions vis-à-vis de ces abus. Et dès que nous pourrons faire fonctionner cette initiative dans le domaine public et qu'on pourra voir le rapport DAAR, de manière bêta et sur le site Web, voilà comment on va pouvoir avancer. Merci.

CATHRIN BAUER-BULST : Oui. On va passer aux interventions dans la salle.

REG LEVY : Quelqu'un a parlé des termes et conditions à l'instant. Et il est vrai que pour beaucoup, il y a des termes et conditions qui stipulent qu'on peut tous retirer des choses pour une raison ou pour une autre. Et que s'il y a quelque chose sur lequel on n'a

pas pris de décision par avent, qui est absolument indispensable sur le moment et que ça n'existe pas simplement pour nous être imposé, c'est quelque chose qui nous est imposé.

CATHRIN BAUER-BULST : Oui. Je pense qu'on va passer à la prochaine section dans une minute. Mais je voulais poser la question à Jonathan par rapport à un point soulevé dans la présentation. Cette idée des indicateurs. Drew a dit qu'il y a un certain type d'abus que l'on recherche, et ensuite il y a plusieurs véhicules comme les spams que vous avez mentionnés, et parfois il y a des attentes aux droits de propriété intellectuelle qui peuvent être associées à des abus ou à des indicateurs d'abus potentiels. Pourriez-vous nous parler de ces indicateurs et de leur utilité pour identifier les cas d'abus ?

JONATHAN MATKOWSKY : Jonathan de RiskIQ et je parle en mon nom propre aussi.

Tout d'abord, en termes de bureau d'enregistrement et de leurs obligations, en termes du RAA, pour faire face aux cas d'abus, ça c'est tout à l'avantage de la communauté. Donc moi, j'encourage la communauté à utiliser cette opportunité pour s'assurer que la communauté protégée des abus. Et ça, ça inclut

toutes les activités illégales. On peut y inclure l'hameçonnage qui porte atteint à vos informations personnelles avec toutes les activités liées aux contenus.

On a entendu la manière dont le rapport SADAG a parlé de domaine qui utilisait de manière malveillante ces informations. Et cela posait des menaces. Des menaces en termes de sécurité. Et vous aurez lu dans la presse la manière dont Adobe Flash, les popups Adobe flash ont été utilisés pour tromper les gens et les inciter à télécharger des informations malveillantes. Donc il y a des bureaux d'enregistrement qui ne régissent pas aux réclamations d'abus. Donc il faut s'assurer, lorsqu'ils sont notifiés, qu'ils prennent les mesures nécessaires et ces informations sont incluses dans les analyses statistiques, techniques de l'ICANN. Et elles sont disponibles à tout moment.

Donc je dirais que le projet DAAR devrait être utilisé en interne, et on devrait encourager la communauté à utiliser ce projet, parce que les séries de données que j'ai vues dans le rapport SADAG m'ont fait voir que ça, c'est une menace, mais il y en a d'autres. Regardez ce qui se passe avec les Dynamic Dolphins par exemple, et regardez ce qui s'est passé.

IRANGA KAHANGAMA : Je vais passer à la deuxième partie de la conversation. Donc, comment créer un système de rapports efficaces et transparents en termes d'abus. Je vais poser la question à Tatiana. Conrad, dans sa présentation, a parlé d'un certain nombre de cas où ces blocklists étaient utilisées, ces listes de blocage étaient utilisées dans les navigateurs Internet et e-mail.

Ma question est la suivante. Est-ce que les données d'abus du DNS peuvent être utilisées pour créer un outil virtuel qui soit facilement accessible au public ?

TATIANA TROPINA : Oui. Merci de cette question. D'abord, pour préciser quelque chose, nous ne représentons pas les utilisateurs commerciaux ou finaux. Nous représentons les utilisateurs non commerciaux et c'est une grande différence. Ce que je voulais dire, c'est que nous avons une position sur les outils de rapports des abus et des systèmes d'identification d'abus.

Et j'aimerais souligner le fait que nous sommes le NCUC. On ne s'occupe pas de collecter des statistiques. On ne suspend pas des sites Web. Mais ce que l'on défend, c'est la chose suivante. Quel que soit l'outil qui va être utilisé, moi, à titre personnel, je peux dire que je suis pour les statistiques, pour l'échange d'informations. Mais ici, à l'ICANN, on défend une ligne claire

entre l'aspect technique des abus du DNS dans le cadre de la mission de l'ICANN et les abus uniquement liés aux contenus. Parce que tout ce qui est illégal, selon la loi en vigueur, ne sera pas forcément un abus technique du DNS. Et nous pensons que l'ICANN et les outils utilisés par l'ICANN devraient être liés à la mission de l'ICANN. Je sais qu'il y a quelqu'un du RAA ici, mais ça, ça date de 2013. Et la mission de l'ICANN à l'époque était différente. Donc il faut être attentif aussi. Parce que j'ai beaucoup entendu parler d'approche préventive.

Mais pour ce qui s'agit d'agir, d'agir en amont et de prévenir, il faut voir quelles sont les parties prenantes en jeu ; que veut dire cette prévention. Je pense qu'il faut être clair ici. Je pense qu'il faut avoir une définition très claire des abus du DNS. Et en tant qu'utilisateurs non commerciaux, nous pensons également qu'on ne devrait pas oublier le fait qu'il ne s'agit pas simplement de suspendre les droits de ceux qui sont en train d'enfreindre la loi, et excusez-moi je vais encore dépasser de 20 secondes, mais on ne veut pas que des intermédiaires agissent comme des gendarmes de contenu ou des gendarmes en aucune sorte.

C'est pourquoi on est préoccupé lorsqu'on entend que l'industrie devrait jouer le rôle de gendarme et se protéger elle-même. On n'est pas d'accord avec ça.

CATHRIN BAUER-BULST : Merci Tatiana. Et je vais demander à Drew si vous, vous avez un point de vue sur la fréquence à laquelle ces données devraient être publiées d'après vous. Est-ce que vous pensez qu'il existe une fréquence idéale pour la publication de ces données ?

DREW BAGLEY : Oui merci. Si vous faites référence à l'étude demandée par le CCT, je pense qu'effectivement ça n'est pas quelque chose qu'on peut faire tous les cinq ans, à chaque fois qu'il y a une équipe de révisions qui se penchent sur cette question ou que d'autres équipes de révision examinent ce genre de choses.

Je pense plutôt que le projet DAAR pourrait régulièrement et de manière périodique à faire une analyse de ces données. Donc vous avez des données disponibles pour la communauté, et ensuite une analyse complète de ce qu'a fait l'étude du CCT peut-être trois fois par an, ça serait très utile. Parce que, pour non, il est très important de comprendre quelles sont les tendances et avoir une vision un peu distante des choses. Parce qu'il est très important d'avoir une évaluation constante et permanente en tant que communauté.

Et si vous êtes d'accord, j'aimerais répondre et réagir un peu au commentaire de Tatiana, parce que Tatiana a fait d'excellents commentaires qui reflètent réellement la diversité de la communauté et les points de vue divergents de la communauté à cet égard. C'est pourquoi j'insiste sur ce que j'ai dit en vous présentant ma première diapo. Plutôt que de passer des années à débattre des différentes choses, qu'est-ce qui pourrait être un abus dans un pays et ne pas être considéré comme un abus dans un autre, se mettre d'accord sur les choses qui font l'objet d'un consensus et qu'on puisse avoir une autorité sous forme de comportement interdit et de choses techniques, plutôt que de se perdre en chemin et de construire sur les choses sur lesquelles on est d'accord, comme dit Tatiana.

Et il a été dit aussi à quel point il est intéressant de voir les choses du côté réactif est de voir ce qui se passe du côté des contrevenants aussi. Parce qu'effectivement, comme l'a dit Tatiana, il y a des fournisseurs qui sont suspendus, mais il faut aussi agir au niveau de la prévention. Donc il faut adopter un modèle proactif où, dès qu'on soupçonne un nom de domaine de choses douteuses, bref, il y a différents modèles qui fonctionnent en fonction de différents fournisseurs, il faudra les analyser.

DAVID CONRAD : Il faut générer un rapport mensuel pour reprendre les statistiques qui sont vues au niveau des agrégés pour les opérateurs de registres et les bureaux d'enregistrement. Et ensuite, les opérations- ces informations, pardon, ou plutôt c'est le plan, ces données s'inscrivent dans le cadre de l'initiative des données ouvertes à long terme, de sorte que les gens puissent faire une analyse pertinente des tendances en fonction des données qu'on collecte.

Mais voilà un peu la fréquence ou la méthodologie que je suivrai pour diffuser ces données.

IRANGA KAHANGAMA : Est-ce que vous avez une date approximative de ce premier rapport ?

DAVID CONRAD : Oui. Pour l'instant, en fait, je ne suis pas très à l'aise pour vous donner une date exacte parce que, bon, c'est toujours difficile à fixer.

IRANGA KAHANGAMA : Intervention dans la salle.

MILTON MUELLER : En fait, il y a deux approches différentes s'agissant du DAAR. Lorsque j'ai entendu David en parler, j'ai entendu parler d'une collecte de toute une série de données qui donne lieu à des rapports qui peuvent être utilisés pour orienter les politiques, mais j'ai entendu les bureaux d'enregistrement et opérateurs de registres qui disent qu'il y a beaucoup de travail à faire entre l'analyse de ces données et la prise d'action.

Et ensuite, j'entends parler d'actions plus préalables. Donc je me demande à quoi va ressembler le DAAR, parce que les menaces changent. Et maintenant, on repose uniquement sur des RBL de parties tierces donc ça me semble très bien, mais les menaces changent, les contrevenants aussi, les techniques aussi. Donc comment allez-vous faire face à ces innovations qui évoluent en permanence ? Est-ce que vous avez les capacités de le faire ou est-ce que vous allez continuer à défendre d'entités tierces pour obtenir ces données ?

DAVID CONRAD : La réponse simple c'est qu'on fait ce que la communauté nous dit de faire.

Si dans le contexte du DAAR, la menace qui est identifiée et que l'on suit, ou la menace qui a été identifiée dans le communiqué

du GAC de Beijing, on va voir ce qu'on doit faire pour l'inclure dans le cadre du DAAR.

Par rapport aux sources de données, la première condition pour les données, pour la source de données, c'est qu'elle soit disponible au niveau public. On pourrait l'incorporer dans le système DAAR, mais, ça, encore une fois, ça dépend de la demande ou des demandes de la communauté.

Et je pense que mon collègue, M. Piscitello, aura peut-être quelque chose à ajouter.

DAVE PISCITELLO : Oui. Je suis ravi que vous ayez posé cette question parce qu'il y a un certain nombre de choses que, d'après moi, nous pourrons faire d'ici un an et qu'on n'a jamais pu faire.

L'une des choses que vous pourrez faire après un an et demi, c'est voir quel est le délai ou le temps qui s'écoule un enregistrement et la manière dont ces noms sont utilisés. Donc je peux vous montrer un graphe qui montre qu'il y a eu un cas avec un millier d'enregistrements, et ensuite ces enregistrements, après une certaine période, sont distribués. Et certaines des mesures du SADAG se fondent sur l'analyse de cela.

Donc par rapport aux menaces qui évoluent, j'ai eu une discussion avec les personnes qui développent ce processus pour parler d'ajouter une black liste si nous pensons que les données dans ces bases de données sont pertinentes, précises, crédibles, etc. Et si c'est quelque chose que l'on veut introduire dans notre système, parce que c'est intéressant pour notre communauté de savoir que c'est une autre menace. Mais comme David l'a dit, on a créé la plate-forme de manière très vaste à bien des égards, et donc plus on va comprendre quelles menaces on veut mesurer, plus on va pouvoir aller dans le sens suggéré.

DAVID CONRAD : Merci Dave. Je crois qu'il y a deux questions à distance. On va donc aller lire et ensuite on y répondra. Et après donc, on passera à la suite de la discussion.

JAMES COLE : Voici une question de Maxim Alzoba, de FAITID. « Est-ce que le bureau technologique de l'ICANN a prévu de travailler avec le DAAR de manière à ce que la ressource soit disponible pour les bureaux d'enregistrement et les opérateurs de registres ? »

IRANGA KAHANGAMA : Deuxième question, s'il vous plaît, aussi.

JAMES COLE : « Quelle est la raison pour laquelle on utilise des sociétés avec des approches un petit peu qui demandent à réfléchir, donc il n'y a pas de transparence, il n'y a pas de recevabilité par rapport à la communauté ? »

DAVID CONRAD : Merci pour ces questions. Alors je commence par la deuxième question. L'utilisation de Spamhaus, pourquoi ? Eh bien, c'est parce que dans la communauté de lutte contre les abus, Spamhaus est une source de confiance. En tout cas, elle est considérée comme telle puisque tous les critères spécifiés dans le rapport initial de sélection ont été respectés. Il faut également savoir, quels que soient nos sentiments par rapport à une liste de blocage, c'est liste de blocage, en réalité, elles sont utilisées par l'industrie, par les universités, par des fournisseurs commerciaux et non commerciaux pour avoir un impact sur le flux de trafic, sur Internet. Et donc, le fait de dire qu'une liste de blocage n'est pas importante simplement parce qu'on n'est pas d'accord avec sa politique ne change pas le fait que d'autres utilisent ces listes de blocage pour bloquer le trafic d'un domaine spécifique ou d'une adresse IP spécifique. Donc les

critères de changement, donc Spamhaus, le fait que ce ne soit pas considéré comme une option fiable, c'est possible et on pourra ajuster les choses au fur et à mesure.

Mais s'il était prouvé donc que Spamhaus ne respecte plus les spécifications dans les manières dont elle traite les demandes, et bien, à ce moment-là, on pourra reconsidérer. Mais de notre expérience, selon notre expérience, les personnes qui se plaignent par rapport à certaines listes de blocage, c'est en général des personnes qui ont des intérêts. Et donc, il nous faut des preuves comme quoi les listes de blocage ne font pas ce qui doit être fait et à ce moment-là cela représente une bonne raison pour laquelle on reconsidérera.

Mais en ce qui concerne la fourniture de donnée à la communauté, notre plan actuel, c'est de rendre ces données disponibles dans le cadre de l'initiative Open Data mensuellement pour l'instant, mais on peut ajuster ceci, je pense, suivant ce que nous demandons à la communauté suivant les besoins.

IRANGA KAHANGAMA : Merci David. Je crois qu'il y a encore une question à distance. Donc je voudrais la poser maintenant.

JAMES COLE : Cette question nous vient de Kristina Rosette de Amazon. « Quels sont les mécanismes et les processus mis en œuvre par l'ICANN pour éviter les faux positifs et éventuellement les problèmes de responsabilité avant que le DAAR soit mis à disposition du public ».

DAVID CONRAD : C'est encore pour moi. D'accord.

Comme je l'ai mentionné déjà, nous ne générons pas ces données nous-mêmes. Nous comptons sur des parties externes et n'importe qui peut s'inscrire, payer pour obtenir une licence pour avoir ceci à disposition. C'est un rapport est considéré comme un faux positif, eh bien, cela a un impact sur les millions d'utilisateurs de ces RBL et sur leur interaction avec les ressources, qu'il s'agisse d'un nom de domaine ou d'une adresse IP.

Certes, il y a eu des faux positifs. Il y a souvent des anecdotes avec des descriptions de faux positifs quelque peu risibles, mais la réalité c'est que les critères de sélection que nous utilisons pour les listes de blocage ont été approuvés par l'industrie, par les universités. Il y a un processus documenté qui est suivi. Et

donc il existe un mécanisme très clair de fonctionnement de ces listes de blocage.

En ce qui concerne la question de la responsabilité, la responsabilité civile, là, je ne suis pas au courant et je n'en parlerai pas.

CATHRIN BAUER-BULST : Merci beaucoup David. Nous passons maintenant à la troisième partie de la discussion. Donc au cours des 12 à 15 minutes donc la question est de savoir comment est-ce que ce signalement d'abus peut aider les bureaux d'enregistrement et les opérateurs de registres dans leurs efforts d'atténuation et de prévention. Et on va parler également des contrats et des politiques. Donc nous n'avons pas vraiment parlé de son utilisation au sein de l'ICANN. Donc Jamie, je peux peut-être vous poser la question. Est-ce que vous avez vu l'impact que cela pourra avoir sur la conformité des contrats l'avenir ?

JAMIE HEDLUND : Effectivement, quand j'ai besoin de quelque chose je le dis. Merci de me donner cette opportunité. Nous avons collaboré étroitement avec OCTO et le département de conformité

contractuelle. Et je crois qu'ils sont très contents de ce projet DAAR pour plusieurs raisons.

Premièrement, parce que cela permet de fournir des données, des preuves qui nous indiquent où déployer nos ressources. Deuxièmement, s'il est vrai que ces listes de DAAR sont utilisées par des entreprises pour prendre des décisions sur les services e-mail et sur les accès etc., eh bien, notre travail en sera facilité. Parce qu'à ce moment-là, ses opérateurs et ses bureaux d'enregistrement se retrouveront un petit peu plus haut dans la hiérarchie.

Pour être clair, par contre, ce que nous apportera le DAAR sera au niveau d'agrégation. Et donc ce niveau-là, ce n'est pas quelque chose qu'on peut utiliser pour la conformité des contrats. Il faut aller un peu en dessous, il faut descendre un peu en dessous pour trouver vraiment des preuves qui pourront être utilisées pour ainsi dire nettoyer certains de ses opérateurs, ses zones d'opérateur et de bureaux d'enregistrement.

Alors, dernier point là-dessus, les résultats que j'ai pu observer montrent qu'il y a en fait très peu de parties contractantes qui sont responsables d'une grande majorité des abus constatés. Et donc, très fréquemment, ce ne sont pas des participants actifs à l'ICANN. Donc si on pouvait, par exemple, utiliser ces données

pour avancer, eh bien, bien sûr que ce sera positif pour les utilisateurs de l'Internet, mais d'une manière générale ce sera positif pour la crédibilité et la légitimité de l'ICANN dans le modèle multipartite. Et suite à la transition, c'est quand même un avantage tout à fait intéressant.

IRANGA KAHANGAMA : Merci Jamie.

ALAN WOODS : Merci, Jamie, de l'avoir mentionné. C'est une très bonne chose. Et ce que je souhaitais dire, c'est que c'est tout à fait vrai. Ces mauvais acteurs qui sont présents dans le monde de l'Internet, vous savez qu'il y a beaucoup d'opérateurs de registres qui sont très impliqués, qui vraiment sont présents aux réunions de l'ICANN, qui sont présents dans les discussions. Et de mon point de vue, du point de vue de Donuts, nous, une fois qu'on a l'épreuve, il faut absolument qu'on fasse quelque chose. C'est vraiment très important pour nous. Nous devons tester les preuves, bien sûr. Nous devons nous assurer qu'elles existent, mais après, bien sûr que nous souhaitons agir.

IRANGA KAHANGAMA : Merci. Graeme. Vous souhaitez dire quelque chose ? Vous m'avez regardé.

GRAEME BUNTON : Les bureaux d'enregistrement sont également tout à fait pour éliminer les mauvais acteurs sur les plates-formes, pour réduire la charge de travail que nous avons tous, pour vraiment nous assurer que nos plates-formes sont propres. Cela réduit également tout ce qui est politique, toutes les implications pour les politiques, parce que les solutions de politique s'appliqueront à tous les bureaux d'enregistrement, à tous les opérateurs de registres, c'est compliqué, alors qu'il faut vraiment cibler lorsqu'il s'agit d'un acteur très spécifique. Et donc, pour en arriver là, si on n'en arrive là, on résoudra beaucoup de problèmes à mon avis.

IRANGA KAHANGAMA : Micro 1.

GREG MOUNIER : Bonjour à tous. Greg Mounier d'Europol. J'ai une question pour Graeme et Alan.

Donc souvent, il y a des mesures qui coûtent cher pour l'industrie. Donc ma question c'est de savoir comment inverser cette logique, comment s'assurer qu'il y a des mesures proactives qui soient considérées comme un avantage concurrentiel. Quand est-ce qu'on va voir par exemple une stratégie de marketing qui dira à Tucows nous avons le taux le plus bas d'abus, donc vous économiser de l'argent et donc vous gagner des sous.

GRAEME BUNTON : Merci Greg. Graeme au micro. C'est une bonne question. Je ne suis pas exactement sûr de la réponse. Effectivement, la productivité, cela veut dire une responsabilité. Il faut prendre en compte les choses lorsqu'on regarde la ligne des résultats. Les technologies doivent en arriver au point où on est proactif par rapport aux enregistrements. Mais on n'y est pas encore ; en tout cas, personnellement, ce n'est pas quelque chose que j'ai pu constater.

IRANGA KAHANGAMA : Rod, allez-y.

ALAN WOODS : Oui. Pour Donuts, c'est la même chose. C'est quelque chose que nous prenons au sérieux. Cela fait vraiment partie du travail, de notre approche des abus du DNS. Mais il y a donc l'initiative, les initiatives volontaires, etc. Ceci veut dire que nous sommes différents en tant que nous sommes vraiment un bon acteur. Mais à chaque fois qu'on élimine un domaine, cela dit simplement à la personne d'aller autre part. Et ça, c'est une initiative à laquelle il faut qu'on pense. On les élimine de notre plate-forme, mais il y a d'autres plates-formes. Donc il faut nous concentrer effectivement sur ces mauvais acteurs.

IRANGA KAHANGAMA : Alors il y a d'autres personnes qui souhaitent prendre la parole.

ROD RASMUSSEN : Donc, ce dont on a parlé, c'est justement pour cette raison que je suis là et que je suis venu pour la première fois à l'ICANN. Je représente l'industrie des abus. J'essaie d'établir la discussion avec les bureaux d'enregistrement. Malheureusement, il y a d'autres choses qui se sont produites et qui ont empêché la discussion de démarrer dès le début. Vous pouvez regarder un petit peu ce qui s'est passé par le passé. Mais bon peu importe, c'était il y a 10 ans.

Il y a beaucoup de choses qui ont été faites et qui ont été faites de manière tout à fait positive. Un des exemples, c'est donc le groupe de travail avec lequel je travaille, Greg Aaron et d'autres. Nous avons un rapport que nous avons publié depuis 2007 sur l'hameçonnage, sur les tendances, sur les enregistrements de noms de domaine. Et donc l'hameçonnage. Et donc ces rapports ont été utilisés avec les bureaux d'enregistrement et les opérateurs de registres pour identifier les problèmes et les tendances, et ont permis d'avoir un impact sur les politiques à la fois au niveau des ccTLD et de l'ICANN. Surtout d'ailleurs pour les ccTLDs. Il y a eu de gros problèmes et nous avons pu les solutionner en identifiant les tendances, etc.

Alors il y a d'autres choses. Il y a des mécanismes de signalement automatisé des opérateurs de registre et des bureaux d'enregistrement avec des cadres de secours, donc dans le cadre des contrats. J'avais une société qui avait des contrats avec ces entités. Et donc, nous étions leur agent. Nous essayons d'identifier si quelque chose représenter suffisamment un abus ou pas, pour déterminer en leur nom et pour éliminer.

Et puis, il y a également un programme de confiance où on est accrédité et où on peut encore une fois appliquer cette confiance à quelqu'un. Donc encore une fois, on peut automatiser. Il y a des modèles qui existent. La question, c'est de

savoir comment communiquer les informations de manière à ce qu'elle soit exploitable. Merci.

CATHRIN BAUER-BULST : Parfait. Micro 1.

DAVID TAYLOR : Merci. David Taylor de Hogan Lovells. Je suis un avocat. Donc voilà, vous pouvez tous vous moquer de moi, mais je fais également partie de l'équipe de révision CCT. Donc là, vous pouvez m'applaudir.

Donc la question que j'ai, c'est par rapport au signalement des abus. C'est vraiment une question clé et il y a beaucoup de bons bureaux d'enregistrement, et il y en a qui sont mauvais. Même chose pour les opérateurs de registres. Des bons et des mauvais. Vous savez quand on poursuit les gens, il faut un certain temps pour qu'un bureau d'enregistrement élimine le domaine même si les choses sont très claires et qu'il y a réellement abus. Vous savez, en plein tribunal, quand on a prouvé vraiment qu'il y avait abus, il faut encore trois-quatre semaines pour que le domaine soit éliminé.

Mais lorsqu'on a un bureau d'enregistrement qui élimine, et Jamie, vous avez mentionné certains cas, il y a vraiment des

hauts niveaux d'abus. Le .science avec 51 % des noms qui sont abusifs. Et lorsque vous voyez que les domaines sont toujours présents, que le bureau d'enregistrement n'a toujours pas ôté l'accréditation au bout de six mois ou un an, on se pose des questions. Comment se fait-il que les choses traînent aussi longtemps alors que ça, c'est vraiment évident. Moi je ne comprends pas pourquoi nous avons cette difficulté.

JAMIE HEDLUND : D'une manière générale, il y a donc les preuves, les rapports, l'agrégation des rapports que les parties contractantes ont. En fait, cela ne suffit pas. Il faut davantage de preuves pour pouvoir agir. Deuxièmement, il y a des limites dans les contrats, qui sont donc inhérentes au contrat. Et on ne peut pas simplement suspendre un domaine. Et j'espère que ce qui ressortira du DAAR, des résultats du DAAR, c'est qu'on pourra identifier les échecs, les réussites et les échecs. Et bien sûr, les échecs ce sont tous les acteurs, tous les contrevenants qui existent toujours. Et donc c'est là que l'on va s'adresser à la communauté et qu'il faudra élaborer des politiques pour ces endroits où il y a des lacunes en fait.

Donc et même lorsqu'on n'arrive pas à nettoyer l'espace, la communauté, ce sont des gens comme vous qui pourront nous

apporter des preuves des lieux où cela ne fonctionne pas et il faudra donc établir certaines modifications dans les contrats.

IRANGA KAHANGAMA : Merci Jamie. Donc dernier commentaire avant de terminer. Denise va également mentionner quelque chose sur le signalement et sur son utilisation.

DENISE MICHEL : Donc le rapport SADAG, le rapport sur les abus CCT nous montre que les nouveaux gTLD ont beaucoup plus d'abus, 10 fois plus que les autres et donc, les données, les informations de ce rapport, sont très utiles est tout à fait pertinentes. Par exemple, pour le mécanisme de protection des droits, PDP qui est en cours par rapport à ce PDP et puis tout ce qui est PDP sur les procédures ultérieures. Donc nous sommes en train de voir quelles sont les politiques ça créer pour la prochaine série des nouveaux gTLD. Il y a d'autres choses qui s'appliquent à la mise en œuvre de l'anonymisation et de l'enregistrement fiduciaire. Mais lorsqu'on en arrive à l'abus de données, aux tendances, à toutes les activités de l'ICANN au sein de la communauté, nous devrions vraiment utiliser des données à la base de nos politiques. C'est vraiment critique.

Et s'il y a quelque chose que l'on peut faire pour effectivement faire avancer les avocats, pour peut-être publier le DAAR dans l'espace public. Il y a également l'initiative ODI. Tout ceci serait très utile. Et donc nous sommes prêts à soutenir ses efforts à l'avenir. Merci.

DAVID CONRAD : Alors, pour être très clair, bien sûr que je rigolais quand je disais que les avocats ne voulaient pas avancer. Bien sûr que les licences, nous sommes prêts à y travailler. Et nous devrions pouvoir avancer avec des rapports statistiques à l'avenir grâce à des informations plus complètes. Peut-être qu'on pourrait avoir un tableur. Je pense que c'est quelque chose qui sera publié sous peu.

CATHRIN BAUER-BULST : Très bien. Merci David. Nous avons pratiquement terminé. Donc on ne peut plus prendre de questions. Nous en sommes arrivés à la fin de la séance. Le débat nous montre qu'il reste encore des questions. Nous avons tous des perspectives différentes par rapport à l'atténuation des abus, et cela nous permet de souligner les différents besoins que nous avons dans la communauté, depuis les politiques à l'action, cela nous a permis d'identifier les différentes manières d'utilisation de données. Et

puis bien sûr, cela nous a permis de voir un petit peu les avantages du DAAR.

Alors, par rapport à ce qu'on nous a dit, il y a très peu de parties où sont concentrés les abus de notre point de vue. C'est là que les choses deviennent spécifiques parce qu'on peut agir même s'il y a deux faux positifs sur 76 exemples comme on a cité tout à l'heure. Eh bien, il existe d'autres données qui pourraient nous permettre d'agir.

Et donc à l'avenir, il faudrait voir comment combler cet écart entre ce qui est du domaine des agrégats et ce qui est du domaine de ce qui peut être fait. Et donc, on parlait des principes dans l'introduction. Donc je vais repasser la parole à Iranga pour terminer.

IRANGA KAHANGAMA : Oui. J'aimerais remercier tous les membres du panel de leur participation. Oui je pense effectivement qu'il faudrait avancer dans cette conversation pour que le groupe de travail pertinent continu à nous orienter. Mais effectivement, il faudrait voir quels sont les bons mécanismes pour commencer à avancer dans la bonne direction. Donc je pense qu'on va réétudier cette question pour voir comment avancer et quels sont les mécanismes à mettre en place pour que la communauté continue d'avancer

dans ses efforts d'atténuation des abus. Donc pour faire en sorte que la communauté continue à être intéressée par cette question et continue aussi à être ouverte et transparente.

Donc merci à tous encore une fois de votre participation aujourd'hui.

[FIN DE LA TRANSCRIPTION]