DEVAN REED : Je vais lancer l'enregistrement. L'enregistrement est en cours.

Bonjour à tous, bonsoir, bienvenue à cette session des politiques de l'At-Large sur l'utilisation malveillante du DNS en ce mardi 19 octobre 2021 à 17 h UTC.

Pour ne pas perdre de temps, nous ne ferons pas l'appel, mais la participation sera notée dans la salle Zoom et par téléphone.

Nous avons l'interprétation en français et en espagnol aujourd'hui. Si vous avez besoin qu'on vous appelle par téléphone, envoyez un message au personnel avec votre numéro de téléphone.

Avant de commencer, je vous rappelle à tous de bien donner votre nom avant de prendre la parole à chaque fois et de parler suffisamment lentement pour permettre l'interprétation. N'oubliez pas d'éteindre votre micro lorsque vous ne prenez pas la parole pour éviter toute interférence. Merci beaucoup.

Je vous passe la parole, Joanna.

JOANNA KULESZA : Merci beaucoup Devan.

Merci à tous d'être là et en particulier, merci à nos intervenants qui ont bien voulu parler de cette question de l'utilisation malveillante du DNS qui, comme vous le savez, est une sujet très important et qui est en

même temps un sujet qui prête à controverse au sein de la communauté de l'ICANN.

Pour cette séance, nous avons pensé à faire un petit exercice pour un petit peu rattraper les différentes activités des unités constitutives sur ce sujet. Jusqu'à maintenant, il ne s'agit pas d'un processus d'élaboration de politiques, mais la question de l'utilisation malveillante du DNS revient régulièrement dans la communauté.

Le contexte. Nous avons pour objectif de conclure avec une meilleure compréhension de l'utilisation malveillante du DNS de manière à présenter ceci au reste du monde. La raison pour laquelle l'At-Large a proposé cette séance comme éventuelle plénière pendant l'ICANN72 était qu'il semblait que nous ne cessons de considérer toutes ces questions de cybercriminalité, de sécurité, d'utilisation malveillante avec différentes perspectives.

Donc aujourd'hui, nous avons eu beaucoup de chance puisque nous avons pu inviter des membres de différentes unités constitutives qui vont pouvoir nous donner leur point de vue par rapport à ce qu'elles ont fait au sein de l'ICANN dans le domaine de l'utilisation malveillante du DNS. Et nous espérons donc pouvoir donner une voix à ceux qui sont avec nous de manière à échanger les idées, les points de vue par rapport au cadre que nous avons sur l'utilisation malveillante du DNS tel qu'il existe, est-ce qu'il est prêt, est-ce qu'on peut l'exporter à l'extérieur de la communauté de l'ICANN ou alors est-ce qu'il y a des problèmes dont nous devons encore débattre et que nous devons traiter.

Je vais présenter les intervenants. Nous avons choisi un ordre des interventions, mais avant de leur passer la parole, je vais présenter ces intervenants de manière à ce que vous puissiez comprendre un petit peu comment nous avons commencé la conception de cette séance, qui sont les intervenants et quel est l'objectif pendant ces 90 minutes.

Nous allons donc commencer avec Graeme Bunton qui est responsable du DNS Abuse Institute. Il a beaucoup géré les questions techniques, donc Graeme va nous donner une perspective assez large de l'utilisation malveillante du DNS. Dans la communauté, de temps à autre, nous avons pu observer certaines préoccupations par rapport à la définition de l'utilisation malveillante du DNS, donc Graeme nous donnera une introduction de ce sujet pour ceux d'entre vous qui peut-être ne connaissez pas bien la question.

Ensuite, nous allons considérer la perspective des registres grâce à Brian Cimbolic du Public Internet Registry, qui veut bien parler au nom du PIR. Il est vice-président où il travaille en tant que juriste. Nous allons essayer de voir, comme nous l'avons déjà vu, comment les choses se passent dans la pratique.

Ensuite, nous avons James Bladel, qui est vice-président de la politique internationale à GoDaddy. Nous essayons de voir un petit peu aussi le point de vue des bureaux d'enregistrement, quels sont les enjeux auxquels cette communauté est confrontée actuellement en ce qui concerne l'utilisation malveillante du DNS.

Avec le point de vue des parties contractantes que nous aurons vu, nous allons passer aux utilisateurs finaux et nous avons le plaisir d'avoir avec nous Lori Schulman, qui est présidente élue de l'IPC et qui est

également directrice sénior de la politique de l'internet au sein de l'association sur les marques de commerce. Donc nous aurons cette perspective sur l'utilisation malveillante du DNS. Lori nous parlera un petit peu de l'ampleur des applications pratiques des politiques que nous avons actuellement.

Et enfin mais certainement pas le moindre, nous avons le grand plaisir d'avoir avec nous notre collègue du comité consultatif gouvernemental. Ce représentant est un ami de l'At-Large, Nigel Hickson, et il nous parlera brièvement de la discussion au sein du GAC telle qu'elle est perçue du côté du GAC. Le GAC et l'ALAC ont déjà travaillé en collaboration sur différentes questions de politique et d'ailleurs, dans le cadre de l'ICANN72, je dois noter que l'ALAC et le GAC ont mis l'utilisation malveillante du DNS en priorité de leur ordre du jour. Nous souhaitons travailler de manière conjointe au sein d'une réunion, mais il nous semblait qu'il est important de bien connaître la perspective du GAC de notre côté à l'At-Large avec le potentiel de réglementation pour que nous comprenions mieux la définition.

Donc la première intervention sera surtout focalisée sur la conformité contractuelle, l'impact sur les utilisateurs finaux de cette conformité. Mais j'espère que Nigel pourra lui aussi nous donner le point de vue des gouvernements et de ce qu'ils sont en train de préparer en termes de révisions et de politiques ascendantes sur l'utilisation malveillante du DNS.

Nous avons en fait assez peu de temps pour ces remarques d'introduction des intervenants et la raison principale, c'est que nous souhaitons que ceci soit autant que possible une table ronde. Nous ne

pouvons pas nous retrouver en personne, donc nous perdons beaucoup cette composante supplémentaire que nous donne une réunion de l'ICANN en présentiel, donc nous avons décidé de ne pas inclure de présentation de diapositives, etc. Nous souhaitons que l'échange d'idées soit convivial et qu'il nous permette de bien comprendre les particularités de l'utilisation malveillante du DNS du point de vue des politiques de manière à ce que nous soyons prêts à présenter cette discussion à la communauté extérieure.

J'ai eu l'opportunité d'agir au sein de l'ALAC et de l'At-Large en tant que vice-présidente pour le renforcement des capacités, donc pour moi, ces discussions sont vraiment un exercice de renforcement des capacités. Nous souhaitons nous assurer que les utilisateurs finaux sachent exactement ce qui se passe par rapport à la protection des activités malveillantes en ligne. Mais j'ai la joie d'être accompagnée aujourd'hui par les deux coprésidents du renforcement des capacités, Jonathan et Olivier. Merci donc à tous les deux d'être avec nous de manière à m'aider à s'assurer que nous restons bien dans la direction de ce que nous souhaitons faire par rapport à cette discussion d'aujourd'hui.

Ceci étant, je passerai par la suite la parole à Jonathan après les interventions. Vous pouvez mettre vos questions dans le chat, vous pouvez lever la main et Jonathan nous guidera dans notre discussion. Et pratiquement à la fin de nos 90 minutes, nous aurons une conclusion et c'est Olivier qui s'en chargera. Il nous fournira une perspective très complète et synthétisée de manière à être prêt à présenter tout ceci au monde externe.

Voilà l'idée que nous avions pour cette séance. Je sais, je suis peut-être idéaliste, mais je pense que nous pouvons y arriver. Ceci étant, maintenant que vous connaissez les objectifs...

INTERPRÈTE : Nous nous excusons, petite interruption.

JOANNA KULESZA : Si vous voulez bien nous présenter une introduction sur ces questions d'utilisation malveillante du DNS. Et nous vous remercions de participer à cette réunion, d'avoir répondu à l'invitation. Donc si vous voulez bien prendre la parole pour nous présenter assez brièvement les différents travaux qui ont été effectués par le DNS Abuse Institute, nous vous serions très reconnaissants. Graeme.

GRAEME BUNTON : Merci Joanna.

Merci à l'ALAC de m'avoir invité aujourd'hui. J'apprécie cette introduction très complète. Je vais d'abord vous donner un peu de contexte par rapport à l'utilisation malveillante du DNS et vous parler un petit peu de ce que nous faisons au DNS Abuse Institute. J'espère que ce sera intéressant. Et je vais ralentir pour les interprètes.

Commençons par la définition de l'utilisation malveillante du DNS. C'est un sujet dont on parle fréquemment et c'est pratiquement ennuyeux me semble-t-il. Mais bon, il nous faut quand même définir des attentes.

Donc l'utilisation malveillante du DNS telle que définie par les parties contractantes, si je tire des enseignements des différentes discussions de la communauté, c'est le hameçonnage, les réseaux zombie et autres actions malveillantes. Donc c'est assez clair, nous avons ces différentes catégories qui ont été établies, ce qui nous permet de lancer la discussion.

À l'institut dont je m'occupe, le DNS Abuse Institute qui vient d'être mis en place suite à une initiative du PIR, nous avons également adopté cette discussion. Sans rentrer dans le détail, je dois vous dire qu'il y a d'autres points de vue. Il y a des faiblesses par rapport à cette définition qui est très catégorisée, que fait-on par rapport aux nouvelles attaques, le pharming, l'empoisonnement qui est en fait un empoisonnement avec le phishing et on ne peut rien faire par rapport à cet empoisonnement du DNS. On avait déjà parlé du phishing, donc je ne vois pas pourquoi on devrait avoir cette nouvelle catégorie.

Tout ce qui est une approche plus sophistiquée – et d'ailleurs, sur ce que CircleID a dit, je peux vous envoyer un article que j'ai publié là-dessus mais qui propose une nouvelle manière de voir les choses – mais du point de vue pratique, pour faire avancer la conversation, la définition résume ce dont on parle et c'est vraiment les lieux où nous devons agir de manière coordonnée. On pourrait parler de ce qui est un petit peu en marge, mais ma perspective, c'est que puisque nous avons cette définition avec les catégories, nous pouvons déjà commencer à faire un travail qui est nécessaire et efficace.

Où est-ce que ces problèmes se produisent ? Comment ? Le problème, c'est qu'il n'y a pas vraiment d'ensemble robuste de données d'analyse

sur l'utilisation malveillante du DNS. L'ICANN a produit l'outil de signalement des activités d'utilisation malveillante du DNS, donc c'est une bonne chose, mais ce n'est pas vraiment utile pour comprendre les différents abus qui se passent.

La communauté a tendance à parler en anecdotes, donc c'est un problème parce qu'il nous faut pouvoir identifier où se produisent les abus, parce que c'est à ce niveau-là qu'on pourra trouver des solutions appropriées.

Le DNS Abuse Institute travaille là-dessus pour élaborer notre propre plateforme d'enseignement de manière à pouvoir vraiment rentrer dans le vif du sujet et savoir quels sont les bureaux d'enregistrement et les opérateurs de registre qui présentent un problème en termes d'utilisation malveillante du DNS et également quels sont ceux qui font un excellent travail et que nous devons féliciter. En partie, ce travail revient à comprendre qu'il y a une différence entre les enregistrements malveillants et les sites web compromis. Cela veut dire qu'on prend l'existence des utilisations malveillantes et la persistance de manière à comprendre à quelle rapidité les registres et les bureaux agissent, et il faut voir aussi si nous avons des preuves, si nous pouvons agir.

Et ceci revient à autre chose d'important. La plupart des données en termes d'utilisation malveillante sont les RBL, donc les listes de blocage et de réputation, qui sont produites par des sociétés de sécurité et avec pour objectif de protéger les réseaux de manière à éviter que les emails ou les activités de réseau deviennent abusifs.

Le problème, c'est que ceci n'est pas produit pour des raisons d'atténuation. Le profil de risque de protection de votre réseau par

rapport à l'élimination d'un domaine, c'est complètement différent. Donc l'outil principal que nous avons pour comprendre l'utilisation malveillante du DNS n'a pas été créé pour l'objectif pour lequel nous l'utilisons et ceci crée vraiment une lacune.

Je pense qu'en tant que communauté, comme Institut, nous allons devoir consacrer du temps à comprendre les RBL, d'où vient l'utilisation malveillante des données et comment faire en sorte que cela soit plus utile pour les bureaux d'enregistrement et les opérateurs de registre.

Mais en termes généraux, pour que tout le monde sache de quoi nous parlons, nous avons 210 millions de noms de domaine de TLD génériques qui sont répertoriés dans leur rapport. Sur ce total, 1 million sont signalés comme coupables d'activité malveillante et une bonne proportion correspond à du spam. Donc on a entre 200 000 et 800 000 noms de domaine au monde qui sont nuisibles d'une manière ou d'une autre, sans faire la distinction entre malveillant et compromis.

La bonne nouvelle est que comme mesure relative, ce 100 000 sur 210 millions, ce n'est pas énorme. Mais pour comprendre les dommages, une campagne de distribution de logiciels malveillants ou le hameçonnage peuvent nuire à des personnes de manière très réelle et très négative. Donc on essaie de comprendre les données. Pour ce faire, nous avons parfois besoin de considérer la question de manière plus holistique.

Alors j'essaierai d'être relativement bref, mais il faut comprendre le contexte dans lequel apparaissent les utilisations malveillantes du DNS dans l'écosystème du DNS. Le contexte économique est qu'il s'agit d'une affaire globalement concurrentielle et que les bureaux

d'enregistrement, où qu'ils soient placés, sont en concurrence pour avoir les mêmes clients dans un secteur où les marges de revenu sont très faibles. La plupart des bureaux d'enregistrement en fait ne font pas la majorité de leurs revenus de la vente de noms de domaine mais plutôt parce qu'ils ajoutent l'offre de service d'hébergement, d'autres petits services. Donc lorsqu'on considère la vente de noms de domaine par des bureaux d'enregistrement et que l'on croit qu'ils font énormément d'argent, en général, ce n'est pas le cas et ce n'est pas l'essentiel de leur secteur, ce n'est pas à cela qu'ils font le plus attention.

Un économiste pourrait parler de cela comme un problème d'action collective, c'est-à-dire qu'il y a quelque chose qui a un impact sur tous mais qu'il y a des désencouragements pour l'action collective. Et c'est là qu'agit le DNS Abuse Institute. Grâce à la générosité de PIR, nous avons pu reprendre le dessus pour dire : « Nous allons faire le travail que nous croyons être nécessaire pour aider à améliorer cet écosystème et absorber une partie du coût qui aiderait tout l'écosystème pour former les parties prenantes, créer des ressources, des outils pour améliorer la situation par rapport à l'utilisation malveillante du DNS. »

Puis finalement, que peut-on faire par rapport à l'utilisation malveillante en tant qu'opérateurs de registre et bureaux d'enregistrement ? Il y a deux approches générales. D'une, du côté de la prévention, quand on empêche l'enregistrement de noms de domaine frauduleux, on essaie d'identifier les attributs d'un enregistrement malveillant et d'éviter qu'il soit complété ou que ce nom de domaine soit résolu. Par exemple, ce nom de domaine contient le titre PayPal. On va le réviser pour être sûr ; un processus de ce type.

D’autre part, on a des mesures réactives sachant que le nom de domaine est enregistré à des fins licites mais qu’il est compromis et commence à agir à des fins malveillantes. Vous allez dans ce cas-là enquêter et répondre. En général, cela implique d’éviter que le nom de domaine soit résolu. Au long terme, bien sûr, il est mieux d’agir de manière préventive que réactive. Il faut éviter que cela se passe. Mais du point de vue économique, dans le contexte dont je parlais, les bureaux d'enregistrement et les opérateurs de registre seraient tenus de rédiger un code qui soit intégré dans leur système. Et la plupart des bureaux d'enregistrement ont énormément de travail à faire pour pouvoir se conformer aux environnements réglementaires changeant. À mon avis, il est possible d’améliorer énormément les réponses réactives, c'est-à-dire d’améliorer le processus de signalement d’abus aux bureaux d'enregistrement et aux opérateurs de registre qui n’est pas très ordonné en ce moment, de meilleures formations pour que tout le monde sache comment protéger leur site web et leurs noms de domaine, les opérateurs de registre et les bureaux d'enregistrement auront un ensemble de meilleures pratiques pour savoir comment s’y prendre. Donc on travaille sur la partie de la formation à l’institut.

Mais le principal – et c’est ce qui nous occupe en ce moment et que j’ai hâte de présenter – est le fait que nous sommes en train de concevoir un site web qui sera appelé autrement, mais qui sera un outil de signalement des cas d’utilisation malveillante, un site web unique où n’importe qui pourra signaler l’abus à un bureaux d'enregistrement ou un opérateurs de registre. Vous n’aurez rien à faire, vous n’aurez qu’à saisir le nom de domaine sans même savoir quel est le bureau d'enregistrement si vous croyez qu’il s’agit de hameçonnage ou d’un

logiciel malveillant ; cela enverra directement un rapport au bureau d'enregistrement ou à l'opérateur de registre. Donc la personne qui aura identifié l'utilisation malveillante aura un processus beaucoup plus simple pour le signaler. Pour les opérateurs de registre et les bureaux d'enregistrement, ils vont recevoir des rapports qui ne seront plus aussi difficiles à mettre en œuvre qu'à présent. Donc cet outil sera d'une énorme valeur pour les opérateurs de registre et les bureaux d'enregistrement et ceux qui signaleront les cas d'abus vont trouver que cela est bien plus utile et cela permettra, nous espérons, de réduire le grand travail des efforts d'atténuation qui est parfois difficile.

Voilà ce qui nous enthousiasme beaucoup. J'espère qu'une partie de cela au moins pourra être lancé entre les premier et deuxième trimestres de l'année prochaine. Je risque un peu ma réponse ici, mais en tout cas, nous allons aussi vite que possible.

J'espère vous avoir donné une bonne idée de ce qu'est l'utilisation malveillante du DNS par cela, ce que nous en savons qui est malheureusement très peu en ce moment, quel est le contexte économique de l'utilisation malveillante au sein des bureaux d'enregistrement et des opérateurs de registre et les méthodes d'atténuation.

Je vais m'arrêter là et recéder la parole à Joanna. Merci et désolé si j'ai pris trop de temps.

JOANNA KULESZA : Merci beaucoup Graeme. C'était très utile, très informatif et très exact. Merci pour cette introduction.

Je sais que vous avez travaillé avec Brian entre autres au préalable et je me demandais s'il était disponible pour compléter cette introduction avec des données plus spécifiques vis-à-vis des activités en cours en ce moment pour garantir que l'utilisation malveillante du DNS soit une menace contrôlée. Alors très rapidement, je vais céder la parole à Brian. Brian.

BRIAN CIMBOLIC : Merci Joanna et merci à l'ALAC de m'avoir invité.

Je suis Brian Cimbolic, conseiller général au PRI, Public Internet Registry, et je vais parler ici en deux qualités. Je suis d'une part le coprésident du groupe de travail des parties prenantes des bureaux d'enregistrement sur l'utilisation malveillante du DNS, et ensemble avec l'institut, nous travaillons pour créer une chambre collective. Mes coprésidents sont Jim Galvin de Donuts et Reg Levy et Luc Seufer. Ensemble, nous avons intégré différents groupes de travail sur l'utilisation malveillante au cours de la dernière année. J'ai travaillé avec Graeme pour essayer de mettre au point différentes pratiques dans le but d'informer les bureaux d'enregistrement et les opérateurs de registre de différents types d'utilisation malveillante.

Nous avons organisé des activités de sensibilisation, nous avons contacté tous les bureaux d'enregistrement de notre groupe de travail et mis au point des pratiques pour répondre aux inquiétudes qui ont été soulevées. Par exemple, suite à la discussion avec le groupe de travail du GAC sur la sécurité publique, nous avons corédigé un document avec le PSWG sur la manière d'aborder les problèmes associés aux logiciels malveillants et aux réseaux zombie. Donc les registres doivent

enregistrer des milliers de noms de domaine pour pouvoir répondre véritablement à la menace qui y est associée. C'est donc relativement compliqué et nous croyons qu'il était important que les opérateurs de registre en soient informés et que les bureaux d'enregistrement soient également au courant de ces menaces pour les bureaux d'enregistrement et les opérateurs de registre.

La semaine dernière, le CPH a élaboré un cadre, qui est un document qui forme les bureaux d'enregistrement et les opérateurs de registre. Et ceux qui veulent s'impliquer vont avoir les principes directeurs pour savoir comment identifier ce qui constitue une utilisation malveillante ou pas. Je vais tout mettre sur le chat à la fin pour que vous sachiez comment trouver notre travail.

Les bureaux d'enregistrement ont également travaillé sur un guide sur le signalement de l'utilisation malveillante pour savoir comment mieux agir face à cela. Nous sommes en train de mettre à jour ce guide en ce moment et il devrait être disponible bientôt. Et nous aurons des informations sur toutes les informations que nous avons au sein de la chambre des parties contractantes. Nous avons également les attaques contre les IDN et dans ce sens, les bureaux d'enregistrement sont en train de travailler à la publication d'un document sur les escrocs et un document sur les appels des bureaux d'enregistrement lorsqu'un nom de domaine est suspendu pour utilisation malveillante.

Voilà en termes très généraux ce que font les groupes de travail de la CPH vis-à-vis de l'utilisation malveillante du DNS. Lundi prochain, nous aurons une séance là-dessus dans le cadre de l'ICANN72, donc venez

nous voir pour savoir ce que nous faisons et quels sont les autres domaines de travail dont nous nous occupons.

Par ailleurs, je suis également conseiller général à Public Internet Registry comme je l'ai dit, et une partie de mes responsabilités comprend la supervision de notre programme anti-abus. Notre programme est très centré sur les principes qui apparaîtront également dans le chat. Nous travaillons avec des principes tels que la transparence, l'engagement au processus dû et la reconnaissance de l'équilibre entre l'échelle des dégâts du DNS et l'échelle des valeurs ainsi que les mesures à prendre.

Parmi ces principes, vous verrez pourquoi PIR est un peu singulier dans le monde des bureaux d'enregistrement, parce que nous publions des rapports de cas d'utilisation malveillante au sein de notre service, avec la fréquence, les cas et le type d'utilisation malveillante, les différentes ordonnances judicaires, tous les détails de ce que nous faisons et comment nous mitigeons ces problèmes.

Nous avons également publié un processus d'appel pour les bureaux d'enregistrement sachant que si nous suspendons un nom de domaine et qu'un bureau d'enregistrement considère que c'était une erreur, ils peuvent remettre en cause cette décision auprès d'une tierce partie neutre. Mais en général, c'est ce que disait Graeme, on prend des mesures proactives et réactives.

Du côté de la réactivité, nous croyons que l'industrie devrait prendre des mesures. On voit des mesures réactives pour supprimer la quantité de réseaux zombie actifs. Ce n'est pas définitif, mais au moins, cela nous donne une idée des problèmes en cours. Et les nouveaux

enregistrements sur la même liste sont également [inaudible] et individualisés pour vérifier s'il s'agit d'un nouveau nom enregistré. Puis, on vérifie s'il s'agit de noms de domaine qui ont été compromis ou s'ils ont été enregistrés à des fins malveillantes pour des activités de mauvaise foi.

Du côté de nos activités proactives, nous avons créé l'indexe de performance de la qualité. Vous aurez peut-être déjà entendu parler de cela : il s'agit d'un programme d'incitation pour les bureaux d'enregistrement où nous avons six critères, y compris la qualification des abus, ce que nous considérons le taux d'abus des bureaux d'enregistrement par rapport aux noms nouvellement enregistrés, l'usage des domaines, entre autres comme critères pour donner aux bureaux d'enregistrement un classement. Si un bureau d'enregistrement a des patrons d'enregistrements sains, l'idée est de leur donner une bonne qualification pour générer une croissance responsable. C'est une espèce d'invitation à s'engager à la lutter contre l'utilisation malveillante du DNS. Donc on essaye vraiment de trouver des moyens pour encourager les parties prenantes à s'impliquer.

Sur ces six critères que nous avons, seul un peut amener à l'échec total et à la disqualification du QPI. Le QPI est un indexe qui a été très utile pour nous et qui nous a montré qu'une quantité de bureaux d'enregistrement ont changé la manière d'utiliser leur patron d'abus. Pour pouvoir recevoir l'incitation financière dont ils bénéficient s'ils ont un bon classement, ils vont améliorer notamment leur performance vis-à-vis de ces six critères. Donc les bureaux d'enregistrement travaillent pour avoir une bonne performance pour être réactifs face à l'utilisation malveillante.

Et pour ceux qui ne peuvent pas se qualifier, ils vont savoir qu'ils ont un désatout concurrentiel, donc ils vont essayer d'améliorer leur classement vis-à-vis de l'utilisation malveillante. C'était le cas avec différents bureaux d'enregistrement qui ont modifié la manière de vendre le .org pour pouvoir être admissibles à cette réduction. Vous pouvez accéder à www.qpi.org et vous trouverez des informations pour que d'autres bureaux d'enregistrement commencent à travailler également.

Nous pouvons parler avec les autres opérateurs de registre souhaitant créer leur propre QPI. À PIR, nous sommes une société à but non lucratif, nous faisons ceci pour améliorer la santé de tout le système de DNS et nous voyons qu'il s'agit d'une bonne pratique commerciale également, non seulement pour nous mais pour les bureaux d'enregistrement. Les bureaux d'enregistrement qui participent à ce programme ont vu une amélioration de 4 % au niveau de taux de renouvellement, ce qui est considérable. Lorsque vous parlez de ce que disait Graeme, de l'état de l'industrie, vu la marge commerciale qu'ils ont, le taux d'accroissement de 4 % au niveau des renouvellements est énorme. On a vu une grande amélioration au niveau des bureaux d'enregistrement. Et ces approches proactives, comme Graeme le disait, me semble-t-il pourraient être un bon moyen pour pouvoir améliorer les approches réactives. Si l'on peut créer et encourager un environnement où l'utilisation malveillante est le concept principal, c'est ce qu'il faut faire.

Je suis là pour répondre à vos questions si vous en avez. Merci.

JOANNA KULESZA : Merci beaucoup Brian. C'est très utile et j'aime beaucoup cette approche pragmatique. J'aime beaucoup le fait que vous mettiez l'accent sur la partie volontaire de ce programme. Au sein d'EURALO, nous avons mis l'accent sur l'impact d'une approche bénévole et ce qui pourrait se passer si l'Union européenne avance dans le cadre de la législation qui a été proposée. Mais nous y viendrons avec Nigel en ce qui concerne le positionnement du GAC et ses préoccupations spécifiques.

Par rapport aux mesures volontaires, du point de vue des opérateurs de registre, je souhaite à nouveau souhaiter la bienvenue à James Bladel, vice-président de la politique mondiale à GoDaddy, qui va nous parler de la perspective du bureau d'enregistrement – donc de GoDaddy – par rapport à l'utilisation malveillante du DNS. Donc sans plus attendre, James, allez-y.

JAMES BLADEL : Merci.

Bonjour à tous. Je suis très reconnaissant pour cette invitation à venir intervenir.

JOANNA KULESZA : Je ne sais pas pourquoi on ne vous voit pas. Votre caméra doit être couverte. On ne vous voit pas.

JAMES BLADEL : Est-ce que ça va mieux ?

JOANNA KULESZA : Ça y est, c'est beaucoup mieux. Et en plus, vous avez mis une chemise de la même couleur que votre fond d'écran.

JAMES BLADEL : Merci beaucoup pour cette invitation. Merci à Graeme et à Brian, qui ont un petit peu donné le contexte. Je peux maintenant à mon tour entrer dans le détail, dans la substance. Tout d'abord, je voudrais revenir sur certaines des choses qui ont été mentionnées dans l'introduction.

C'est un sujet qui prête à controverse, cette thématique de l'utilisation malveillante du DNS. Moi, je ne suis pas tout à fait d'accord. Il me semble simplement que c'est un sujet complexe. Il faut donc reconnaître que le sujet de l'utilisation malveillante du DNS n'a pas une source unique, n'implique pas une seule partie ou un seul secteur de l'industrie pour l'atténuer ; cela nécessite l'implication de différentes entités, de différentes parties. Voilà pourquoi il est important d'impliquer tout le monde, de coordonner le travail de manière à lutter contre l'utilisation malveillante du DNS.

Comme Graeme l'a dit, il n'y a pas de parties contractantes, que ce soit les bureaux d'enregistrement ou les opérateurs de registre, qui soient d'accord pour dire selon moi que les marges sont tellement étroites que les différents acteurs de l'industrie soit ne comprennent pas qu'il y a utilisation malveillante ou qu'ils n'aient pas la possibilité de s'en occuper sur leur plateforme. Ce ne serait que les grandes sociétés qui pourraient faire les investissements nécessaires avec les outils et du

point de vue des ressources humaines. Et même de notre point de vue, il semble que nous sommes toujours à la poursuite des différentes évolutions du problème. Mais je crois que je suis d'accord avec mes collègues : il faut absolument que la démarche concerne tous les acteurs dans le secteur.

Je vais commencer avec une déclaration assez commune qui revient souvent, mais je crois qu'il est important de prendre le temps de faire le travail initial pour définir de manière précise le terme d'utilisation malveillante du DNS. Le cadre qui a été mis en place par les différentes parties est un début de travail dans ce sens. Le DNS Abuse Institute aime bien cette définition, c'est bien, mais je crois qu'en tant que communauté, il faut que nous puissions tous bien comprendre quel est le problème, quels sont les aspects du problème que l'on peut traiter ou pas, que ce soit par des changements de politique, par des bonnes pratiques ou par différents outils tels que les RBL. Je le dis parce que parfois – et je vous dis ceci pour l'anecdote –, on met beaucoup de choses dans l'utilisation malveillante du DNS, cela peut être des litiges commerciaux, des plaintes par rapport à la véracité des informations associées à un site web ou tout ce qui est désinformation ; tous les problèmes finalement de l'intérêt se retrouvent dans cet espèce de melting pot d'utilisation malveillante du DNS. Vous avez sans doute entendu parler du EPDP associé avec le WHOIS et avec la vie privée, donc il est très important d'avoir un consensus sur la définition du problème avant de se lancer dans des solutions.

Je souhaite également mentionner que même si GoDaddy est une société intégrée, nous sommes un bureau d'enregistrement et un opérateur de registre. Nous avons des contrôles institutionnels très

stricts pour séparer ces deux choses. Mais nous considérons qu'il est important de collaborer sur cette question de l'utilisation malveillante du DNS. Et nous cordonnons notre travail à l'interne. En tout cas de notre point de vue, cela nous a permis de souligner certaines différences entre les deux rôles : quel est le rôle de l'opérateur de registre dans ce domaine et que est le rôle du bureau d'enregistrement.

En ce qui concerne le bureau d'enregistrement, je crois que là, on en est à la première ligne de l'utilisation malveillante du DNS puisqu'il y a enregistrement de nom de domaine, il y a très souvent aussi le signalement qui est fait à ce niveau. Donc l'idée est vraiment de faire l'investigation et l'atténuation au niveau de ces signalements pratiquement de manière réactive comme Brian l'a dit étant donné les enjeux de ces problèmes et de la réaction proactive.

Nous avons vu certaines statistiques où 90 % des signalements envoyés aux bureaux d'enregistrement ne sont pas exacts ; soit ils manquent de preuve, soit c'est des campagnes de réseaux sociaux qui signalent un site web spécifique. Et on voit des milliers de signalements de ce type sur un nom ou un site web, donc savoir si oui ou non on peut faire quelque chose, c'est quelque chose d'important. Cela génère énormément de bruit.

L'opérateur de registre a également un rôle. Comme Brian l'a dit, c'est une perspective un petit peu différente. Mais je crois qu'étant donné que l'opérateur de registre n'a pas de relation contractuelle avec l'utilisateur final, sa focalisation est surtout sur la gestion de la performance par rapport à l'abus du bureau d'enregistrement. Donc la perspective de PIR est très encourageante, donc on veut aligner ces

perspectives avec le QPI et d'autres programmes mis en place pour les bureaux d'enregistrement qui encourent ces coûts supplémentaires et qui mettent en place ces différentes étapes de lutte.

Pour ce qui est de l'industrie des noms de domaine... Pardon, je me trompe toujours sur le nom de votre institut, donc le DNS Abuse Institute, la standardisation des signalements et le filtrage de tous ces signalements qui ne mène à rien, on veut s'assurer qu'il y a des preuves et des normes en termes de preuves. Ceci est un travail très important.

Et par rapport aux notificateurs de confiance, il faut bien comprendre que leurs rapports doivent venir d'une organisation qui justement met en place certains critères de manière à ce que le travail puisse être effectué.

Voilà, je crois que c'est à peu près tout ce que j'ai à dire. J'ai hâte d'écouter vos questions. Comme je le disais, l'idée est qu'il faut coordonner le travail. Très souvent, les incitatifs ne sont pas alignées, donc nous devons travailler en tant que communauté pour aider les parties contractantes qui ont les bonnes intentions de traiter le problème mais qui peut-être ne sont pas assez bien informées ou qui n'ont pas les capacités nécessaires. J'écouterai vos questions par la suite. Merci encore pour cette invitation et j'ai hâte d'entendre les autres intervenants.

JOANNA KULESZA : Merci beaucoup James, nous apprécions. Encore une fois, nous essayons d'identifier ce qui est au cœur de l'utilisation malveillante du DNS pour faire avancer la discussion.

Nous allons maintenant passer la parole à Lori. Lori va nous parler au nom de l'IPC, mais il y a aussi l'angle des utilisateurs finaux et je sais qu'elle va également en parler. Toutes ces présentations sont concentrées sur les obligations contractuelles qui sont présentes dans les contrats de l'ICANN. Mais tout le monde a bien dit que c'est aussi un processus ascendant pour assurer la sécurité du réseau. Pour cela, il nous faut le point de vue des utilisateurs finaux. Donc je passe la parole à Lori de l'IPC. Et je sais que Lori va également parler de la démarche réglementaire. Et Nigel y reviendra très certainement. Donc vous êtes un petit peu entre les deux grands sujets Lori. J'ai l'honneur de vous passer la parole.

LORI SCHULMAN : Merci beaucoup. Merci à mes collègues du panel et à tous ceux de l'IPC, de l'ALAC et des autres unités constitutives qui rentrent dans le vif du sujet. Je vois que nous avons 111 participants en plein milieu de cette Prep Week et de l'IGF, donc c'est remarquable et cela nous montre bien à quel point cette question est importante pour la communauté.

James, je suis tout à fait d'accord, le sujet est très complexe. Il n'y a pas de réponse rapide, facile, sinon, cela fait 20 ans qu'on aurait déjà mis en place cette solution. Donc nous sommes dans un monde qui finalement est le même par rapport au fonctionnement du DNS, par rapport à ce qu'il fait, mais le monde a quand même beaucoup évolué parce que nous avons plus d'utilisateurs, plus de personnes qui se préoccupent de la sécurité en ligne. Et les questions qui se présentent dans le domaine de l'internet et de la réglementation sont le résultat du fait que l'internet est une bonne chose. Mais il est important d'avoir des

mesures de sécurité en place. Il est important pour la communauté d'être responsable par rapport à l'utilisation de l'infrastructure du DSN maintenant et pour l'avenir.

Je dois dire qu'au nom de l'IPC, d'une manière générale, en tant que participante à l'IPC, c'est un problème à trois volets. Les intervenants précédents se sont concentrés sur les pratiques volontaires qui est le premier volet. Nous souhaitons avoir des principes qui soient plus stricts, plus prévisibles, qui correspondent aux besoins des utilisateurs finaux. Donc dans cette mesure, je dirais que nous sommes relativement optimistes par rapport aux évolutions, mais il nous reste quelques préoccupations dont je vais parler tout à l'heure.

Je veux également mentionner le travail du réseau de la juridiction de l'internet avec la participation des gouvernements, du secteur privé et des parties contractantes et des détenteurs de propriété intellectuelle. Donc élaborer ces normes, c'est quelque chose de très important, quelle que soit l'option que nous choisissons, contractuelle ou réglementaire. Il faut bien comprendre qu'il y a un élément contractuel à la définition de l'utilisation malveillante du DNS et justement, le problème a été la définition. Cela a déjà été mentionné, il y a beaucoup de définitions de l'utilisation malveillante du DNS, il y a tout ce qui est volontaire, il y a la spécification 11 du contrat des opérateurs de registre et dans le contrat d'accréditation 3.18, il y a également le devoir de faire des investigations et d'avoir les contacts. Donc nous savons que l'abus existe depuis longtemps et il est suffisamment grave, donc ceci doit être intégré dans les contrats. Mais le problème, c'est que veulent dire ces contrats ? Nous n'avons pas suffisamment déterminé ceci du point de vue juridique, il n'y a pas eu suffisamment de litiges pour ce

faire, donc nous comptons sur la communauté pour qu'elle élabore des définitions. C'est là qu'il y a beaucoup de tension parce que du point de vue de la propriété intellectuelle, l'utilisation malveillante des noms va plus loin que les définitions limitées que nous avons. La communauté considère ceci comme un continuum de mauvaises actions donc il est important de reconnaître ce continuum. Et du point de vue de la propriété intellectuelle plus spécifiquement, nous souhaitons voir tout ce qui est piratage, infraction aux marques de commerces reconnues parce que ceci est très important dans le thème du hameçonnage, des réseaux zombie, etc.

Il y a une solution simple et nous savons que l'industrie comprend cela et y répond. Mais il reste énormément à faire du côté réglementaire et je pense qu'il serait important que Nigel apporte cette perspective législative, les résultats, les propositions. Nous savons que l'Union européenne dans ce sens a eu un rôle d'importance pour établir les paramètres dans le dialogue et l'accès aux informations par rapport au WHOIS. Dans énormément d'autres juridictions, il y a l'accès aux données qui est fait valoir, alors que la réglementation n'est pas bien comprise ou qu'elle est trop générale, le gouvernement finit par essayer de corriger les mesures possibles. C'est ce que nous essayons de faire en ce moment avec le directeur de l'Union européenne.

À l'Union européenne, il y a une étude qui a été demandée qui est très exhaustive. Il y a eu énormément d'ateliers, nous y avons participé avec nos collègues dans le but de comprendre ce qu'implique l'utilisation malveillante du DNS et la manière de la gérer. Du point de vue gouvernemental, nous serions favorables à une solution réglementaire, mais je vois qu'on a ces trois implications des réglementations qui sont

volontaires et réglementaires et qui finalement ne permettent pas de résoudre ce problème.

Alors que fait l'IPC ? C'est la question suivante. L'IPC a créé une équipe de réponse à l'utilisation malveillante. C'est la première fois qu'on a une telle équipe. Elle a été très active à la contribution au travail de l'ICANN avec des commentaires et des contributions. Nous avons à présent un groupe que je dirige qui vise à fournir des réponses plus concrètes aux mesures volontaires avec les documents qui ont été formulés par nos collègues. Nous essayons de donner des réponses, nous essayons également de participer aux réunions, de comprendre ce qui y est dit. Et nous sommes contents de voir qu'il s'agit d'un groupe qui est très impliqué. L'une des principales préoccupations des propriétaires est de voir que les pratiques qui sont discutées ne prennent pas en considération la perspective du titulaire ou pas autant qu'ils le devraient. Donc nous sommes prêts à nous mettre au travail, à nous retrousser les manches pour essayer de trouver des solutions pratiques si possible et pour aider la communauté à rester sur la bonne route pour pouvoir continuer à avoir un système de DNS qui fonctionne pour les 20 prochaines années. C'est ce qui est important.

Dans mon organisation, nous avons créé une boîte à outils sur le DNS et je partagerai le lien pour y accéder à la fin de la présentation. Mais cet outil du WHOIS a été créé pour les titulaires de propriété intellectuelle qui souhaiteraient devenir des bureaux d'enregistrement ou des opérateurs de registre. Nous savons qu'il y a des informations qui doivent être envoyées, mais ils ne savent pas quand et ce qui est approprié. Alors ici, nous sommes là pour contribuer à comprendre quel

est le but de ces plaintes et quelles devraient être les conventions de service et les niveaux acceptables.

Et bien sûr, ce dont personne ne parle est l'accès aux informations sur le WHOIS. Il s'agit d'une question où l'on a vu quelques progrès qui ne suffisent pas. Donc même si l'on voit des informations énumérées qui sont envisagées par toutes les lois, la situation reste très obscure. C'est une question controversée et nous essayons de défendre le besoin d'équilibre, de garantir la protection du droit et de la liberté des personnes tout en protégeant les utilisateurs de la fraude. Il y a énormément de personnes qui sont lésées par cela, par l'information compromise, des noms qui sont utilisés à des fins malveillantes.

Et finalement, le principal résultat de ce que nous voyons dans l'interprétation du RGPD et d'autres règles de confidentialité, c'est que les forces d'application de la loi elles-mêmes ne peuvent pas accéder aux informations, ce qui cause un énorme problème. Là aussi, les agences d'application de la loi font partie d'autres initiatives de grande importance et c'est le fait que le secteur privé et le secteur public doivent travailler ensemble pour s'entraider dans le cas des enquêtes et fournir des informations lorsque cela s'avère possible.

Voilà pourquoi il me semble que l'on doit redresser cet équilibre. Et je voudrais que cela soit davantage incorporé. Nous sommes là pour vous aider, nous sommes prêts à discuter. Nous participons aux activités de cadrage, nous avons le document qui a été publié et nous espérons pouvoir avancer dans ce sens. Mais nous avons des négociateurs et des personnes qui nous accompagnent aujourd'hui que je vois connectés qui sont véritablement épuisés parce que nous avons un peu avancé par

rapport à l'action de mettre en œuvre vis-à-vis d'un système SSAD, mais on ne sait pas ce que cela va donner, quel en sera le coût, quels seront les délais. Et c'est l'obligation de toutes les parties contractantes de divulguer les informations qui devraient l'être.

Et je vais m'arrêter là. Merci.

JOANNA KULESZA : Merci beaucoup Lori. J'adore lorsqu'on nous parle de l'utilisation malveillante avec autant de passion que vous, donc merci.

Je suis là en tant que modératrice et je ne pourrai pas faire de suggestions sur des opinions et je ne peux pas ajouter des commentaires sur le chat, mais ce que vous signalez Lori est le fait que la préoccupation que le système ne fonctionne pas bien sur le terrain est une préoccupation commune à différentes parties prenantes. L'étude sur l'utilisation malveillante du DNS qui a été demandée par la Commission européenne reflète très clairement ce souci qui pourrait également être reflété dans une loi proposée.

Ce n'est pas tout simplement la directive du NIS ni le RGPD qui ont donné tant de maux de tête à la communauté de l'ICANN, mais il y a également la loi des services numériques sur laquelle nous nous sommes centrés au sein d'At-Large et d'EURALO lors de la table ronde précédente. Il y avait également le Conseil de l'Europe qui semblait avoir hâte au cours du processus de EPDP et qui a proposé un nouveau protocole supplémentaire qui s'ajoute à la convention qui pourrait soulever des préoccupations, surtout au niveau de l'accès aux informations par les forces d'application de la loi.

J'évite encore une fois de changer de rôle, je reste modératrice et j'invite Nigel Hickson – merci de nous avoir rejoints. Je sais que Chris Lewis-Evans est également connecté aujourd'hui. Je suis prête à vous permettre de participer tous les deux. Nous ne vous demandons pas de parler au nom du GAC, mais plutôt d'apporter un peu de lumière sur les discussions vis-à-vis de l'utilisation malveillante du DNS que vous tenez au sein du groupe. Chris copréside le groupe de travail du GAC sur la sécurité publique, groupe avec lequel l'At-Large a échangé beaucoup au cours du temps. Alors sur ce, Nigel, je vous cède la parole et je veux vraiment voir ce que vous allez apporter à ce débat. Merci.

On m'a demandé de parler lentement. J'essaie de parler lentement. Et je vous transmets cette demande. Merci. Nigel, vous avez la parole.

NIGEL HICKSON : Merci beaucoup Joanna. C'est un véritable plaisir. C'est Chris qui va commencer et il va parler aussi lentement que moi.

CHRIS LEWIS-EVANS : Merci Nigel. Bonsoir à tous.

Comme le disait Nigel, nous allons nous diviser plutôt que de porter deux casquettes. Moi, je vais parler de la sécurité publique et Nigel partagera le point de vue gouvernemental vis-à-vis de l'utilisation malveillante du DNS.

À ce sujet, qu'entend-on par cette formule du point de vue de la sécurité publique ? Pour nous, il s'agit d'activités qui portent un dommage pour les personnes qui utilisent l'internet et pour ceux qui

l'utilisent à des fins commerciales. Lorsqu'on parle de dommages, on parle de faillite d'une entreprise, d'un coût que cela pourrait impliquer, de services qui pourraient nuire aux gens en raison de cette utilisation malveillante.

Quel est le lien de cela avec l'utilisation malveillante du DNS ? Quel est le lien entre ce terme défini de l'utilisation malveillante du DNS et le reste ? Comme Brian et Graeme l'ont dit, le terme de cadre d'utilisation malveillante comprend un grand pourcentage des dommages des entités de délinquants qui utilisent le DNS pour générer un profit pour eux mais qui sont également nuisibles pour les utilisateurs. Comme Graeme le disait, l'approche à ce qui appartient à ce cadre pourrait nous permettre d'arrêter en une bonne mesure ce que nous voyons comme utilisation malveillante et nous essayons d'éviter ces dommages.

Comme Graeme le disait, il y a également des noms qui sont compromis qui ne sont enregistrés à des fins malveillantes. On voit surtout l'effet que cela a sur les victimes, mais cela comprend des personnes qui sont les titulaires de noms de domaine qui se sont vues enlevé la propriété de leur nom de domaine qui a été usurpé par quelqu'un d'autre à des fins malveillantes. Le PSWG travaille pour essayer de former les agences d'application de la loi à la manière de créée les meilleures normes pour les preuves et pour permettre aux bureaux d'enregistrement et opérateurs de registre de prendre des mesures qui permettent d'arrêter l'utilisation malveillante du DNS en ligne.

Nous comprenons qu'il peut y avoir une suspension temporaire d'un domaine compromis. Même cela aura un impact, cela peut être la bonne option si ce domaine crée de multiples victimes. Donc cela peut

être une option, mais on ne peut choisir cette option qu'en ayant suffisamment de preuves. L'orientation des discussions au cours des deux dernières années a été vraiment d'avoir des systèmes beaucoup plus cohérents de manière à avoir des activités efficaces et proactives. Elles ne sont pas préventives, ce serait idéal, mais il faut au moins que ces actions se fassent rapidement. L'éducation est vraiment clé pour protéger les victimes qui ont un domaine compromis, donc je crois que ceci est une grande partie de notre travail. Il ne faut pas l'oublier parce que ceci a un impact sur tout le système.

Pour revenir à la prévention, je crois que là, c'est une fonction législative et Nigel le mentionnera sans doute, Joanna l'a évoqué également, donc voir ce que l'on peut faire du point de vue législatif pour permettre des actions plus préventives et également la Convention de Budapest peut-être permettra d'élargir l'espace sur lequel nous pouvons agir. C'est un mécanisme international qui existe, donc cela est vraiment compliqué d'agir au niveau de la sécurité publique sur les législations. Donc avoir les bons outils est très important de manière à pouvoir agir avec les compagnies d'hébergement, les fournisseurs de services, les opérateurs de registre et le bureaux d'enregistrement, non seulement pour agir mais pour également stopper les préjudices, ce qui est très important.

Et je crois que justement, être en lien, le GAC, le PSWG, c'est très important pour avoir un impact direct sur ce que nous faisons dans le domaine de l'utilisation malveillante du DNS. Donc nous espérons que nous pourrons continuer dans ce sens grâce au modèle multipartite de l'ICANN. Ceci est selon nous très important pour le GAC et pour les

autorités d'application de la loi. Cela nous semble essentiel pour faire évoluer la situation.

J'espère que je n'ai pas utilisé tout le temps que nous avions. Nigel, je vais quand même vous passer la parole rapidement. Et quoi qu'il en soit, je suis prêt à répondre à vos questions par la suite.

NIGEL HICKSON : Merci beaucoup Chris. En fait, vous avez bien fait d'utiliser tout le temps que j'avais. Comme ça, je ne me fatiguerai pas trop. Mais merci Joanna.

Pour moi, c'est une question extrêmement importante. Je crois que je suis la dernière personne. Je n'aurai jamais pensé en fait être passionné par rapport à l'utilisation malveillante du DNS et ce n'est pas parce que c'est une utilisation malveillante du DNS, mais c'est parce qu'il nous faut absolument trouver une solution. Ce qui me passionne en fait, c'est l'ICANN. Ce qui me passionne, c'est le modèle multipartite. Ce qui me passionne, c'est la gouvernance de l'internet. Et nous avons un rôle clé dans tout ceci parce que vous savez, les gens nous observent, le monde entier regarde l'ICANN et ce que nous faisons. Les législateurs nous observent et nous devons avancer.

Mais nous avons déjà avancé, il faut le dire. Il semblerait que nous comprenions mieux ce que nous souhaitons faire, il y a énormément de bonne volonté, il y a énormément d'activités dans les différents espaces de la communauté. Aujourd'hui, nous avons entendu parler de l'excellent travail des parties contractantes et d'autres en ce qui concerne les notificateurs de confiance, nous avons entendu parlé du DNS Abuse Institute et l'excellent travail qui est effectué. Nous avons

entendu parler du travail dans le réseau ING – j'y ai un peu contribué d'ailleurs. Et ces contributions sont excellentes. Ce sont des membres de la communauté de l'ICANN qui sont impliqués d'ailleurs.

Pourquoi sommes-nous toujours là où nous en sommes ? Pourquoi est-ce que nous continuons de parler de ces questions plutôt que de parler des actions spécifiques ? Nous avons les données, nous avons le DAAR – j'ai toujours du mal avec ce mot – donc l'excellent travail que l'ICANN a effectué pour fournir des données. Alors comment allons-nous maintenant progresser ? En tant que communauté, comment nous allons répondre ? Est-ce qu'on va toujours être là dans trois ou quatre ans au sein d'une séance plénière à échanger nos points de vue ou alors est-ce que nous allons réellement avancer comme Lori et d'autres l'ont dit ?

Donc je crois qu'il faut absolument avancer. Je ne parle pas au nom du tout le GAC, mais je crois que pour beaucoup d'entre nous au GAC, nous avons les mêmes expériences. Nous avons les gouvernements, nous avons les ministres qui reçoivent des lettres régulièrement. Au Royaume-Uni, nous avons le *Daily Mail* qui publie des lettres des différentes unités constitutives, des différents lecteurs. Donc ceci met en jeu la nature même du système de noms de domaine. La question, c'est comment se fait-il qu'un site web qui est par exemple censé vendre des gâteaux ou quoi que ce soit puisse être subtilisé pour diffuser des images pornographiques ou pour avoir une action malveillante de fraude ? Comment se fait-il qu'un site qui est prêté de manière légitime ou qui est enregistré de manière légitime et qui fait quelque chose de tout à fait légitime est soumis à un réseau zombie ou autre activité malheureuse ? Comment se fait-il que l'ICANN ne puisse

rien faire ? Ce sont les questions des ministres et nous devons avoir des réponses.

Donc comment procéder ? Comment avancer ? Comment allons-nous ensemble solutionner ces problèmes. Très souvent, nous avons parlé d'un PDP sur l'utilisation malveillante du DNS, nous avons parlé d'autres solutions éventuelles. Certes, il y a d'énormes problèmes par rapport au processus d'élaboration des politiques, par rapport à la longueur du processus, par rapport au nombre de volontaires et par rapport à toute l'énergie qui serait requise. Et je crois que beaucoup d'entre nous au GAC en sommes tout à fait conscients.

Mais quelles sont les autres méthodes que nous avons ? Faut-il former un groupe de travail intercommunautaire peut-être ? Faut-il résoudre ce problème dans le cadre de ce groupe intercommunautaire ? Ou alors est-ce que l'ICANN devrait former un groupe qui regarde les obligations contractuelles qui existent actuellement et travailler de ce point de vue ? Je ne sais pas, mais ce que je vous suggère, c'est qu'il nous faut faire quelque chose maintenant. Il faut être positif, il faut être très clair, articuler clairement les choses.

Nous avons fait la transition de l'IANA, nous sommes la communauté de l'ICANN – ce n'est pas moi, c'est vous. Moi, je faisais simplement partie du personnel de l'ICANN à l'époque. Mais nous avons fait des choses extraordinaires. Les gens se souviennent de l'ICANN pour ce que l'ICANN a fait dans le cadre de ce modèle multipartite, donc nous devons encore une fois répondre à cet enjeu et nous montrer à la hauteur de l'enjeu.

JOANNA KULESZA : Merci beaucoup pour cet appel à l'action, mais je dois noter que Graeme, Brian et d'autres ont déjà parlé de toutes les activités qui sont en cours, donc j'écoute votre commentaire comme en fait un encouragement à aller plus loin pour s'assurer que les politiques soient vraiment complètes et efficaces de manière universelle.

Merci à tous pour cette excellente contribution. Le travail de Jonathan est maintenant très compliqué parce qu'il ne nous reste que peu de temps, mais nous avons quand même collecté les questions, et Jonathan les a. J'espère qu'il va les résumer et les communiquer à nos intervenants sous un format synthétique. Donc je passe la parole à Jonathan qui va s'occuper de la partie questions et réponses. Et à la fin, Olivier résumera. Jonathan, j'espère que votre vidéo fonctionne, votre audio aussi. J'espère que vous m'entendez. Allez-y.

JONATHAN ZUCK : Merci Joanna.

Merci à tous pour cette discussion. Je vais essayer de vous poser les différentes questions qui ont été mises dans le chat, et je vais essayer en fait de les faire ressortir de manière synthétique.

La première question, c'est qu'il semblerait qu'il y a une dynamique assez étrange entre la communauté de l'ICANN et les parties contractantes d'un côté parce que tout ce qui pour nous est une réforme ou un changement de politique, une proposition au niveau des parties contractantes avec une activité à basse marge avec une certaine résistance de l'appel à l'action que Graeme a mentionné et de l'autre côté, nous avons l'ICANN qui investit énormément d'argent dans tout

cela. Et pourtant, il y a des preuves évidentes comme quoi ces outils ne sont pas aussi efficaces qu'ils pourraient l'être.

Donc le DAAR va être révisé, il y a une période de commentaires publics qui va bientôt être lancée sur le DAAR. Donc la question que je me pose, c'est si la générosité du PIR qui a créé cet institut ne réplique pas certaines des fonctionnalités dont on a déjà parlé au sein de l'ICANN. Ce système centralisé pour les plaintes, c'est un petit peu comme le SSAD semblerait-il auquel on a pensé pendant le EPDP, donc la possibilité de mieux faire le suivi, de créer un système de suivi ; ceci me semble étrange dans le contexte du DAAR. Comment se fait-il qu'il y a cette distance entre les outils que l'ICANN a cherché à créer pour aider et les outils pragmatiques dont la communauté a besoin ? Comment faire dans ce contexte ? Il existe des ressources, donc il semblerait que ces ressources ne correspondent pas nécessairement aux besoins. Donc c'est une question que je pose aux panelistes qui peut-être souhaitent y répondre, en particulier Graeme je pense. Donc cette question de répéter les initiatives me semble un petit peu malheureuse.

GRAEME BUNTON : Vous m'avez donné beaucoup de choses à penser.

L'utilisation malveillante du DNS, c'est quelque chose qui dépasse l'ICANN ; cela va au-delà des opérateurs de registre et des bureaux d'enregistrement. Nous ne sommes qu'une partie d'un puzzle. Et James en a parlé un petit peu, moi non, j'ai parlé des bureaux d'enregistrement et des opérateurs de registre dans le contexte économique, mais les gens qui sont malveillants sur l'internet sont parfois des gens simplement dans leur sous-solution qui sont vraiment

de tout petits acteurs, mais il y a aussi les gangs, les organisations criminelles, le crime organisé qui ont énormément d'argent et de ressources à leur disposition. Donc lutter contre individuellement est impossible, donc voilà pourquoi il nous faut des solutions collectives.

Le DAAR par exemple, à la base, c'est une preuve de concept de collecter des abus et ensuite de signaler. Mais cela ne fournit aucune information pour que les gens puissent agir. Donc je crois qu'il y a plusieurs raisons à cela. Il existe depuis un certain nombre d'années, donc cela nous prouve que c'est possible. Mais il y a aussi le problème de la conception de l'ICANN, le problème des contrats, donc il faut faire très attention.

Je tire l'enseignement du DAAR. Il y a quelque chose qui existe, cela fonctionne. Maintenant, peut-être qu'on peut faire les choses plus rapidement et mieux de manière à fournir davantage d'informations plus utiles et plus valables. Donc je crois que c'est vrai par rapport à ces initiatives entre l'ICANN et la communauté. Le travail de l'ICANN, c'est peut-être de dire : « Nous croyons que ceci est utile et bon. » Mais la mission de l'ICANN ne couvre pas tout l'internet. Et ces problèmes justement sont transfrontaliers pour ainsi dire. C'est un petit peu comme le DNS Abuse Institute, donc il faut tirer les enseignements et voir ce que nous pouvons faire pour entrer en lien avec les compagnies d'hébergement, les opérateurs de registre, les bureaux d'enregistrement, les fournisseurs de contenu, les RIR, etc. Donc il y a différents éléments et ils ont tous un rôle à jouer dans l'écosystème de l'utilisation malveillante du DNS.

J'espère que j'ai à peu près répondu à votre question. J'imagine qu'il y a d'autres points, mais je vais quand même vous repasser la parole, Jonathan.

JONATHAN ZUCK : Merci Graeme.

Je pense que pour moi, il est raisonnable de faire cette distinction entre pilote et mise en œuvre. Devrait-on dire à l'ICANN d'arrêter les investissements au DAAR ou, au lieu d'investir dans un système similaire, ne devriez-vous pas plutôt orienter l'ICANN ? Parce que je sens qu'on a un doublon ici qui représente un gaspillage de ressources, et c'est le département des parties contractantes finalement qui verse ces fonds-là.

Donc on en a beaucoup discuté avant, vous avez dit que vous avez un coût élevé qui est associé à l'analyse de la prévisibilité. Et il y a énormément de chambre des parties contractantes qui n'ont pas les ressources pour y investir. Le DNS Abuse Institute ou l'ICANN ou les deux ensemble ne pourraient-ils pas potentiellement permettre d'avoir des données analytiques du web comme investissement potentiel ? N'y a-t-il pas un meilleur usage des ressources que de les destiner à ce projet ?

GRAEME BUNTON : Oui, vous avez probablement raison. L'outil de signalement centralisé que nous avons l'intention de développer, si on pouvait être aussi agressif dans notre approche et que l'on pouvait développer cela avec le soutien de l'ICANN, ce serait l'idéal, que ce soit une obligation

contractuelle ou une politique qui contraigne les parties prenantes de devoir suivre ces politiques qui sont appuyées par communauté par exemple, entre autres. Ce serait génial. Donc la communauté, l'institut et tous les autres pourraient avancer dans la réduction de l'utilisation malveillante du DNS. Mais nous n'avons pas d'exemples de cela pour l'instant. Et je pense qu'il est vrai qu'il y a par rapport au DAAR un doublon d'efforts de travail. Oui.

JONATHAN ZUCK : Comme projet pilote, ne devrait-on pas reconnaître que le DAAR soit arrêté ? Il y a une consultation publique en ce moment. Devrait-on le proposer ?

GRAEME BUNTON : Je ne vais pas répondre à cela. Je vais céder l'honneur à Brian.

BRIAN CIMBOLIC : Je pense que le DAAR est devenu un outil brillant, mais qu'il n'était pas censé pouvoir être mis en œuvre du côté des bureaux d'enregistrement et des opérateurs de registre qui ne pourraient jamais dire : « Nous avons identifié 10 000 domaines qui ne suivent pas cela, qui font un usage malveillant. » Ce n'est pas cela. L'utilisation du DAAR est comme essayer d'utiliser un tournevis pour marteler sur quelque chose ; cela pourrait vous aider mais ce n'est pas à cette fin que l'outil a été créé. Le DAAR existe comme fiche de santé générale de l'espace des gTLD. Les rapports n'arrivent même pas au niveau des opérateurs de registre et il n'y a rien dedans qui puisse être mis en œuvre pour nous donner une idée de notre situation en général.

Donc si on pouvait reconnaître son usage limité et si on reconnaissant l'usage limité sans essayer d'extrapoler et de résoudre les problèmes compliqués avec un outil aussi limité, je pense qu'on verrait bien quelle est sa valeur sans essayer de faire autre chose.

JONATHAN ZUCK : D'accord, merci.

Une autre question qui apparaît dans le chat porte sur la disponibilité des informations des données qui sont collectées par ce système. Je pense que c'est une question pour Graeme parce qu'on demande à quelle fin sont collectées ces données. Mais c'est également une question pour James et pour vous par rapport aux fins escomptées. On finit par parler de plaintes et de ce que vous informez. On a les demandes de conformité, les demandes de DAAR pour pouvoir en dériver des informations qui auraient un impact sur le comportement des acteurs malveillants avec le haut niveau de plaintes, avec les temps de réponse, etc. Serait-il possible à ce moment-là que les informations soient mises à disposition dans un programme de confiance ou autre ?

GRAEME BUNTON : Merci Jonathan. C'est une bonne question.

J'en parlerai très rapidement du point de vue de l'institut, parce que nous considérons le développement d'une solution centralisée pour l'industrie qui puisse être utilisée lorsque cela est nécessaire mais également d'un outil qui permette de comprendre l'utilisation malveillante lorsqu'elle a lieu ou du point de vue des opérateurs de registre et des bureaux d'enregistrement avec des preuves et tout ce

qu'il faut. J'en parle sur le site web de l'institut en davantage de détails, donc allez voir notre feuille de route qui comprend énormément de détails.

Mais je pense énormément à la manière de mettre tout cela en rapport. Mais pour l'instant, ce n'est pas possible parce qu'il nous faut un système de signalement robuste indépendant et transparent sur l'utilisation malveillante du DNS et un système qui puisse prendre ces plaintes et les transmettre là où on en a besoin. Donc si on pouvait utiliser ces mêmes données pour pouvoir créer une opinion publique, ce ne serait pas véritablement réaliste. Donc il faut faire attention à la manière d'utiliser ce système. Pour l'instant, je ne vois pas que ce soit possible de les mettre en rapport.

JONATHAN ZUCK : D'accord, merci.

Oui, Lori.

LORI SCHULMAN : Je voulais apporter mon opinion ici parce que je pense que c'est une question de portée également. Le cadrage du DAAR est limité. On ne peut pas savoir quelle en est la portée et on finit par avoir des problèmes pour essayer de transmettre cette idée, de montrer le fonctionnement. Les gens demandent des données, on a différents rapports à chaque fois avec énormément d'informations et je pense que le problème plutôt que la définition est de faire confiance à la source des données que nous avons.

Donc si on continue à remettre en cause les données de chacun, je ne sais pas si on pourra faire confiance aux différents processus, au processus de l'ICANN, au CPI. On ne saura autrement pas quelle est l'importance des données si on ne fait pas confiance aux sources. Comme vous le savez Jonathan, on travaille à la révision du CCT RT, qui finit par être chère. Les rapports par exemple ne disent pas toujours la même chose. Et les rapports deviennent trop compliqué parce qu'on n'a pas trouvé d'accords universels de comment on devrait procéder. Donc je ne pense pas que l'on puisse définir l'utilisation malveillante si on ne peut même pas définir la portée de ce qui nous occupe.

JONATHAN ZUCK : Merci Lori. Les données sont définitivement un problème ici. Donc à chaque fois que quelqu'un parle de la création de données, tout le monde veut accéder à ces données. Donc oui, c'est la question constamment. Et lorsque les données sont présentées, elles sont présentées de manière modifiée et les autres finissent par ne pas y confiance.

J'ai une liste de personnes souhaitant intervenir, mais je voulais poser une question à James. Une partie de ce qu'on voit est qu'il y a des bureaux d'enregistrement plus grands que d'autres et qui ont par conséquent plus de possibilités de se conformer à une pratique ou autre et que les meilleures pratiques ont été remplacées par les règlements qui sont apparus. Alors auriez-vous une idée de la situation des personnes qui participent à l'industrie mais dont on n'entend pas beaucoup parler et qui prennent des mesures qui intègrent ces

mesures, qui essayent d'avoir une influence sur les meilleures pratiques ? Est-ce que vous pouvez élaborer ?

JAMES BLADEL : Merci Jonathan.

Je vais donc sauter la queue, désolé Chris.

JONATHAN ZUCK : Oui, mais on ne va pas vous permettre de poser votre questions, c'est pour que vous répondiez à ce que je viens de vous demander.

JAMES BLADEL : Oui, c'était en fait pour rebondir sur ce que disait Lori.

Mais en fait, c'est un défi. On voit des personnes qui changent de trajet à mi-chemin. Il y a des personnes qui se sont impliquées davantage pour voir comment collaborer. Mais cela fait partie du grand problème que nous avons dans l'industrie, et c'est le fait qu'il va y avoir des personnes qui répondent beaucoup, qui s'impliquent, qui participent aux réunions de l'ICANN, qui ont des idées, qui ont une influence sur la prise de décision, et il y a une liste énorme de fournisseurs plus petits qui ne sont pas prêts ou qui ne sont pas en mesure de pouvoir se conformer à ces engagements.

Et d'après ce que nous voyons dans ce que décrivait Brian au sein de la CPH, au sein du DNS Abuse Institute, dans le cadre et dans les initiatives du projet de juridiction internet, on essaie de pouvoir rabaisser cette ligne limite pour que même ceux qui ne sont pas à la hauteur de cette

échelle d'atténuation de l'utilisation malveillante du DNS puissent également s'impliquer pour que tout le monde puisse agir sur un pied d'égalité.

Je pense qu'il va toujours être difficile et qu'il y a différentes réalités que la communauté doit affronter, entre autres le fait qu'on n'a pas un seul point où trouver l'origine du problème pour essayer de le résoudre.

Mais il y a également différentes dimensions et différents aspects de ce problème qui existent en dehors de la mission de l'ICANN. Ce domaine particulier pourrait peut-être devenir un petit peu plus amer pour les acteurs malveillants. Mais il y a également des problèmes sociaux, intergouvernementaux, juridictionnels, tout type de chevauchements dont nous pourrions parler à l'ICANN mais qui, depuis notre point de vue, ne peuvent pas être modifiés. Je reviens toujours sur la définition et il faut que l'on comprenne que la partie de ces problèmes qu'on ne peut pas résoudre, les réseaux zombie par exemple, peut être adressée très différemment du hameçonnage en tant que problème, donc il se pourrait que l'on doive avoir différents processus et différentes politiques pour chacun.

Et dans le cas des PDP, on a des politiques et des procédures internes pour les parties contractantes qui pourraient évoluer trois ou quatre fois dans la durée d'un même PDP qui est ouvert également. Mais les PDP n'avancent pas suffisamment vite, donc on essaie de trouver quel est le bon moyen et quelle est la bonne école pour résoudre ces problèmes. Et à chaque fois, on revient sur la question et c'est le fait qu'on pourrait être plus rapides, plus efficaces.

Alors je ne sais pas si j'ai bien répondu à la question, mais en tout cas, l'objectif est de faire en sorte que la fin de la liste puisse s'intégrer et être plus efficace et mieux s'adapter ou faire en sorte qu'ils puissent collaborer davantage avec l'ICANN.

JONATHAN ZUCK : Merci James.

On n'a vraiment plus de temps. Je vais clore la liste d'intervenant après Chris Lewis. Christopher, vous n'allez pas pouvoir prendre la parole. On va voir comment répondre à votre question à la fin de cette activité. Chris Lewis, vous souhaitez prendre la parole ? Après vous, je cèderai la parole à Olivier.

CHRIS LEWIS-EVANS : Oui, j'irai très rapidement. C'était pour rebondir sur ce qu'ont dit James et Lori.

Il n'y a pas de panacée ici, on n'a pas de données qui fassent autorité ou on n'a pas autrement de système DAAR qui existe ou de mécanisme transparent de collecte de données qui nous permette de voir quel est l'effet des différents cadres volontaires. Il serait utile de les avoir et d'avoir un bon moyen pour enregistrer ces informations ; cela nous aiderait énormément.

Merci.

JONATHAN ZUCK : Merci Chris.

Joanna m'a demandé de céder la parole à Olivier. Hélas, Olivier, vous n'avez pas de temps, mais si vous avez des remarques finales ou des leçons que vous avez tirées, allez-y.

OLIVIER CRÉPIN-LEBLOND : Merci beaucoup Jonathan. Je suis sur Adigo, je vais mettre ma vidéo pour que vous me voyiez quand même. Mais quelques points.

Nous avons appris beaucoup aujourd'hui. Je pense que la discussion a été très utile.

La première chose sur laquelle nous avons commenté, c'est que l'utilisation malveillante du DNS est une partie des utilisations malveillantes que l'on voie. Donc le malware, le hameçonnage, le spam, etc. ; tout ceci existe. Et la plupart des données – Graeme vient de nous en parler – d'utilisation malveillante nous viennent des listes de blocage et de réputation qui parfois voient les choses un petit peu différemment. Ce n'est pas l'atténuation mais c'est plutôt interrompre.

Les opérateurs de registre et les bureaux d'enregistrement font de leur mieux dans ce domaine de l'utilisation malveillante du DNS, mais parfois, ils ne peuvent pas agir, ils n'ont pas les bonnes informations nécessaires pour agir.

Brian du PIR nous a parlé de la quantité de travail effectué au niveau des parties contractantes pour atténuer l'utilisation malveillante du DNS, dont le renforcement des capacités auprès des parties contractantes. Il y a un travail qui a été effectué pour promouvoir des principes au sein de la chambre des parties contractantes.

Le PIR a également lancé différents programmes pour motiver les différents bureaux d'enregistrement à avoir des domaines de qualité. Ils utilisent pour ceci l'indice de qualité qui a été très bien accueilli. C'est un programme volontaire pour améliorer la façon dont les bureaux d'enregistrement travaillent.

James nous a parlé de l'importance de bien définir l'utilisation malveillante du DNS. Pourquoi ? Parce que parfois, nous mettons beaucoup de choses dans l'utilisation malveillante du DNS, les litiges commerciaux, etc. et en fait, les bureaux d'enregistrement n'ont aucun contrôle sur tout cela. Donc il nous faut bien nous comprendre là-dessus. Lorsqu'on considère le nombre de rapports qui arrivent aux bureaux d'enregistrement, 90 % des rapports ne sont pas exploitables et il y a beaucoup de bruit et auquel on est soumis. Aussi, étant donné que le registre n'a pas de contrat avec les utilisateurs finaux, il est difficile d'agir. Le travail du DNS Abuse Institute, dans le filtrage de ces rapports pour s'assurer qu'ils sont de qualité, c'est quelque chose qui serait utile.

Nous avons également écouté Lori Schulman de l'IPC qui a dit que l'internet était très bien, mais il faut absolument avoir des limites et agir de manière responsable. Ce n'est pas simple, l'Union européenne a défini des paramètres par rapport au WHOIS, par rapport à l'accès des informations. Donc pour Lori à l'IPC, l'un des plus gros problèmes, c'est justement cet accès aux informations. Il faut que les démarches soient volontaires, contractuelles et il faut également des réglementations au sein de l'industrie. L'IPC est en train de mettre en place une réponse et elle apprécie les méthodes inclusives d'atténuation du DNS. Mais l'accès aux informations, c'est important, nous l'avons vu récemment lors du

EPDP sur les questions du WHOIS relatives au RGPD, il n'y a pas nécessairement tout l'équilibre que l'on souhaite voir.

Chris Lewis-Evans du PSWG du GAC a mentionné qu'il y avait beaucoup de préjudices suite à cette utilisation malveillante du DNS, les pertes commerciales, et c'est beaucoup plus que simplement quelques problèmes. Donc le groupe sur la sécurité publique essaie de voir avec les autorités d'application de la loi des meilleures approches, des normes adéquates. Avoir suffisamment de preuves est particulièrement important, surtout que ce réseau est mondial, donc les lois et initiatives nationales ne suffisent pas. Donc pouvoir travailler avec les opérateurs de registre et les bureaux d'enregistrement ainsi que les prestataires de service d'hébergement est quelque chose d'important dans le cadre du modèle multipartite.

Et Nigel Hickson, représentant du Royaume-Uni au GAC, a souligné l'importance de ce travail multipartite qui est effectué à l'ICANN. Et il suggère qu'on devrait peut-être aller plus loin parce que l'ICANN certes inclut les gouvernements, mais les journaux, la presse, souvent pointent du doigt les sites qui ont été subtilisées et les gens se disent : « Comment cela se fait-il ? Pourquoi le gouvernement ne fait rien ? » Donc il y a vraiment une pression sur la communauté de l'ICANN pour travailler là-dessus.

Questions et réponses. Il y a plusieurs questions qui ont été posées. Premièrement, tout ce qui est relatif au fait que l'utilisation malveillante du DNS dépasse l'ICANN. Puis ce n'est pas des petits problèmes, de petits acteurs mais parfois de la criminalité organisée qui est impliquée et qui représente une réelle menace.

Le DAAR, ce n'est pas une solution, c'est un projet qui ne fournit pas suffisamment de détails. Donc en tant que démonstration de faisabilité, c'est une bonne chose, mais il faut encore y travailler, peut-être pour que le DAAR soit utilisé plus largement avec une plus grande publication de données. Pour l'instant, c'est un outil qui brille mais qui n'est pas forcément exploitable. Cela veut donc dire qu'il est limité.

On parlait d'un portail de plaintes, Graeme en a parlé. Il y travaille dans son institut, donc une plateforme d'accréditation pour les bureaux d'enregistrement et les opérateurs de registre, peut-être aussi avoir des moyens de signalement robustes. Mais ceci ne fonctionnera pas si l'objectif est de mettre les bureaux d'enregistrement dans le coin et de les pointer du doigt. Donc il faut faire attention par rapport à cette éventuelle solution.

Lori a parlé de la difficulté d'accès aux données. Personne ne fait confiance aux données qui sont communiquées. Et les personnes qui amènent des données sont vues d'un œil suspect.

Et la dernière question, il y a des personnes dans l'industrie qui ne viennent pas aux réunions de l'ICANN et on ne sait ce qu'ils font. Est-ce que ces personnes-là sont vraiment impliquées ? Et il faudrait de meilleures pratiques.

James a parlé du cadre sur l'utilisation malveillante du DNS et du fait que certains s'étaient manifestés suite à cette initiative, donc cela avance. Mais il faut savoir que certaines initiatives ne font pas partie de la mission de l'ICANN, donc c'est juridique parfois, ceci crée certaines complexités.

Et enfin, dernière intervention de Chris, il n'y a pas une seule solution. Les RBL, le DAAR, tout ceci existe, mais il faut qu'il y ait un système transparent de manière à avoir le feedback et améliorer la situation.

Voilà de manière générale la discussion. C'était beaucoup en 90 minutes.

JOANNA KULESZA : Merci Olivier

Merci à tous les intervenants. Je voulais en arriver à un compromis mais encore une fois, nous n'avons que gratté la surface. Mais je crois que c'est quand même un pas dans le bon sens. Je l'ai déjà noté dans le chat, il y aura une séance conjointe du GAC et de l'ALAC sur l'utilisation malveillante du DNS et nous parlerons de la sécurité, de la sûreté et de l'utilisation malveillante du DNS pendant la semaine de l'ICANN72.

Donc nous nous retrouverons lors des séances de l'At-Large de l'ICANN72. Et nous poursuivrons ces discussions en ligne et j'espère même en personne lorsqu'enfin nous nous retrouverons pour la prochaine réunion de l'ICANN. En tout cas, je l'espère.

Merci à tous de nous avoir rejoints, merci aux excellents intervenants, merci pour le résumé d'Olivier, pour la gestion des questions et réponses Jonathan. Je vous remercie tous. La réunion est terminée.

DEVAN REED : Merci à tous. La réunion est terminée. Nous vous souhaitons une excellente journée, soirée. Au revoir à tous.

[FIN DE LA TRANSCRIPTION]