ICANN81 | Réunion générale annuelle – Séance conjointe : ALAC et SSAC
Dimanche 10 novembre 2024 – 13h15 à 14h30 TRT

YESIM SAGLAM : Si on va commencer, je vous prie de lancer l'enregistrement. Bonjour à toutes et à tous et bienvenue à cette session conjointe entre l'ALAC et le SSAC. Je m'appelle Yesim Saglam et je suis la responsable de la participation à distance pour cette séance. Veuillez noter que cette séance est enregistrée et qu'elle suit les normes de comportement attendus de l'ICANN ainsi que la politique anti-harcèlement de la communauté de l'ICANN. Lors de cette session, les questions et les commentaires ne seront lus à voix haute que s'ils sont soumis dans la fenêtre Questions-réponses. L'interprétation pour cette session sera garantie en anglais, français et espagnol. Si vous voudriez prendre la parole lors de cette session, veuillez lever la main dans Zoom. Lorsqu'on appellera votre nom, les participants à distance auront le droit d'activer leur micro. Les participants sur place utiliseront un micro physique pour parler. Veuillez indiquer votre nom pour l'enregistrement, la langue dans laquelle vous parlez si vous parlez une autre langue que l'anglais et veuillez parler à un rythme raisonnable. Je vais maintenant donner la parole à Jonathan Zuck, le président de l'ALAC, et à Ram Mohan, le président du SSAC.

JONATHAN ZUCK : Merci, Mesdames et Messieurs, de nous avoir rejoint aujourd'hui. C'est toujours un plaisir d'avoir cette session conjointe entre la communauté de l'ALAC et du SSAC. Notre objectif, bien sûr, est d'améliorer l'expérience de nos utilisateurs dans l'ensemble et nous partageons cet engagement. Donc c'est toujours un plaisir d'apprendre ce sur quoi travaille le SSAC. Alors que nous nous approchons de plus en plus de la nouvelle série de nouveaux gTLD, l'intensité des conversations sur ce sur quoi nous allons devoir travailler avant la mise en œuvre de cette nouvelle série va être importante. Donc nous allons parler de la collision de noms et de ses effets. Nous allons parler aussi de ces sujets qu'on appelle les sujets evergreen ou les sujets récurrents, tels que les utilisations malveillantes du DNS. Un rapport sera bientôt publié à ce sujet. Il aurait dû être publié avant cette réunion et j'espérais pouvoir avoir l'occasion d'en parler à cette réunion, mais malheureusement, il n'a pas encore été publié. Donc ça va raccourcir, écourter notre conversation.

RAM MOHAN : Bienvenue à toutes et à tous et merci d'être là. Jonathan, merci. J'ai l'impression que l'ALAC est ma deuxième maison ici au sein de l'ICANN. C'est toujours un plaisir d'être avec vous. Comme vous l'avez dit, nous partageons des valeurs. Nous partageons aussi une intention s'agissant de ce que nous désirons accomplir. C'est vraiment ce qui nous anime. Outre les sujets récurrents, les sujets evergreen, nous avons aussi pour objectif de vous informer concernant le travail et le rapport que nous avons publié plus tôt cette année, qui se concentre notamment sur l'automatisation DS, donc du signataire de délégation du DNSSEC. On

vous a consulté à ce sujet et nous n'allons pas vraiment un groupe de travail qui a pour mandat de travailler spécifiquement dans ce domaine. Nous bénéficions d'une expertise de certains de nos membres qui travaillent notamment dans le domaine de l'IA et de l'utilisation malveillante du DNS. Donc nous avons certaines réflexions par rapport à ce sujet et nous espérons pouvoir susciter des conversations ici, car cela va avoir des répercussions très claires pour les utilisateurs de l'Internet à l'avenir. Donc voilà certains des grands sujets avec lesquels nous souhaiterions échanger avec vous, sur lesquels nous souhaiterions échanger avec vous. Je souhaitais aussi vous informer qu'avec Matthias, qui est votre agent de liaison avec le SSAC, la coopération a été très agréable. Il s'est activement impliqué dans notre travail. Et je pense que vraiment maintenant notre travail ne fait qu'avancer. Merci.

Bien, passons à la diapositive suivante. Jonathan, plutôt que de parler d'une vision d'ensemble, moi je me disais qu'il y avait deux points importants à discuter. Une des choses qui nous a poussés à travailler à vos côtés dans le cadre de la campagne Un cyberespace sûr, c'est que nous disposons d'une expertise technique et que nous l'utilisons pour nous pencher sur des sujets qui, selon nous, sont importants et dans l'idée de rédiger des rapports. Mais nous nous sommes rendus compte qu'on ne pouvait pas se dire que voilà, une fois que c'est fait, c'est fait. Mais non, il y a encore beaucoup de pain sur la planche et il s'agit par après de faire circuler ce rapport en tant que tel, mais pas seulement. Il s'agit aussi de tirer des leçons de ce rapport. Il ne s'agit pas seulement de recommandations adressées au conseil d'administration ou à la

communauté, mais vraiment de leçons à apprendre. Et il s'agit de trouver des façons de traduire, de rendre accessibles ces rapports aux utilisateurs que nous visons.

Nous avons déjà commencé à travailler sur l'hameçonnage et sur d'autres risques en ligne et je suis très heureux des progrès que nous avons effectués jusqu'à présent dans ce domaine. Aussi Jonathan, je me disais que peut-être nous pourrions passer un peu de temps à parler de ce travail-là qui est déjà en cours, et puis ensuite dédier le reste de notre temps à parler de cette vision que nous avions pour cette campagne d'Un cyberespace plus sûr et qui comporte, bien évidemment, nombre de volets. Nous avons aussi travaillé dans toute une série d'autres domaines qui, selon moi, sont tout à fait pertinents pour les utilisateurs de l'Internet. Aussi, je me disais qu'on pourrait peut-être parler aussi de ces autres domaines auxquels il serait utile de réfléchir. Les autres volets de cette campagne, donc ces autres volets de cette campagne qui vont nous mener vers 2025.

JONATHAN ZUCK : Oui, c'est tout à fait logique. Nous avons créé un cours sur l'hameçonnage notamment, et sur Un cyberespace plus sûr, sur la cybersécurité. Nous avons déjà organisé plusieurs réunions. Vous avez parlé aussi du smishing qui devrait être aussi un domaine de travail, même si ça semble moins lié au DNS, mais pourquoi pas. Donc nous avons travaillé pour ajouter cela à notre campagne. Nous avons aussi travaillé avec Sébastien qui enseigne, je pense en France, à des citoyens plus âgés. Donc il a traduit notre travail en français et il a organisé un

atelier. Il a reçu un retour d'information par rapport à cela, l'idée étant d'apporter plus de clarté pour les utilisateurs. L'ICANN avait un feedback par rapport à cela sur cet atelier concernant l'hameçonnage par SMS et je pense qu'actuellement nous sommes dans une position… Nous serons à même de lancer ceci en début d'année. En début d'année, je me suis entretenu avec la Library Association qui enseigne ce cours également et qui travaille sur leur propre processus de révision pour voir si les organisations régionales veulent aussi apporter certains changements. Nous espérons pouvoir atteindre un résultat similaire à la réussite et au succès de la journée sur l'UA. L'idée vraiment est de fournir les informations aux utilisateurs finaux.

RAM MOHAN : C'est un travail d'envergure. Je serai aussi curieux d'avoir plus d'informations sur ce que vous avez dit. Vous avez entendu Sébastien, vous avez parlé de Sébastien et donc de cette importance de clarté. Et nous, ce que nous tentons de faire, l'une des choses qu'on tente de faire, notamment lorsqu'on travaille sur nos sujets récurrents, les sujets evergreen persistants, nous tentons de réaliser un résumé en 5 000 mots, plus ou moins, de notre travail. Donc nous rassemblons toutes ces informations et nous les rédigeons de façon à ce que ce soit accessible pour les utilisateurs, de façon à ce que ça puisse être utilisé comme document de base. Peut-être aussi pour lancer les conversations sur ce qui a été lancé dans le cadre du DNSSEC par exemple, ou ce qui a été lancé dans le cadre de la blockchain, de la chaîne de blocs et du DNS. Donc je pense qu'on aimerait en savoir plus

sur la façon dont vous améliorez aussi la façon de communiquer les messages que vous souhaitez communiquer.

JONATHAN ZUCK : Voici aussi un bel historique du courrier direct qui n'est parfois jamais envoyé. On envoie ceci, puis on reçoit un retour d'information, on le modifie, puis on le renvoie. Donc il s'agit de marketing direct. L'idée aussi est de savoir aussi un peu quels messages passent et peut-être que nous allons devoir bientôt créer des vidéos TikTok pour pouvoir communiquer ces informations. Mais en général, l'idée c'est de faire en sorte que les personnes dans cette pièce, vous savez, pour que les personnes dans cette pièce lisent 10 000 mots, 1 000 mots, 5 000 mots, c'est peut-être difficile. Il faut peut-être trouver aussi des façons d'attirer davantage leur attention. Et c'est la raison aussi pour laquelle je souhaitais que notre collègue partage avec vous ce que nous avons fait à ce niveau.

SÉBASTIEN BACHOLLET : Je vais m'exprimer en anglais. Merci de reconnaître mon travail. Bon, c'est pas vraiment mon travail aussi, mais bien sûr, les personnes qui ont élaboré ce cours, cette formation. Pour nous, c'était un test, car il s'agissait de personnes plus âgées qui ont parfois des difficultés à comprendre et donc une partie de mon travail, c'était de traduire ce cours en français. Et lorsqu'on traduit vers une autre langue, il faut aussi faire attention à la façon dont s’est écrit en anglais. Et donc je vous suggérerais vraiment qu'avant d'envoyer quoi que ce soit, vous demandiez à vos collègues, vous nous demandiez à nous d'effectuer la

traduction du document en question si c'est un document bref, parce que comment dire, ça peut être utile, mais nous n'avons pas besoin d'une traduction professionnelle. Nous avons besoin d'une traduction qui ciblera les personnes à qui on s'adressera. Et l'une des difficultés que nous avons avec l'interprétation et la traduction, c'est que la langue que vous utilisez en anglais, la façon dont nous nous exprimons en anglais diffère. Vous, c'est votre langue maternelle. Parfois, un mot qu'on utilise peut sembler convenir, mais lorsque nous nous l'entendons, ça ne signifiait peut-être pas la même chose. Donc la complexité de la formulation des mots qu'on choisit, ou parfois la simplicité de certains mots a une importance. Et donc, je pense qu'on doit d'abord traduire les documents en un anglais simple et puis ensuite les traduire dans d'autres langues. C'est ça la première étape.

Et parallèlement, ce qui est important, par rapport à ce que Jonathan vient de dire, c'est qu'il faut diviser ses présentations en plusieurs parties, car il est très difficile d'expliquer quelle est la différence entre tel type d'hameçonnage ou tel type de risque. En français, la traduction n'est pas toujours si évidente et donc l'image parfois que vous donnez en anglais ne fonctionne pas en français. Pourquoi phishing en anglais? Pourquoi hameçonnage en français? Peu importe les mots qu'on utilise au final. Parfois, il y a certains mots qui sont impossibles à traduire en français. Et l'image que vous avez, vous, en anglais est très bonne et je ne suis pas certain que l'image qu'on a trouvé pour la traduction française est aussi bonne et je pense qu'il en va de même probablement pour toutes les autres langues. Mais s'agissant de la communication, Jonathan s'y connait mieux que moi. C'est très compliqué. Mais

commençons par une langue à utiliser, une langue qui pourrait nous aider pour la suite. Mais encore une fois, bien sûr, le travail effectué par Jonathan pour ce premier jet de document était un travail excellent et c'était une très bonne base pour pouvoir commencer à travailler ici. Merci de m'avoir permis de faire ceci en français. Merci.

JONATHAN ZUCK : Oui, il s'agit de phase d'expérimentation. C'est comme cela que cela fonctionne. Il y a des choses que nous rédigeons et que nous allons essayer de passer à des phases d'expérimentation pendant les années à venir, les quelques années qui arrivent. Il y a des mots qui sont très chargés parce qu'il y a des choses qui correspondent à nos statuts aussi. Donc il faut faire un peu de sensibilisation. Je sais que la sensibilisation fait partie du monde de l'At-Large, mais l'idée est d'utiliser ce parcours de communication, cette infrastructure que nous utilisons, que nous avons mis en œuvre pour essayer de disséminer le message à plus de personnes que possible. Il y a beaucoup de manières de le faire et alors que nous observons ce que nous faisons, le message que nous voulons envoyer, il faut savoir exactement qui nous ciblons. Donc, si on parle de l'acceptation universelle, par exemple, il y a des cours et nous copions un peu cela. Et en attendant, il serait illogique de mettre en œuvre une campagne X ou Twitter pour essayer de partager cela avec le plus de personnes possible, par exemple de mentionner le nom d'une compagnie aérienne pour savoir s'ils sont prêts pour l'acceptation universelle. Est-ce qu'on peut partager le même message? Il faut que ce soit des messages qui soient compris. Il faut savoir donc qui nous ciblons, quelles sont les institutions que nous ciblons. Et dans le cas du

DNSSEC, l'utilisateur final typique, ce n'est pas votre audience finale, votre public final. Ce que vous essayez de faire, c'est d'essayer de tirer profit de cette unité constitutive pour faire passer le message à leurs directeurs techniques, etc. Donc, il faut absolument que l'on sache à quelle audience on s'adresse.

RAM MOHAN : Au SSAC, de notre côté, quand on prépare nos rapports, on se préoccupe de nos audiences, de notre public. En fait, il y a des publics auxquels on ne pensait pas, donc on n'a pas vraiment rédigé le document pour eux. Donc maintenant, on se rend compte que ce sont les personnes qui utilisent ces documents. Donc, il y a des leçons à tirer de cela, car au début il y avait beaucoup de rapports qui avaient été écrits et en fait les rapports avaient été acceptés par l'ALAC. Vous les aviez pris, vous les aviez lancés et vous les aviez utilisés. Ça nous a amenés à penser que peut-être nous devrions intégrer plus de points de vue. Donc c'était une façon valide de faire la chose.

JONATHAN ZUCK : Oui, on lisait vos rapports très denses et on se disait : Oh la la, on cherchait des mots clés.

RAM MOHAN : Oui, on essaie de faire mieux.

JONATHAN ZUCK : Peut-être que l'IA va nous aider.

RAM MOHAN : Oui, je pense qu'on s'améliore de ce côté-là, c'est sûr. A ce jour, nous travaillons sur deux sujets, deux thématiques au sein du SSAC. En fait, les coprésidents de ces deux groupes sont dans cette salle. Donc nous travaillons sur le filtrage du DNS. Donc on parle de ce filtrage de DNS. On se refocalise sur ce domaine, on a recommencé à travailler sur ce domaine. On a aussi étudié les questions open source et de toutes leurs implications vis à vis du DNS. Voilà donc deux thématiques courantes en ce moment au sein du SSAC. S'il y a à votre avis d'autres domaines qui sont importants pour votre communauté sur lesquels on pourrait peut-être initier de nouveaux travaux ou peut-être continuer le travail qui a déjà été fait et recommencer un peu le travail pour pouvoir cibler votre audience. Laissez-nous savoir, nous sommes ouverts. Y a-t-il quelque chose à rajouter sur cela?

En fait, je suis là pour jeter les bases et parler des projets Cybersécurité 2024. C'est une campagne conjointe entre l'ALAC et le SSAC que nous avons développé et que nous allons lancer durant dans l'avenir, au-delà de vos mandats, de mes mandats, de mon mandat. Passons donc à la prochaine diapo, s'il vous plaît. Nous avons Peter Thomassen qui est ici et qui va partager avec vous les informations d'un rapport que nous avons présenté plus tôt cette année le SAC-126.

PETER THOMASSEN : Vous vous rappelez peut-être que nous en avons parlé auparavant. Mais lorsque nous avons parlé de ce rapport dans le passé, il n'était pas complété. Donc, je veux faire un petit aperçu de ce à quoi ça correspond. Nous avons utilisé le DNSSEC pour avoir un lien, pour avoir

une validation, une clef de validation DNS dans la zone pour authentifier. Alors comment ça fonctionne? Le bureau d'enregistrement, c'est la même organisation que l'opérateur du DNS et cela est fait au niveau interne. En fait, c'est un problème pour une partie parce que les bureaux d'enregistrement peuvent le faire eux-mêmes Quand le titulaire du nom de domaine utilise un différent opérateur de DNS, c'est un problème multipartite. Donc le titulaire de nom de domaine a une approche centrique et donc il passe par un revendeur.

Ce n'est pas très simple en fait, parce qu'il y a des interfaces différentes qui sont parfois contradictoires. Cela dépend du TLD ou du bureau d'enregistrement. Il y a différentes opérations qui doivent être faites ou mises en œuvre. Et si c'était automatisé, ce serait beaucoup plus simple, c'est sûr. Donc, pour nous, au SSAC, nous avons fait une petite enquête sur ce problème, sur cet espace avec le SAC-126.

Voilà donc la déclaration liée au problème. Pouvez-vous passer à la prochaine diapo, s'il vous plaît? Donc le rapport. Prochaine diapo, s'il vous plaît. Le rapport a émis trois recommandations. Donc cela enquête les solutions qui existent maintenant pour l'automatisation des provisions du domaine. Et donc il y a une méthode standardisée avec des standards IETF et c'est une approche basée sur la CDS. C'est un mécanisme qui présente des limitations dans la zone enfant. Et donc la zone parent les trouve et les publie. Et donc c'est le RFC 73 44 et 9615.

Le mécanisme présente donc… Alors, il y a une méthode recommandée qui contient des limites, bien sûr, des limitations décrites dans le document. On voit que ce n'est pas la meilleure manière de faire les choses. Cela ne nous aide pas à savoir s'il y a un problème avec un verrouillage du bureau d'enregistrement. Bon, voilà, c'est la méthode que nous recommandons. La recommandation 2 dit que l'ICANN Org devrait soutenir les registres et les bureaux d'enregistrement qui souhaitent mettre en œuvre l'automatisation des DS à l'aide des mécanismes de la recommandation 1, par exemple en facilitant le RSEP. Donc les bureaux d'enregistrement peuvent déployer cela et cela pourrait permettre d'utiliser la voie RSEP accélérée, ce qui est moins onéreuse. Nous voulons encourager à ce que l'ICANN org puisse faire avancer ce projet.

En trois, j'avais déjà parlé de l'orientation opérationnelle, mais il y a d'autres sortes d'orientations quand on parle de l'acceptation technique, les validations qui doivent être faites par la zone parent. On parlait des données DS. Et donc il y a des choses qui doivent être refaites. Ça prend du temps. Donc il y a plein de choses, de détails à considérer. Sinon, il y a des choses qui ne sont pas standardisées à travers les TLD. Alors certains, cet été, ont déployé cette automatisation aujourd'hui et nous encourageons, bien sûr, l'ICANN org et la communauté de trouver des solutions qui seraient pertinentes, cohérentes, et qui permettraient de travailler de façon alignée à travers tout l'espace TLD. Il y a une solution qui serait peut-être plus holistique à notre problème. Ce n'est pas une résolution, une solution complète, mais cela pourrait fonctionner. Voilà donc un aperçu de ce que nous

faisons. Nous avons des rapports qui sont publiés. Si vous avez des questions, n'hésitez pas.

RAM MOHAN : D'accord. Oui. Donc il y a deux parties dans ce travail. Tout d'abord, on aimerait vous appeler à l'aide. Regardez la recommandation numéro 2. Donc, soutenir les bureaux d'enregistrement, les opérateurs qui souhaitent mettre en œuvre l'automatisation des DS à l'aide de mécanismes de recommandation 1. Et c'est là qu'on aimerait donc avec le RSEP accéléré, c'est là que nous aimerions recevoir votre soutien, avec l'aide bien sûr, de l'ICANN Org. Nous aimerions que vous compreniez que cela est important, utile pour améliorer la sécurité et la stabilité du système en général. Ces éléments, le plus d'avis, le plus d'opinions autour d'une table nous recevrons, le mieux nous pourrons faire le travail, car nous savons que l'ICANN Org peut répondre rapidement à la communauté, surtout aux questions venant de la communauté. Et donc parfois, quand nous parlons, nous, ils nous disent : Ah, c'est les gars techniques, c'est eux qui parlent. Mais quand vous combinez cela avec le groupe qui ne parle pas nécessairement des choses techniques, mais qui a des intérêts spécifiques, je pense que cela améliore la probabilité qu'ils nous écoutent et qu'ils fassent quelque chose à ce sujet. Donc, peut-être une lettre entre les deux communautés ou une lettre conjointe pourrait nous aider.

JONATHAN ZUCK : Vous parlez de contextualiser l'Icann Org pour demander à accélérer dans ce contexte spécifique ou en général? Qu'est-ce qu'on devrait demander? Quel document va-t-on diriger vers l'organisation?

RAM MOHAN : On ne parle pas seulement du conseil d'administration. Le RSEP accéléré, c'est un exemple. Est-ce qu'on devrait parler de la mise en œuvre, de comment on va faire les choses? Est-ce que ça doit être la responsabilité de l'organisation? Ce qu'on aimerait faire, c'est d'avoir un document qui va aller vers l'organisation et qui va rassembler les informations venant des deux communautés avec le soutien des deux communautés. C'est un sujet très important. Alors ça ferait passer un message. Non seulement vous vous préoccupez de ce problème, mais vous y mettez votre concentration. Nous avons déjà parlé du RSEP accéléré, nous n'avons pas besoin de le rappeler, mais maintenant nous voulons parler de priorité. C'est un moment important. Il faut mettre la priorité sur cela.

JONATHAN ZUCK : Je pense que nous serions ouverts à une telle collaboration.

RAM MOHAN : Très bien. Je pense que le personnel SAC est ici dans cette salle. John est là, je sais. John, vous voulez mettre ça sur notre agenda, un point d'action pour que nous puissions donc collaborer avec l'ALAC et continuer? Et donc, en notant cela, nous prendrons conscience du

problème et nous serons redevables. Voilà. Voilà, c'était vraiment une question importante pour nous.

JONATHAN ZUCK : Oui, c'est une bonne question. Vous parlez devant une communauté qui comprend très bien tous les enjeux.

RAM MOHAN : Oui, nous essayons de collaborer au mieux possible.

JONATHAN ZUCK : D'autres questions? Y a-t-il des questions en ligne?

YESIM SAGLAM : Je suis du personnel de l'ICANN. Nous avons une question en ligne d'Alejandra Perez. La question est celle-ci : Y a-t-il un document existant pour ce qui est des utilisateurs finaux pour l'installation du DNSSEC ou le DNS récursif? Est-ce que cela considère cela important de manière à ce que les utilisateurs finaux puissent l'installer sur leur LAN eux-mêmes?

PETER THOMASSEN : Peter. Oui, c'est de nouveau moi. Alors la question comprenait une observation selon laquelle le DNSSEC, il y a aussi un aspect validation. C'est correct, et la plupart des logiciels de résolveurs ont une validation DNSSEC et des boutons pour l'activer. Donc il y a des résolveurs contraignants, liés ou non liés. Tout ceci représente des capacités

DNSSEC qu'on peut retrouver dans une configuration LAN. On peut aussi utiliser un résolveur public tel que ceux de Google par exemple, ou de Cloudflare ou de Quad9. Et donc 8.8.8.8., 9.9.9.9. ou 1.1.1.1. La plupart des personnes utilisent le résolveur DNSSEC de leur fournisseur de services Internet et donc vous connaissez qui est votre fournisseur ou quand vous ne connaissez pas, il va vous assigner un résolveur DNS pour votre connexion internet lorsque vous l'établissez et on peut contourner cela. Et bien sûr, si vous souhaitez, comment dire, une très faible friction entre vos différentes capacités DNS, votre ISP pourrait peut-être le permettre. Je ne sais pas si ce sera le cas. Il faudra leur demander et encourager d'activer cette capacité si ce n'est pas encore le cas.

S'agissant des documents, tout ce que j'ai mentionné est mentionné dans les différents documents. Donc, si vous entrez ces noms dans une barre de recherche Google, vous vous atterrissez sur une bonne page, sur des documents par exemple Qud9. Mais certains... Mais je n'ai pas vraiment de documents de résumé qui résumerait toutes ces différentes options, mais peter@desec.io. Vous pouvez m'envoyer un mail. Et bien sûr, je pourrais vous envoyer des recommandations.

JONATHAN ZUCK : Y a-t-il d'autres questions ici, autour de la table, ou sur Zoom?

RAM MOHAN : Jonathan, c'est ça la directe conséquence du fait d'organiser une réunion juste après la pause déjeuner.

JONATHAN ZUCK : Oui, c'est bien vrai.

RAM MOHAN : Passons à la diapo suivante, s'il vous plaît. Je vais maintenant donner la parole à Tara.

EDUARDO DIAZ : Ici, on parle de l'impact sur les utilisateurs, n'est-ce pas? Mais là, vous parlez des titulaires de noms ou des opérateurs de registre des bureaux d'enregistrement. Parce que vraiment, moi, je suis un expert technique. Mais tout ce que vous venez d'expliquer, j'avoue n'y avoir rien compris. Je dois dire que c'est très difficile, du moins pour moi, de comprendre ce que vous avez expliqué, c'est-à-dire ce qu'est l'automatisation du DS, du signataire de délégation. Mais voilà, ici vous parlez, vous vous adressez à des utilisateurs finaux, à un public d'utilisateurs finaux.

PETER THOMASSEN : Alors peut-être que l'élément le plus important sur lequel j'aurais dû être plus clair, c'est que derrière cette automatisation, en fait, l'idée, ce serait de rendre la tâche moins difficile aux utilisateurs. Et les capacités activées par les opérateurs et par les bureaux d'enregistrement correspondants pour enregistrer ces configurations du DNSSEC de manière automatique, donc l'idée derrière, en fait, c'est de faire en sorte que les utilisateurs finaux n'aient pas à se soucier de ça. Mais dans les domaines parents, il y a des interactions avec les titulaires de noms.

Et dans le rapport, on suggère que les interventions manuelles… Si on supprimait en fait les interventions manuelles, ça rendrait la tâche plus facile aux utilisateurs finaux.

EDUARDO DIAZ : Mais que voulez-vous dire par utilisateur final?

JONATHAN ZUCK : Un titulaire de nom de domaine. C'est une distinction importante à faire, effectivement.

TARA WHALEN : Oui, si je puis me permettre. Effectivement, certains de ces éléments sont très compliqués et beaucoup des membres du SSAC sont très impliqués là-dedans. Moi, par exemple, je voudrais activer le DNSSEC. Si vous voulez faire ça, vous devez gérer des clés, des clés publiques, des clés privées et les titulaires de noms doivent comprendre cela et doivent entrer les bonnes informations et cela peut causer des problèmes. Donc ici, ce qu'on essaye de faire au sein du SSAC, c'est d'automatiser tout ça de façon à ce que les titulaires de nom, un titulaire de nom qui voudrait que son nom de domaine soit sécurisé d'un point de vue du DNSSEC, on voudrait faire en sorte qu'il n'ait qu'à cliquer sur un bouton et tout se fera de manière automatique. Et donc, de cette façon, le titulaire de nom n'aura rien de plus à savoir, il pourra juste le faire. Voilà, j'espère que cela vous aide à mieux comprendre la question.

EDUARDO DIAZ : Oui, j'ai bien compris cela.

JONATHAN ZUCK : Oui, c'est une question en cours, bien sûr, parce que cette distinction entre utilisateur final et titulaire de nom, il est important de la faire. On pourrait parler aussi d'utilisateur final du système DNS, mais bon, cela implique différentes informations des serveurs. Il y a de plus en plus de personnes qui parlent de Squarespace, qui font référence à des constructeurs de sites différents et qu'ils modifient leurs dossiers de manière manuelle. Donc effectivement, parfois les distinctions sont un peu floues. Mais ici on parle bien de quelqu'un qui a un nom de domaine.

RAM MOHAN : Oui. Encore d'autres questions? Satish?

SATISH BABU : Merci beaucoup, Ram. Alors ça me semble être une très bonne idée, notamment pour les utilisateurs finaux, parce qu'il s'agit de garantir la sécurité. Et si comme vous le dites, il suffit de cliquer sur un bouton et que tout devient plus sécurisé, c'est une très bonne façon de procéder. Donc oui, moi je suis un fervent supporter de cette proposition, car cela pourrait bénéficier à énormément de personnes et l'idée c'est que cela bénéficie au plus de personnes possible.

RAM MOHAN : Bien, je ne vois pas d'autres questions posées en ligne aussi. Tara, je vous donne la parole.

TARA WHALEN : Merci Ram. Alors je pense que Ram a déjà parlé du fait que le SSAC travaille sur toute une série de sujets techniques déjà depuis de nombreuses années. Mais maintenant, nous avons ce concept des sujets evergreen, les sujets récurrents. Car même si le paysage dans lequel nous travaillons évolue constamment, il y a toujours des sujets qui reviennent. Et donc nous souhaitons travailler sur ces sujets et trouver des façons de pouvoir nous exprimer constamment au travers de rapports. Mais il y a aussi d'autres façons de communiquer, par exemple au travers de blogs, de présentations, car il y a beaucoup de personnes qui viennent nous voir pour nous parler de ces sujets. Et donc nous aimerions faire en sorte que les individus qui veulent des informations à ce sujet puissent avoir accès à ces informations plus facilement. Donc, ces cinq sujets sont affichés à l'écran. Vous ne serez probablement pas surpris de voir que l'utilisation malveillante du DNS y figure, étant donné que le DNS est un système très important et très important aussi pour les personnes qui, malheureusement, mènent des activités d'abus ou de harcèlement en ligne. Et donc il est important de pouvoir continuer à avoir des opinions, des orientations, des recommandations à ce sujet, notamment au vu de l'évolution de la situation et afin de pouvoir aussi faire évoluer nos activités d'atténuation.

Il y a aussi le sujet des nouveaux gTLD qui est peut-être tout à fait opportun. Il est opportun d'en parler parce que la nouvelle série va bientôt être mise en place. Il y a aussi des considérations de sécurité et de stabilité à prendre en compte. Les nouvelles chaînes. On a beaucoup travaillé aussi sur la collision de noms ces derniers temps. Donc voilà, ça c'est un de nos sujets récurrents et comme Peter l'a dit, il y a le DNSSEC et des technologies fondatrices pour la sécurité du DNS qui sont, elles aussi, très souvent très complexes et en constante évolution. Et cette complexité, innée par nature, veut dire aussi que parfois, il est difficile pour vous de déployer cette sécurité, que vous avez des difficultés à avoir accès à des informations, que parfois il est difficile de trouver ces informations et donc que l'automatisation pourrait permettre cette sécurisation comme cela était prévu au départ.

Il y a aussi les espaces de noms, par exemple les espaces de noms pour la chaîne de blocs – la blockchain. Il y a beaucoup de discussions concernant le nommage qui n'implique pas forcément le DNS et donc certains et certaines d'entre vous savent déjà depuis longtemps qu'il y a aussi tout un univers d'espaces de noms en dehors du DNS. Et donc il faut savoir comment travailler par rapport à cela, comment intégrer cela avec le DNS? Est-ce que cela impliquerait pour la sécurité et la stabilité entre les différents espaces de noms? Donc voilà, ça c'est un sujet sur lequel nous continuons à travailler. Et bien sûr, il y a aussi la gouvernance de l'Internet et notamment la sécurité et la stabilité qui est le mandat donc du SSAC. Il y a beaucoup de politiques techniques qui portent sur cette question. Lorsqu'il y a des personnes qui élaborent des politiques, il y a parfois aussi des chevauchements entre l'espace,

les différents espaces technologiques et techniques. Et donc on essaie de fournir des informations techniques fiables pour venir en aide aux personnes et les aider à prendre les meilleures décisions possibles dans la mesure de leurs capacités. Donc, nous tentons de trouver des façons de fournir ces informations techniques à envoyer aux différentes communautés, de façon à ce que les individus sachent quelles sont les possibilités et les limites auxquelles ils sont confrontés par rapport à ces décisions politiques, techniques.

Nous avons différents groupes de travail actuellement. Alors parfois, il y a aussi des chevauchements entre différents domaines. Mais nous avons deux groupes de travail qui travaillent par exemple, notamment sur la gouvernance de l'Internet, sur les questions de sécurité telles que le filtrage. Il y a donc le filtrage. Le groupe de travail sur le filtrage et le verrouillage du DNS rassemble différentes entités des gouvernements, des autorités réglementaires qui assurent, qui font l'intermédiaire pour l'accès des utilisateurs au DNS. Le SSAC a déjà émis des recommandations par rapport à cela, mais elle date déjà d'il y a dix ans. Pendant cette période, le paysage réglementaire a changé, a évolué, le paysage technique aussi. Par exemple, le DNS sur HTTPS avec les demandes, la visibilité du DNS qui n'est plus aussi évidente pour d'autres parties. Et donc il s'agit de savoir quelles sont les approches qui ont été entreprises par rapport au filtrage et au verrouillage du DNS. Donc, nous avons décidé de retravailler sur la question de lancer un groupe de travail, notamment pour répondre à la question à quoi ressemble le paysage actuellement. Quels sont les outils à notre disposition? Qu'est-ce qui est possible? Quels sont les effets

secondaires qu'on pourrait anticiper lorsqu'on prend certains choix par rapport au verrouillage? Et donc ça, c'est très utile pour notamment les décideurs et décideuses politiques.

On a aussi un groupe de travail qui travaille sur les logiciels open source dans le cadre de l'infrastructure du DNS. Et cela comporte, bien sûr, différents volets, par exemple les résolveurs qui sont utilisés par des collectifs de personnes ou par des petits groupes de personnes qui ne sont pas forcément des entreprises et qui ne sont peut-être pas forcément très bien organisées ou bien financées. Peut-être qu'ils n'ont pas une relation contractuelle avec vous, mais pourtant ce sont ces personnes qui maintiennent certaines structures essentielles au sein du DNS. Et donc ces personnes qui nous donnent ces infos, qui nous procurent ces informations, peut-être ont-ils des présomptions par rapport à ce qui existe en termes de sécurité, par rapport à ce qu'ils peuvent ou ne pas faire. Et donc ce groupe de travail vise aussi à rendre certaines de ces dépendances plus visibles et voir aussi quelles sont les présomptions que certaines personnes ont par rapport à toutes ces infrastructures clés. Merci.

JONATHAN ZUCK : Oui, pardonnez-moi, je vous interromps. Mais est-ce que c'est quelque chose auquel vous réfléchissez ou est-ce qu'on devrait émettre des recommandations par cela? Est-ce que l'ICANN devrait davantage s'engager sur cette question? Il y a vraiment ces toutes petites infrastructures qui ressemblent à un cure-dent comparé au reste de

l'infrastructure qui sont maintenues par un gars dans sa cuisine. Qu'en est-il de ça?

TARA WHALEN : Le groupe de travail vient de commencer son travail, donc je ne peux pas trop en parler. Nous avons les présidents qui sont là, mais bon, je vais quand même essayer. Ce n'est pas un problème simple. De toute façon, lorsque l'on peut apporter des recommandations, on aime le faire. Il y a parfois de la médiation qui peut être claire et un point de vue que l'on peut apporter. Voilà, vous pouvez passer à telle ou telle étape. Il y a un élément technique qui pourra vous aider à réussir. C'est quelque chose avec lequel vous allez pouvoir avancer. Nous recommanderons ce moyen-là, mais aussi on a des démarches un peu plus systémiques. Si c'est un peu compliqué, on a des manières de vous aider, vous donner des exemples en disant : Bon, cela ne va pas fonctionner. Dans l'espace des noms de domaine, il y a des enjeux lorsqu'il s'agit des infrastructures critiques, par exemple les dépendances sur ce qui est des logiciels open source et donc je ne sais pas s'il y a des solutions claires dans ce sens. Mais parfois il y a des opinions. Enfin, il y a des gens qui nous demandent : Qu'est-ce que vous pouvez faire pour aider tel ou tel groupe? Vous avez des questions très spécifiques et on vous demande ce que vous pouvez faire et fournir les ressources nécessaires. Et donc on peut peut-être faire plus que leur apporter des ressources pour les aider à renforcer leur code, par exemple. Et on peut les diriger dans une direction ou dans une autre. Mais je ne veux pas m'avancer parce que notre travail sur le sujet vient juste de commencer. Donc j'espère que nous aurons plus

d'informations à faire passer dans l'avenir. C'est l'idée aussi de… C'est toujours bon de pouvoir dire : Oui, nous allons trouver une solution fantastique qui va se résumer en cinq recommandations. On aimerait tous faire cela.

SATISH BABU : J'ai une question sur le numéro 4 que vous avez avancé sur la diapositive. Il y a une séance sur tout ce qui est des racines alternatives. Alors comment est-ce que c'est notre priorité d'intégrer ou est-ce que c'est la priorité de ces routes alternatives de s'intégrer avec l'ICANN?

RAM MOHAN : Oui, nous sommes du côté de l'interopérabilité. Si vous avez un espace de noms alternatifs et que vous avez besoin d'un autre nom, d'un autre espace pour le DNS, il y a des étapes logiques à suivre. Les personnes qui utilisent ces fonctionnalités, par exemple dans l'espace numéro 1, qui veulent intégrer les fonctionnalités de l'espace 2. C'est ce qu'on voit aujourd'hui. En fait, c'est ce qui se passe quand il y a deux identifiants sur un nom d'espace blockchain qui veut intégrer les deux avec des identifiants variés, il faut mettre en place des sauvegardes. En général, quand on a un espace qui a une utilité et une valeur pour les utilisateurs, cela concerne le même ensemble d'utilisateurs en général, mais il faut essayer d'intégrer.

On peut penser à l'intégration et cela va se produire de plus en plus. Quand cela va se produire et quels seront les enjeux? Donc il y aura un chevauchement parfois, par exemple dans l'espace des blockchains et

dans les rapports publics. Et il y a des organisations dans cet espace de blockchain qui ont déjà dit qu'ils avaient « réservé » des TLD. Ce ne sont pas des TLD comme nous l'entendons, nous, ici dans l'espace DNS. Non, vous avez les collisions de nomenclature. Ça commence avec ça, n'est-ce pas? Mais vous avez d'autres enjeux de stabilité et de sécurité avec cette collision de noms. Que se passe-t-Il lorsqu'il y a des identifiants de noms qui existent déjà et qui sont déjà utiles dans un autre espace de noms et lorsque l'on a un identifiant qui est le même, comment est-ce que vous allez gérer ça? Nous n'avons pas de solution pour cela, mais nous voyons très bien et cela clairement, que les enjeux vont être... Il va y avoir des gros problèmes. Notre travail, c'est de sonner l'alerte, l'alarme et de dire : Voilà, soyez prudents. Si vous ne faites pas attention, vous allez vous retrouver à un point où la première fois que vous allez examiner ce problème, c'est que le problème a déjà commencé.

OLIVIER CRÉPIN-LEBLOND : Par rapport à ce que vous venez de dire, Ram, je comprends très bien que l'ICANN devrait être capable de s'assurer que son espace de noms est unique et je comprends très bien cela, que l'ICANN doit faire de son mieux pour ne pas avoir d'espaces alternatifs qui seraient en conflit les uns avec les autres. Mais comment est-ce qu'on empêche les parties tierces de se fracasser les uns les autres? On sait qu'il n'y a pas de conflit dans l'espace ICANN, mais il pourrait y avoir des conflits dans les autres espaces alternatifs. Moi je trouve que ça, c'est vraiment difficile à comprendre et difficile à gérer.

RAM MOHAN : Je ne pense pas qu'on devrait essayer, d'ailleurs, de gérer ça. Vous avez des parties privées variées qui mettent en œuvre des espaces de noms. Vous pouvez faire ça sur votre réseau privé et vous pouvez prendre tous les TLD qui existent déjà et installer cela au niveau local. Et vous pouvez vous amuser beaucoup lorsque vous avez essayé de sortir de l'Internet. Vous pouvez le faire. Il n'y a rien qui vous arrête. Mais nous, ce n'est pas notre but. Notre but, c'est de dire : Est-ce qu'un espace de nom devrait interagir avec un autre? Est-ce que cela apporte des enjeux de sécurité et de stabilité? Donc il faut qu'on priorise cela pour garantir la conception correcte avant la mise en œuvre de cette intégration. Sébastien, vous avez une question?

SÉBASTIEN BACHOLLET : Je vais parler. Je m'excuse auprès des interprètes, mais je vais parler en anglais. La question que je veux soulever, Ram, est très importante. C'est un déjà vu en fait. L'ICANN est passé par là plusieurs fois déjà, lorsqu'il s'agit des espaces alternatifs ou les systèmes de noms alternatifs. Donc cela ne veut pas dire que les choses vont être différentes cette fois-ci. Mais bon, nous devons prendre en compte notre histoire. Donc, vous avez soulevé ce point. Comment allons-nous appeler cela si on utilise notre nom pour parler de l'autre? Eh bien, on va être coincés. Parce qu'eux, ils vont utiliser nos mots et on va être obligés de suivre. Donc, si je peux vous demander, c'est de commencer à nous dire comment est-ce qu'on peut parler de cela sans utiliser nos propres mots, parce que ce sera bien meilleur pour la communication. Et aussi, il nous faut démontrer que nous vivons dans deux mondes

différents. Ce dont vous parlez, c'est de la manière dont nous allons protéger notre monde pour que ces entités ne peuvent pas nous perturber s'ils veulent faire leurs choses de leur côté, dans leur propre monde. C'est la vie. Peut-être un jour vont-ils vouloir outrepasser leur système et communiquer dans notre monde pour remplacer l'Internet? Ce n'est pas le cas pour le moment, mais nous devons nous protéger. Ce n'est pas parce que nous voulons être une forteresse, mais c'est notre système. Il fonctionne bien pour tout le monde et surtout il fonctionne bien pour les utilisateurs finaux.

RAM MOHAN : Oui, c'est un très bon point, Sébastien. Notre approche est celle-ci : la technologie va continuer à évoluer et nous devons accepter l'innovation. Nous devons accepter ces nouvelles technologies qui arrivent sur le marché. Nous ne pensons pas que notre rôle, comme vous l'avez dit, est de protéger les choses et d'en faire une forteresse. Nous voulons accepter tout cela, mais en même temps, on doit être clair. Si on utilise des termes, il faut qu'ils soient clairs. Et quand par exemple, moi personnellement, quand je pense TLD, je pense TLD dans l'espace des noms de domaine. Mais je vois aussi le mot TLD utilisé dans d'autres espaces de noms et cela porte à confusion, du moins pour moi. Quand j'entends le mot résolveur, cela veut dire quelque chose pour moi dans mon espace, parce que ce que j'appelle l'espace de l'utilisateur lambda. Donc il devrait y avoir une certaine clarté sur ces termes. Que signifient ces termes? Et bien sûr, c'est naturel pour les gens, surtout chez les jeunes, dans la technologie, d'adopter la nomenclature, la syntaxe, cette nouvelle langue dans ces domaines

déjà établis. C'est tout à fait normal. Ce que nous devons faire, enfin du moins nous devons réfléchir sur le fait que si cela se produit et que vous allez jusqu'au bout, s'il y a l'échec dans les autres espaces, cet échec va utiliser la nomenclature et la technologie qui est utilisée dans notre espace. Alors quelqu'un va parler de 2 000 TLD qui ont échoué dans cet espace, que cela va-t-il vouloir dire s'il y a un échec de résolution dans cet espace? Qu'est-ce que cela veut dire? Donc voilà, c'est là où il faut qu'on soit plus ou moins pas forcément protecteur, mais clair sur ce langage que nous utilisons. Ces mots ont des significations spécifiques et il y a de la confiance qui est associée avec ces mots dans cet espace. Donc, il n'y a pas de mal pour que d'autres espaces puissent tirer profit de ce sentiment de confiance, bien sûr, mais nous voulons nous assurer de préserver cette confiance, cette intégrité dans notre espace.

OLIVIER CRÉPIN-LEBLOND : Merci Ram. Vous avez parlé de la signification d'un nom. Un nom ne peut être qu'un nom de domaine lorsqu'il est dans un espace accrédité par l'ICANN. A-t-il dit accrédité par l'ICANN?

RAM MOHAN : Il y a des ccTLD qui ont des noms et ils ne sont pas forcément accrédités par l'ICANN. Donc ce que je dis, c'est que si un nom n'est pas dans la racine de l'Internet, c'est un TLD. Donc s'il est dans la racine d'Internet, c'est un TLD. Donc ce nom délègue d'autres noms. Ça, c'est un nom de domaine. Ce que je veux dire, c'est un nom dans une blockchain pourrait décider de l'appeler un nom de domaine, mais rien ne nous arrête. Il n'y a pas d'enjeu de propriété intellectuelle, de marque

déposée, etc. Voilà, Ce que je dis vraiment, c'est que si vous pensez en amont et que vous permettez ce mélange de termes dans un espace, il y aura un échec dans cet espace et cela apportera des problèmes collatéraux dans l'autre espace. Et voilà, c'est une question de stabilité. Allez-y.

JUSTINE CHEW : C'est une très bonne discussion que nous avons aujourd'hui. Il y a deux questions pour moi. Pouvez-vous clarifier cette initiative pour nous dans cet espace? Est-ce que c'est une collaboration avec OCTO? Donc je suppose que OCTO est au courant. Alors pour la deuxième question, comment l'At-Large peut vraiment surligner ces questions qui ont été soulevées dans la collaboration dans cette recherche pour faire quelque chose à ce sujet?

RAM MOHAN : Sur ce sujet, nous avons une collaboration très importante de la part d'OCTO, du chef de la technologie et du bureau du chef de la technologie. Donc, durant l'atelier à Washington D.C. pour le SSAC, nous avons une personne qui… Nous avons eu un panel sur le DNS, sur le blockchain, et le chef de la technologie a participé et a contribué. Nous avons partagé nos travaux. Donc beaucoup de travail a été fait dans ce sens. Et ce qui nous reste à faire. Et donc maintenant, c'est apparent, il faut qu'on le fasse puisque qu'on en parle aujourd'hui. D'ailleurs, ça fait plusieurs fois qu'on me pose la même question, donc je suppose qu'on a encore du pain sur la planche. Pour l'instant, nous avons fait du bon travail de communication. Nous avons collaboré,

mais l'opinion du chef de la technologie est en conflit avec l'opinion du SSAC. Quel est son point de vue? Il est différent parce que OCTO réagit par rapport à ces notions institutionnelles. Nous, on vient avec notre expertise technique de notre côté. Donc on voit vraiment qu'il y a une différence. Mais en général, lorsqu'il s'agit des espaces de noms alternatifs et des blockchains, et en ce qui concerne les interactions avec OCTO, nous avons des points communs. Donc OCTO nous dit : Voilà, la technologie évolue, il nous faut trouver des manières responsables pour nous intégrer. Voilà, j'espère que cela répond à votre question.

Bien. Il nous reste environ quatorze minutes pour cette session. Aussi, pourquoi ne pas passer à la suite, la section IA et utilisation malveillante du DNS? Peut-être qu'on pourrait prévoir ça pour notre prochaine session car je pense que ça va nous prendre plus de quinze minutes à passer en revue. Est-ce que ça vous va?

JONATHAN ZUCK : Oui, ça va. Oui, effectivement, c'est une conversation récurrente, mais le rapport final maintenant à ce sujet a été publié. Donc je ne sais pas s'il y a des personnes dans le public qui sont en train de le lire peut-être alors à l'heure actuelle. Et nous avons parlé du fait que des enregistrements en gros pourraient avoir un impact important sur les enregistrements. Donc je pense que à ce niveau-là, on devrait peut-être se coordonner avec vous pour parler des priorités à venir au sein de la GNSO. Je sais qu'ils ont lancé une petite équipe pour parler de cette question, notamment la question des enregistrements en particulier.

L'idée, bien sûr, c'est d'éviter de minimiser les enregistrements malveillants. Alors je pense qu'on en arrive bientôt au dernier sujet. Il y avait des questions encore, une de Georgia Osborn.

GEORGIA OSBORN : Je m'exprime en mon nom, mais en tant que nouveau membre du SSAC, je travaille notamment sur la chaîne de blocs, les noms de domaine et sur le document qui a été publié un an. Évidemment, ça a évolué un peu depuis. Au sein de l'ALAC, nous avons trois différents utilisateurs de ces systèmes. Donc tout d'abord, nous avons les utilisateurs de la blockchain. Puis après, on a les personnes de la communauté DNS qui sont tout simplement curieux et une troisième catégorie qui représente les personnes qui pourraient peut-être chercher à tirer profit de cela. Et il existe un diagramme de Venn de la blockchain. Ce serait intéressant peut-être en fait d'avoir ce diagramme de Venn pour voir qu'est ce qui se recoupe, quels sont les défis qui se recoupent avec la propriété intellectuelle, quelles sont les occasions à saisir. On a par exemple .art qui permet aux artistes de préserver leurs œuvres. Il y a aussi des évolutions à ce niveau. Donc voilà, c'était ce que je voulais mentionner et pardonnez-moi d'avoir pris de votre temps.

JONATHAN ZUCK : Il me semble qu'il y avait encore quelqu'un d'autre qui avait levé la main. Donc une question dans le chat : Comment le travail du SSAC sur l'utilisation malveillante du DNS pourrait permettre que l'Internet soit plus accessible pour les utilisateurs au quotidien?

RAM MOHAN : Je pense que c'est une question ouverte et récurrente. Eh bien, je pense que pour ça, je dirais : Aidez-nous, nous avons besoin de votre aide, car nous ne sommes pas des experts de la communication. Nous, nous sommes en train de recruter. Nous travaillons avec Sally Newell Cohen et avec l'équipe de communication de l'ICANN afin de nous améliorer justement sur cette question de la communication. Parce que je pense qu'au sein du SSAC, on se rend compte que la production de rapports techniques, ce n'est que le début de notre travail. Ce n'est pas l'aboutissement. Donc n'hésitez pas à nous aider à rendre notre travail plus accessible et plus facile à mettre en œuvre.

JONATHAN ZUCK : Oui, effectivement, je pense qu'on cherche tous comment mieux communiquer. En à peine huit ans, nous avons fait en sorte que l'ICANN travaille sur beaucoup de petits sujets et on s'habitue vraiment à ce rythme. Peut-être qu'il y aura aussi un autre mécanisme qui nous permettra d'avoir un document qui permet de rassembler toutes les informations à ce sujet. On en a déjà entendu beaucoup. Même avec la plateforme ICANN Learn, on a déjà fait beaucoup de progrès. Il y a cinq ans, tous les cours sur la plateforme provenaient de cursus des années 70. Maintenant, nous avons connu des avancées technologiques. Et donc oui, je pense qu'ici, l'effort sera effectué sur plusieurs fronts pour améliorer nos capacités de communication.

OLIVIER CRÉPIN-LEBLOND : Étant donné qu'on a encore quelque temps, je voudrais parler du DNSSEC. Une question concernant le DNSSEC. La question n'était pas qu'est-ce qui est arrivé en premier : l'IPv6 ou alors le DNSSEC? Je ne sais pas. Ceci étant dit, et j'ai entendu très souvent ce genre d'inquiétude étant soulevé et formulé de façon différente, certains pays s'inquiètent du DNSSEC et de la chaîne de clés, de la gestion des clés avec cette clé unique en haut de la pyramide qui est détenue par je ne sais qui. Et il y a aussi la question de la souveraineté liée à cela. La personne qui détient cette clé peut avoir une certaine forme de contrôle sur votre nom de domaine. Est-ce qu'il y a quelque chose qui est fait par rapport à ça pour répondre à ces inquiétudes? Est-ce qu'on travaille sur la question des clés partagées ou pas?

RAM MOHAN : Au sein du SSAC, nous n'avons pas vraiment travaillé sur cette question en particulier. Mais dans l'imaginaire public et je l'ai vu dans la presse, certaines personnes disent que les détenteurs de ces clés ont tout le pouvoir, qu'ils peuvent allumer ou éteindre l'Internet. Mais il existe des mécanismes très clairs et établis qui permettent d'éviter que ce genre de choses ne se produise. Mais bien sûr, encore une fois, on doit mieux communiquer à ce niveau. Steve va lever la main.

STEVE CROCKER : Alors moi, je suis impliqué sur toutes ces séries d'activités déjà depuis longtemps, comme nombre d'autres personnes, y compris le personnel de l'ICANN très compétent qui supervise tout ceci. Si la crainte qu'on exprime dans certaines entités selon lesquelles l'ICANN pourrait

contrôler l'accès de certains pays à l'Internet grâce à ces clés, je pense que cette question a déjà été soulevée de manière directe ou indirecte dans le cadre de nombre de conversations. Il semble facile de penser que l'on comprend à quel point cela serait problématique si cela se produisait. Et donc, au sein de la structure de l'ICANN, on comprend bien qu'il ne faut pas abuser de cela. Il y a certains cas spécifiques qui se sont déjà produits et qui sont bien connus. Par exemple, les Etats-Unis ont une certaine vision de Cuba et les services DNS de Cuba n'ont pas été modifiés pendant très longtemps. Je me suis entretenu avec des hauts responsables en Russie pour leur demander : Mais que se passerait-il si l'ICANN nous faisait sortir de la racine, il pourrait se produire quelque chose de très négatif? Cela pourrait se produire, mais cela aurait de graves conséquences si on pouvait forcer les États-Unis à faire cela. Il me disait donc : Si on pouvait forcer les États-Unis à faire cela, ce serait très bien pour nous. Et on pourrait ainsi aspirer l'ICANN dans ce genre de de mauvaise activité. Donc, il y a les hostilités qui font rage en Ukraine. Et l'Ukraine nous disait : Mais retirez la Russie du système. Mais nous, bien sûr, nous ne pouvons pas faire cela. Je ne pense pas que l'on doive faire quoi que ce soit, pour être honnête. Les pays qui pensent à cela ont également le contrôle de leurs propres clés à un niveau en deçà de la racine, et chaque niveau de clé peut être utilisé pour susciter la confiance. Et donc ces utilisateurs dans ces pays bien spécifiques pourraient être encouragés à utiliser certains logiciels à utiliser ces ancres de confiance. Et si c'était le cas, tout irait bien. Merci.

RAM MOHAN : Merci beaucoup, Steve. Oui, effectivement, il y a beaucoup de garde-fous qui sont mis en place. Évidemment, il y a-t-il d'autres questions?

STEVE CROCKER : Oui, j'ai l'impression que c'est très important aussi pour l'éducation de notre communauté, pour la formation de notre communauté.

RAM MOHAN : Jonathan, un rapport vient d'être publié, et nous allons le Faire circuler au sein du SSAC. Et peut-être aussi grâce à Matthias, nous pourrions lancer une discussion pour joindre nos forces et nous rassembler.

JONATHAN ZUCK : Oui, ce serait une très bonne chose. Je suis d'accord. La nouvelle série de gTLD ne représente pas forcément un intérêt pour la mauvaise utilisation du DNS, mais il y a tout de même certains points de friction et il y a certaines conversations qui, si on ne les envisageait pas sous cet angle seraient reléguées aux oubliettes. Peut-être qu'on pourrait aussi prévoir quelque chose pour après le lancement de cette nouvelle série de gTLD. Je ne sais pas si vous avez déjà ressenti cela, mais voilà.

MATTHIAS HUDOBNIK : Je voulais juste préciser que je serai heureux de résumer les résultats du rapport et puis, ensuite, de les faire circuler et puis ensuite peut-être de répondre aux questions. Je pense que ce serait une bonne façon de procéder. Merci.

RAM MOHAN : Ceci nous amène à la fin de cette session, Jonathan. Merci encore une fois de nous avoir accueilli. Merci aussi pour toutes les excellentes questions que vous avez posées et toutes les excellentes suggestions que vous avez émises. Nous avons bien pris note de tout cela. Nous espérons poursuivre notre coopération et je vais sortir de cette salle avec un nouveau sentiment d'espérance.

JONATHAN ZUCK : Oui, pareil pour moi. Et vraiment, je voudrais vous féliciter pour les efforts que vous effectuez pour améliorer l'accessibilité de votre travail. C'est tout à fait logique. Bien évidemment. Sinon, c'est comme si quelqu'un écrivait une thèse, et puis cette thèse restait sur les étagères de la bibliothèque à tout jamais et n'était jamais ouverte. L'idée, bien sûr, est de partager cela avec un plus large public. Nous voulons que la plupart de ces informations soient accessibles. Donc, continuons à travailler sur cela ensemble. Merci.

[FIN DE LA TRANSCRIPTION]