ICANN67 | Forum virtuel de la communauté – Séance de politique d'At-Large - DoH/DOT - Menaces et défis
Mardi 10 mars 2020 – 13h00 à 14h30 CUN

YEŞIM NAZLAR : Bonjour à tous et bienvenue sur l'appel. Nous allons contacter Holly Raiche et ainsi, nous pourrons commencer très bientôt. Merci.

Nous avons des problèmes techniques. Soyez patients. D'ici quelques minutes, nous allons résoudre le problème. Merci.

Bonjour Maureen. Je vois que Maureen est connectée sur Zoom.

MAUREEN HILYARD : Je suis en train de m'organiser, excusez-moi. Très bien.

Cette réunion est enregistrée.

YEŞIM NAZLAR : Bonjour à tous, bon après-midi, bonsoir à tout le monde. Bienvenue à l'ICANN67 et à la session virtuelle de l'At-Large, DoH sur DoT, DNS sur HTTPS, menaces et défis. Nous sommes le 10 mars et il est 18h00 UTC.

L'audio de la salle Zoom est en anglais. Afin d'accéder à l'audio français ou espagnol, veuillez joindre le streaming français ou espagnol. Il y a le lien sur le site principal de l'ICANN67. Tous les détails ont été envoyés sur la liste d'annonces de l'ALAC avec tous les

liens pertinents. Les détails de ces connexions peuvent également être trouvés sur les page de d'ordre du jour wiki d'At-Large de l'ICANN67.

Nous ne ferons pas l'appel nominal aujourd'hui pour gagner du temps, mais la présence des membres de l'ALAC, du leadership des RALO et des liaisons sera notée.

Si vous souhaitez poser une question ou faire un commentaire en anglais, français ou espagnol, veuillez le taper dans le chat en commençant et en terminant votre phrase par « question » ou « commentaire ». S'il vous plaît, soyez bref si possible. Les questions en français ou en espagnol seront traduites en anglais et lues à haute voix par les responsables de la participation à distance, Claudia Ruiz et moi-même. Le personnel fera des rappels périodiques de ce processus dans le chat de la salle Zoom.

Si vous êtes dans la salle Zoom et que vous souhaitez parler, vous pouvez également lever la main et le personnel gèrera la file d'attente.

Je vous rappelle d'indiquer vos noms lorsque vous parlez, non seulement à des fins de transcription mais aussi pour que les interprètes vous identifient sur le streaming audio.

Veuillez également parler clairement à une vitesse raisonnable pour permettre une interprétation précise.

Enfin, cette séance, comme toutes les autres activités de l'ICANN, est régie par les normes de comportement attendu de l'ICANN. J'ai d'ailleurs mis un lien dans le chat qui va vous diriger vers ces normes pour référence.

Sans plus tarder, je cède maintenant la parole à Maureen, présidente de l'ALAC. À vous Maureen.

MAUREEN HILYARD : Merci à tous. J'espère que vous m'entendez bien. J'attends qu'Holly s'organise avec sa connexion. En attendant, sachez que cette séance est réservée aux menaces et défis du DoH sur le DoT. C'est Heidi qui a organisé cette séance. J'espère qu'elle va nous rejoindre aussi tôt que possible pour qu'elle puisse présenter cette séance puisque ce n'est pas une de mes compétences.

Je sais que nous avons des invités. Nous avons Paul. Je suppose que Rod est aussi disponible. Je voudrais souhaiter la bienvenue à toutes les personnes qui sont sur la liste. J'espère que les autres sont un petit peu plus préparés que moi, mais si vous pouviez être un peu patients avec mois pendant que je vérifie si Holly est disponible. Merci. Je ne reçois aucun message, donc on va commencer.

Peut-être pourrions-nous avoir une introduction. Je sais qu'Holly a eu quelques conversations avec Rod, donc peut-être que Rod pourrait nous faire une petite introduction. Nous discutons de cette question au sein de l'At-Large. Nous l'avons fait dans le passé. Donc peut-être pourrions-nous faire un petit résumé de la discussion sur ce sujet. Est-ce que c'est possible ?

ROD RASMUSSEN : Bonjour Maureen. Certainement, nous pouvons commencer à en discuter un peu.

Nous avons dialogué là-dessus auparavant. Je sais et je crois que sur l'ordre du jour... Attendez, je vais regarder. Je suis devant mon ordinateur et je vais ouvrir l'ordre du jour. Je pense que Paul doit faire sa présentation, Barry aussi. Paul, est-ce que c'est cela ?

PAUL HOFFMAN : Oui. Un petit peu avant cette séance, il a été décidé que je ferais la présentation et qu'il n'y aurait pas de présentation formelle du SSAC mais qu'on pourrait parler de ce qui va se produire dans l'avenir.

HOLLY RAICHE : Est-ce que je peux parler maintenant ? Est-ce que vous m'écoutez ?

J'écoutais Paul. C'est fantastique.

PAUL HOFFMAN : En fait Holly, vous ne pouviez pas écouter ma présentation puisque je ne la faisais pas. Je l'ai fait pour m'entraîner un petit peu tout à l'heure.

HOLLY RAICHE : Je suis contente de commencer. Je suis en ligne depuis longtemps mais je suis désolée de mon retard maintenant. Ne criez pas sur moi.

Je suis donc prête à commencer. J'entends Paul parler dans mes écouteurs. Est-ce que je peux entendre cette séance ou dois-je parler ?

ROD RASMUSSEN : Vous avez une introduction à faire. Allez-y, faites cette introduction. Attendez, Paul ne parle pas en ce moment.

HOLLY RAICHE : Je vais donc commencer.

Cette séance va donc discuter du DNS sur TLS, ce qui est le DoT, ou du DNS sur HTTPS, qui est le DoH, le DNS sur les couches de transport ou le HTTPS, qui sont des systèmes sécurités. Voilà l'introduction qu'il y a dans l'ordre du jour, mais cela n'explique pas tout.

Quand je vois les autres séances, je vois qu'on a beaucoup parlé de vie privée et du fait de savoir si les données privées devraient être rendues publiques. Mais on n'a pas fait suffisamment attention à cette problématique tout aussi importante pour l'ICANN. Là, il s'agit de se préoccuper de ce que font les gens sur l'internet, de qui ils contactent sur l'internet. Ces informations s'appellent des métadonnées et cela est très important puisqu'il s'agit des noms et des contacts des personnes. Tout cela est passé sous le radar, si vous voulez.

Donc Paul Hoffman est là pour tout nous expliquer. Il va nous donner un petit peu un historique. Paul Hoffman est arrivé à l'ICANN en 2015. Il est responsable de la technologie. Il est là pour améliorer les capacités techniques de l'ICANN au niveau interne et aussi au niveau externe pour tout ce qui s'agit de la communauté internet.

Nous passons la parole à Paul.

PAUL HOFFMAN : Je vais faire une brève présentation pour couvrir les aspects dont Holly vient de vous parler. Ensuite nous aurons, je pense, une discussion avec les gens du SSAC et il y aura du temps pour poser des questions. Nous allons passer à la prochaine diapositive.

Je suis l'éditeur principal d'un document que nous venons de publier. Et puisque tout le monde ne peut pas cliquer sur son écran, j'ai copié le lien directement sur le chat. Il s'agit d'un document en PDF. Le titre de ce document et de cette discussion s'appelle « Implication des politiques locales et internet sur le DNS chiffré ».

Il y a beaucoup d'implications au niveau des politiques par rapport au fait que les gens peuvent voir les métadonnées de chacun ; il faut donc savoir ce que l'on recherche. Il y a du positif et du négatif. Nous allons en parler dans cette présentation. Le SSAC va apporter un document complètement différent dans l'avenir proche. Donc nous allons aussi en parler.

Mais pour ce document, il y avait quatre sujets importants : il s'agissait du filtrage et de la surveillance dans le DNS, pourquoi les gens font telles ou telles choses ; et quelles en sont les implications, les conséquences en matière de politiques en général ; qui sont les parties intéressées ; et ensuite, nous parlerons des positions de l'ICANN.

On va continuer. Il serait bon d'attendre pour poser des questions à la fin de la présentation, même si ce sont des questions techniques. Le côté technique est beaucoup moins intéressant que le côté politique si vous voulez. Prochaine diapositive.

Comme vous le voyez, ce diagramme, c'est une diapositive qui est obligatoire dans toutes les présentations. Qui sont les participants techniques qui travaillent pour les utilisateurs ? À gauche, vous avez le client stub DNS et c'est ce que vous avez sur votre téléphone ou sur votre ordinateur. Un peu sur la gauche, vous avez les serveurs récursifs du DNS, ce sont des systèmes qui fonctionnent pour l'utilisateur. Et ensuite, vous avez le nuage obligatoire géant de l'internet. Et à droite, vous avez les serveurs racine d'autorité qui sont ceux qui connaissent vraiment la réponse.

Beaucoup d'entre vous ont vu des diapositives telles que celle-ci auparavant. La chose la plus importante à retenir, c'est que toutes ces flèches grises sont chiffrées. Le DNS chiffré, il correspond aux flèches de la gauche, les flèches qui vont du client stub au serveur récursif. Il y a des opportunités pour faire plus de chiffrement après, mais pour notre discussion d'aujourd'hui, nous allons en rester au chiffrement entre le client stub et le serveur récursif. Prochaine diapositive s'il vous plaît.

Parlons maintenant d'où est-ce que le chiffrement va être fait, de l'endroit spécifique. Pour l'instant, nous en sommes au début, à la base, parce qu'il y a des implications au niveau des politiques dans ce sens, le chiffrement à partir de l'utilisateur final vers le prochain boîtier. Après cela, ce chiffrement est moins nécessaire. Les résolveurs minimums n'apparaissent que dans les systèmes d'exploitation à certains endroits. Le système d'exploitation pour le service DNS. Si vous êtes sur votre téléphone, il y a quelques années, vous auriez pu voir qu'il y avait un seul résolveur minimum. Maintenant, vous en avez

peut-être plusieurs, certains dans les navigateurs ou dans les autres applications de type navigateur.

On va aller plus loin. En fait, on devrait parler du comment et non pas de l'emplacement. Passons à la prochaine diapositive. Parfois, l'IETF fait des choses standards et a des protocoles standardisés. Et parfois, l'IETF fait les choses d'une façon pire. Il y a plusieurs manières de faire la même chose. Je dis cela en blaguant parce que vous allez trouver cela sur les deux documents. J'accepte le blâme pour cela.

Il y a deux protocoles standardisés pour le chiffrage du DNS. Il y a le DNS sur le TLS et tout le monde appelle cela le DoT. Et ensuite, va le DNS sur HTTPS, ce qu'on appelle DoH. Pour ceux qui connaissent la bande-dessinée *Les Simpsons*, là, nous on appelle cela « D'oh ! »

La chose importante, c'est de savoir qu'il s'agit de l'implication des politiques. Là, on ne parle pas de la technologie. Ce sont des protocoles qui sont similaires mais qui comprennent tout de même des différences et cela est important pour les opérateurs de réseaux. Donc il faut parler de ces différences avant de passer au côté politique. Prochaine diapositive.

Pour le DNS sur le TLS, c'est ce qui est arrivé en premier, le résolveur minimum démarre une session TLS avec le résolveur et cela est identique à la manière dont votre navigateur démarre une session TLS quand vous allez sur une page web qui est chiffrée. Donc le TLS est le protocole de sécurité qui fonctionne dans différents contextes et qui fonctionne assez bien dans ce contexte précis.

Il y a beaucoup de choses que vous avez certainement vues auparavant. L'authentification au sein du TLS est très importante. Si vous essayez d'aller sur un site web et que le site web ne peut pas être authentifié au sein du TLS, le navigateur va vous le dire et il va essayer de vous convaincre pour que vous ne puissiez pas y aller. Dans ce cas-là, c'est une option, l'authentification du résolveur est facultative mais nécessaire pour empêcher les attaques d'un tiers. Mais c'est nécessaire si vous voulez être rassuré. Cela est facile à mettre en place. Prochaine diapositive.

Le DNS sur HTTPS, c'est celui qui est arrivé quelques années après. C'est un résolveur minimum qui démarre une session HTTPS, ce qui sera fait littéralement comme s'ils allaient envoyer une requête comme si c'était une navigation de web normal. Cela commence à envoyer du trafic DNS qui a été encapsulé dans les requêtes HTTPS.

Vous pouvez regarder l'historique de l'internet et voir cela de deux manières. Le DNS est arrivé en premier, donc c'est certainement plus primaire. Mais vous pouvez voir aussi les choses différemment. Il y a eu beaucoup de travail qui a été fait maintenant par rapport à ce qu'ont fait les gens du DNS. Et c'est la genèse de ce qu'on a maintenant. Maintenant, nous avons deux façons différentes de chiffrer le DNS. Si vous faites le DNS sur HTTPS et que vous utilisez la version deux, cela permet au serveur d'envoyer du contenu DNS sur TLS au client.

La nouvelle version a des avantages, des avantages techniques. Ce n'est pas de cela dont on parle aujourd'hui puisqu'on veut vraiment parler de l'implication au niveau des politiques. Prochaine diapositive.

Le document que j'ai édité contient ces sept points en matière de politiques. Cela, c'est un aperçu si vous voulez. Quand on fait du DNS chiffré, on a une confidentialité accrue pour le trafic DNS des utilisateurs, une assurance accrue pour ce même trafic DNS des utilisateurs. On voit si le DNS est chiffré et on pense que c'est une chose positive.

Ensuite, vous voyez, on utilise le mot « contournement ». Cela a une connotation plutôt négative pour des bonnes raisons. Le DNS chiffré est utilisé pour contourner les politiques de filtrage que quelqu'un peut avoir ou des politiques locales ou même des politiques mandatées par les gouvernements. Donc il faut regarder le point au milieu et là, on se dit : « Le DNS chiffré, c'est vraiment mauvais. »

Les deux derniers points sont aussi importants. Vous avez la possibilité d'avoir une centralisation indésirable de la résolution DNS. Il y a des désaccords sur ce sujet, à savoir si c'est positif ou négatif. Et aussi, vous avez le problème de vitesse des réponses DNS. Nous parlons de millisecondes, bien sûr, donc ce n'est pas très important pour la conversation aujourd'hui. Prochaine diapositive.

Voyons maintenant ce que j'ai appelé les points positifs. La protection de la vie privée est en générale bonne. On essaie de donner aux utilisateurs finaux une meilleure protection. S'ils utilisent le même ordinateur, ils vont utiliser le DNS chiffré et vont tous avoir la même

protection. Et à la base, il s'agit d'une protection pour les personnes qui vont utiliser internet et qui vont dire : « Tiens, regarde cette personne demande ce DNS. » ou ce type de chose. » Donc en général, cela a été considéré comme quelque chose positif ; c'est pour cela que nous avons commencé ce travail.

Le fait d'utiliser un DNS chiffré protège les utilisateurs des observateurs entre le stub et le résolveur. Vous allez être sûr que les réponses que vous recevez sont les bonnes réponses. Par exemple, un attaquant ne peut pas voir si vous demandez une adresse sur un site du gouvernement et ne pourra pas vous envoyer à un mauvais quand il s'agit d'informations privées. Donc le DoH et le DoT augmentent la sécurité du DNS, tout comme l'utilisation du HTTPS sur le web. Prochaine diapositive.

Donc ces trois points ici vont porter sur le contournement. C'est une des raisons pour lesquelles beaucoup de gens sont inquiets concernant le DNS chiffré. C'est parce qu'à la base, vous avez un problème... Il y a du bruit de fond.

Il s'agit d'un problème d'utilisation. Si vous utilisez un service qui filtre ou qui surveille le trafic du DNS, ce que certains fournisseurs d'internet font, ils essaient de voir quelles sont les requêtes de DNS que vous faites, si vous faites une requête pour quelque chose qui va vous amener sur un site de malware, ils vont arrêter cela. Ils vont arrêter votre requête ou ils vont l'envoyer de nouveau et vont vous dire que c'est un problème. À ce moment-là, vous n'irez pas sur ce site de malware.

C'est assez courant, c'est plus courant dans certaines régions, dans certains pays que dans d'autres. Et même dans notre région aux États-Unis – puisque je suis des États-Unis –, certains fournisseurs d'internet le font gratuitement, d'autres le font contre un paiement, certains le font plus ou moins. Mais c'est un service qui est souvent donné pour améliorer la sécurité de l'utilisateur.

Certains filtrages sont mandatés par les gouvernements. Il y a des lois dans certains pays qui disent que les fournisseurs de services doivent faire ce type de filtrage du DNS pour empêcher les gens d'être envoyés sur des adresses erronées. Si vous faites cela avec un DNS qui va vous empêcher ce filtrage, l'utilisateur, à ce moment-là, ne sera plus protégé, il n'aura plus le bénéfice d'être protégé par ces lois gouvernementales. Prochaine diapositive.

Je pense que nous aurons beaucoup de temps pour poser des questions après si vous avez des questions à poser. Pas de problème, nous aurons le temps de le faire.

Il y a aussi une question de la centralisation indésirable. Il y a des clients qui implémentent un DNS chiffré qui peuvent le faire en disant : « On va chiffrer ce que vous avez envoyé. » mais ils vont aussi l'envoyer à un endroit différent qui va vous donner une meilleure protection. Quand ils font cela, ils le font pour ce qu'ils considèrent un bénéfice, pour vous donner une meilleure protection de vos données. Mais le résultat est qu'ils vont envoyer ces requêtes à un petit nombre de résolveurs et à ce moment-là, il y a une possibilité ici de diminution de réponses. La possibilité ici, c'est qu'on vous dise : « Si vous avez

confiance dans ce logiciel qui va faire des choix pour vous, vous aurez tel résultat. » Le problème, c'est que cela va envoyer toutes vos requêtes à un petit nombre d'endroits et les gens vont pouvoir les utiliser. C'est quelque chose qui n'est courant qu'aux États-Unis actuellement et c'est seulement pour les personnes qui utilisent le navigateur Firefox. Cela peut changer dans le futur, il va y avoir peut-être d'autres navigateurs qui vont l'appliquer aussi mais pour le moment, c'est comme cela.

En tout cas, la discussion portant sur la centralisation non désirée est quelque chose qui augmente ; il y a des préoccupations dans ce sens. On va en parler.

La rapidité des réponses. Ici, on parle de secondes seulement. Prochaine diapositive.

Dans ce document, l'ICANN prend quelques positions. Et puisqu'il s'agit d'un appel de l'ALAC, vous le savez tout cela peut-être mieux que moi, il y a une différence au niveau des positions au niveau de l'ICANN au niveau des politiques. Il y a des choses qui peuvent être positives ou pas dans ces sens. Et la position de l'ICANN, c'est que la protection de la vie privée est quelque chose de positif. Donc augmenter la protection de la vie privée est quelque chose qui est bon.

Le filtrage du DNS peut aussi être bénéfique. On a vu beaucoup d'endroits où on avait ce filtrage qui peut empêcher les gens d'accéder à des endroits qui peuvent être dangereux.

Troisième point, ici, c'est un petit peu plus compliqué. Ce troisième point porte sur le fait qu'actuellement, les applications et les systèmes d'exploitation n'ont pas suffisamment d'informations pour prendre des décisions de contrôle du réseau. Comme par exemple, cet utilisateur utilise un ISP qui utilise un bon système de filtrage ou au contraire, cet utilisateur est sur un réseau qui est dangereux donc je vais essayer de voir si je peux faire quelque chose. Les applications et les systèmes d'exploitation n'ont pas suffisamment d'informations actuellement.

Et le dernier point qui est un petit peu la base de tout ce qu'on fait ici au sein de l'ICANN, c'est que les données DNS doivent être protégées le mieux possible. Dernière diapositive.

La dernière diapositive, pour ceux d'entre vous qui ont vu ce document plus tôt, vous savez que nous avons fait une mise à jour il y a quelques jours. Nous sommes à la version deux. C'est le même document mais il y a quelques mises à jour. Et je vais parler.

La première mise à jour est le fait que Mozilla, pour les personnes qui utilisent Firefox, accroît leurs programmes aux États-Unis mais jusqu'à présent, nulle part ailleurs. Donc la première version de ce document va parler de Mozilla, qui a fait beaucoup de publicité là-dessus d'ailleurs. C'est quelque chose que les gens connaissent mais qui est encore considéré comme une grande nouveauté.

Depuis que nous avons fait ce premier document, Microsoft a aussi annoncé qu'ils ajouteraient une mise à niveau sécurisée pour les connexions au résolveur à Windows en utilisant DoH, pas DoT. Ils vont

le faire en utilisant le DoH. Ils parlent la possibilité de faire cela cette année.

Puis, le point le plus important – et on verra cela plus tard dans le détail – c'est le fait que de plus en plus d'opérateurs de réseau se sont impliqués dans les discussions sur la manière de déployer le DNS chiffré parce que les utilisateurs pensent souvent qu'ils ont leur service de DNS d'un autre opérateur ou d'un ISP. Et ces personnes participent davantage ; on voit cela de plus en plus.

C'était la dernière diapositive que j'avais à vous présenter. Je ne sais pas si Holly veut prendre la parole ? En tout cas, je serai ravi de répondre à vos questions et je pense que Rod Rasmussen aussi.

HOLLY RAICHE : Merci beaucoup. Vous parlez de la version deux du 24 février, c'est cela ? Ici dans le chat, je vois qu'il y a eu une certaine activité, donc on va regarder un petit peu. Les gens voudraient savoir où est ce document qui est un document très intéressant, assez épais, je dirais assez long.

La première question qui a été posée était de Thomas De Haan de la Commission européenne, qui pose plusieurs questions. Est-ce que Thomas est en ligne ? On voudrait savoir si Thomas est en ligne. Est-ce que vous voulez poser les questions vous-même ou est-ce que vous voulez que je les pose et que je lise vos questions ?

THOMAS DE HAAN : Est-ce que vous m'entendez ?

HOLLY RAICHE : Oui, allez-y, on vous entend.

THOMAS DE HAAN : Bien. Alors, je vais poser les questions moi-même. Peut-être que la deuxième question est plus importante.

On a une date ici de mars 2020. On a parlé d'un déploiement mondial avec le même résolveur. Donc j'aimerais que quelqu'un me confirme cela. Merci.

Je vois qu'on m'a déjà donné la réponse ici sur le chat.

PAUL HOFFMAN : Je vais prendre la deuxième question que vous avez posée parce qu'il y a des réponses sur le chat dont certaines me surprennent, je dois dire.

Puisque nous sommes à l'ICANN, les noms sont importants. Il y a un problème de nommage ici dans votre première question. Vous parlez de Chrome ; il y a beaucoup de choses que Google a appelé Chrome. Mais le navigateur de Chrome ne sera pas déployé, que je sache, sur DNS chiffré. Ils n'ont fait aucune annonce à ce propos.

Ils ont fait une annonce cependant : ils ont dit qu'ils faisaient du DNS chiffré sur le système d'exploitation actuel. Donc cela veut dire que vous allez vous connecter sur votre résolveur et ils vont aussi vérifier

que le résolveur fasse du DNS chiffré, ils vont donc vous dire qu'ils vont faire une mise à jour ou une augmentation des capacités. Jusqu'à maintenant, ils n'ont pas dit la façon dont ils allaient faire cela. Peut-être qu'ils vont le faire dans le futur, ils vont peut-être faire des annonces à ce propos, mais je ne sais pas.

En tout cas, je peux vous dire que ce que nous savons, ce qu'ils déploient – et ça, on le sait – le personnel de Google a dit qu'ils allaient faire cela sur Chrome à un moment donné. Mais on n'a pas entendu de commentaires de leur part depuis. Donc on ne sait pas quand ils vont faire cela. Je pense que cela veut dire qu'on l'ignore. Autant Google que Firefox ont été très efficaces pour dire des choses quelques semaines avant leur déploiement. Donc c'est une tendance qu'ils ont.

HOLLY RAICHE : Merci beaucoup.

Jonathan, vous aviez deux ou trois commentaires que vous avez faits dans le chat. Est-ce que vous voulez poser vos questions ? Jonathan, allez-y, vous avez la parole.

JONATHAN ZUCK : Allez-y Dave, je peux attendre.

HOLLY RAICHE : Dave, allez-y. Est-ce que vous pouvez parler ou est-ce que vous voulez que je lise vos questions dans le chat, Dave ?

Je n'entends rien. Paul, la question de Dave est : « Quel est ce qui justifie le chiffrement du DNS et le système de serveurs récursifs du DNS ? Pourquoi un chiffrement partiel ? »

PAUL HOFFMAN : Je dirais que poser des questions concernant des justifications des actions de certaines personnes est toujours un petit peu compliqué.

La justification par exemple pour pourquoi est-ce que je n'ai pas voulu chiffrer tout le canal, c'est parce qu'il y a moins de bénéfices à faire un chiffrement entre un résolveur récursif et le résolveur faisant autorité parce que ce résolveur récursif en général est responsable des requêtes de millions d'utilisateurs. L'information qui est identifiable est vraiment minime ; ce n'est pas zéro mais c'est très bas. Donc c'est plus difficile pour un serveur faisant autorité de se rendre compte de combien de ressources techniques ils doivent utiliser pour faire un chiffrement, et c'est beaucoup plus que pour un résolveur récursif.

Je pense qu'on est dans une situation dans laquelle tout le DNS pourrait être chiffré. Mais actuellement, le monde technique se focalise plutôt sur la première partie parce que c'est la partie qui affecte le plus directement les utilisateurs. Pourquoi ? C'est une des choses que le SSAC est en train d'analyser justement.

ROD RASMUSSEN : Je vais donner la parole à Barry qui est le coprésident de notre groupe de travail. Je pense que nous allons profiter de ces dernières minutes.

Nous avons vu la dernière version PDF du document qui devrait être publié. Bien sûr, cette discussion a lieu à la dernière minute. Nous avons dû faire notre magie SSAC et nous avons dû produire un document. Il sera disponible très bientôt.

Nous avons fait une présentation qui est prête. Je ne sais pas exactement quel est le planning sur cela. Je vais passer la parole à Barry qui va mener la réponse SSAC.

BARRY LEIBA : Je n'ai pas grand-chose à rajouter à ce qu'a dit Paul.

Le rapport SSAC ne couvre pas l'idée de chiffrement entre le récursif et l'autorité parce que les protocoles ne le spécifient pas pour l'instant. Nous avons discuté de cela dans un groupe de travail.

Je suis d'accord avec la réponse de Paul. Fondamentalement, la concentration d'informations privées est moins présente entre le récursif et l'autorité. Donc il était plus facile de déployer le DoT sans aller jusqu'au bout. Je n'ai rien d'autre à rajouter.

Mais si je peux me le permettre, j'ai vu les trois autres questions dans le chat, des questions que j'aimerais aborder. Nous avons parlé aussi dans notre document SSAC du DNSSEC contre DoT ou DoH. Et il y avait beaucoup de question à ce sujet sur le chat.

Le DNSSEC aborde un aspect de la réponse du DNS. Le protocole chiffré, c'est autre chose. Le protocole chiffré empêche l'espionnage sur le trajet. Cela permet aux serveurs de communiquer correctement.

Mais s'il y a une mauvaise information, elle peut aussi être transmise. Donc il faut trouver un moyen de la modifier sur le chemin. Le DNSSEC permet d'arrêter le transfert de cette mauvaise information avec leur système de signature. Les deux protocoles sont tous les deux très importants.

Il y a une autre question que j'ai vue dans le chat à laquelle je voudrais répondre. « Pourquoi est-ce que les navigateurs veulent utiliser DoH au lieu d'utiliser DoT ? » Les navigateurs et les autres applications navigatrices ont déjà les moyens à travers les programmes de faire face à tout ce genre de connexion et à tous les aspects qui sont impliqués. Il est donc plus facile pour eux d'utiliser le DNS sur cela au lieu d'utiliser un port différent ou un protocole différent. Ils n'ont ainsi pas besoin de rajouter de logiciel aux applications qu'ils ont déjà.

J'espère que cela répond à vos questions.

HOLLY RAICHE : Merci Paul. Si vous revenez au début de votre présentation, sur la première diapositive, on voit que cela se produit au tout début, lorsque la recherche démarre. Cette technologie est mise en place pour protéger cette première recherche, cette première demande. C'est une technologie différente pour résoudre un problème différent.

PAUL HOFFMAN : Non, vous n'avez pas tord mais ce que vous venez de dire, c'est juste une partie de la réponse. Je voudrais recevoir la réponse du SSAC sur ce sujet. Au SSAC, ils sont très inquiets en ce qui s'agit de l'authenticité

des données DNS. Avec les problèmes que nous avons toujours eus, c'est qu'avec le DNSSEC, vous pouvez vérifier l'exactitude des réponses. Tout le monde peut vérifier cette exactitude. Quand cela a commencé à être développé, le DNSSEC, on s'est dit : « L'utilisateur va vérifier cela. » Mais en fait, de nos jours, aucun utilisateur ne vérifie. Ils font confiance au résolveur et ce résolveur va faire la vérification pour eux.

Donc cela pose deux problèmes. Le premier c'est que vous, en tant qu'utilisateur, vous ne savez pas vraiment si le résolveur à qui vous parlez fait ces vérifications. Donc vous n'avez aucune manière facile de vérifier vous-même sans avoir à passer à travers plein d'obstacles techniques. Donc l'idée de la confiance de la réponse qu'on obtient du DNS, c'est bien moins clair que celle qu'on a sur le web. Sur le web, on regarde, on voit s'il y a un verrouillage, etc. Il y a un feedback qui est visible. Il est donc plus facile pour vous de vous dire : « Pourquoi je dois faire confiance à tel ou à tel ? » Avec le DNSSEC, vous avez une réponse, vous êtes correct. Le DNSSEC répond à certaines de ces inquiétudes, mais seulement si vous faites le DNSSEC. Et comme on l'a vu, aucun utilisateur ne le fait. Peu de requêtes envoyées au résolveur sont vérifiées. Il y a peu d'organisations qui signent le DNSSEC. Ce n'est pas très clair, tout cela.

HOLLY RAICHE : Excellent.

Nous avons encore quelques questions. Ensuite, nous passerons à Barry.

La première question – je vais mal prononcer le nom de la personne, bien sûr – Gangesh Varma : « Quelle a été la réponse des forces d'application de la loi au niveau des juridictions ? »

PAUL HOFFMAN : Ce n'est pas une question pour moi.

HOLLY RAICHE : Est-ce que c'est une question pour Barry ?

PAUL HOFFMAN : Peut-être pour d'autres personnes qui participent à la réunion.

HOLLY RAICHE : Barry, voulez-vous répondre à cela ?

BARRY LEIBA : Non, j'ai dit non. Je ne peux pas répondre à cela.

HOLLY RAICHE : Donc nous allons laisser cette question sur la table.

Prochain question de Joanna : « Quand il s'agit de la fragmentation de l'internet, quelle est l'implication ? »

PAUL HOFFMAN : Pour la question sur la fragmentation de l'internet, dans ce cas-là, avoir des politiques locales, c'est quelque chose de central. La façon la plus rapide d'expliquer cela, c'est « mon réseau, ma réglementation ».

Alors, comment je partage les mêmes réglementations entre mon réseau et l'internet, cela dépend de l'organisation qui s'occupe de l'informatique ou des clients, même si je suis un fournisseur de services ou un protocole. Donc à travers l'historique de l'internet, nous avons permis d'une façon silencieuse que vous fassiez votre propre réglementation. Des choses comme le DNS chiffré peuvent contourner ces réglementations et cela peut mener à des politiques locales inattendues.

HOLLY RAICHE : Il y a des mains levées. Il y a Jonathan, Gabriel. Et je voudrais lire une des questions. Mais Jonathan, vous pouvez prendre la parole.

JONATHAN ZUCK : Il y a eu beaucoup de conversations sur le chat par rapport aux dangers qui sont associés avec la centralisation des données. Et la raison pour laquelle il y a ces questions, c'est qu'il y a un petit nombre de navigateurs qui peuvent mener cette notion de centralisation. Ils ont la capacité maintenant de choisir un simple résolveur maintenant, donc on leur donne ce pouvoir. Et ce pouvoir vient de ce DNS qui est chiffré ; cela peut être amené par cela justement. Il n'y a pas d'autres résolveurs alternatifs ? S'il y avait plus de serveurs qui pourraient gérer ces chiffrements, on aurait peut-être moins de problèmes.

PAUL HOFFMAN : Je vais essayer de répondre à cela.

Encore une fois, je parle de la part de peu de personnes. Cette question devrait être posée aux gens chez Mozilla. Ça va, mais...

JONATHAN ZUCK : La partie technique de la question, c'est de savoir qu'ils avaient le pouvoir de choisir leur résolveur parce qu'il y avait l'absence d'autres systèmes. Donc pourquoi est-ce que cette centralisation a existé depuis le début ?

PAUL HOFFMAN : Nous avons vu beaucoup de conversations sur ce sujet de nos jours mais pour qu'un navigateur ou n'importe quelle application sur n'importe quel instrument puisse faire cela, cela existe depuis au moins 20 ans. Donc le fait que Mozilla a dit aux gens que ce qu'ils faisaient était dangereux, ce n'est pas nouveau.

La chose qui est importante maintenant – je ne parle pas de la part de Mozilla – mais si vous lisez le document que j'ai écrit, vous allez voir que je parle pour eux dans ce document. Je le fais avec beaucoup plus de prudence que je ne le fais maintenant. Ils sont clairs. Ils disent que le résolveur récursif auquel ils vont envoyer votre requête est sûr. Il y a beaucoup de restrictions qui ont été mises sur ce résolveur. Le nombre va augmenter aussi rapidement que Mozilla le veut. Ils aimeraient bien sûr avoir une liste plus étendue et comme cela, ils auraient moins de

plaintes. Mais ils ont des normes sur les emplacements où ils veulent envoyer vos requêtes. Pour l'instant, ils n'en ont que deux. Et dans la version un du document, ils n'en avaient qu'un à qui ils font confiance pour gérer ces restrictions de vie privée.

Je travaille pour l'ICANN et comme vous dites, l'ICANN a un service informatique. Et ce département a décidé qu'ils allaient utiliser leur propre résolveur récursif pour les utilisateurs de l'ICANN. Il y a beaucoup de gens sur cet appel dans cette réunion qui travaillent pour des compagnies IT et qui disent : « Je vais envoyer toutes les requêtes à tel ou tel résolveur récursif ouvert. » Il y a beaucoup de résolveurs ouverts qui font cela. Cela, c'est une décision que quelqu'un a prise au sujet de votre vie privée, et vous ne connaissez pas cette décision.

HOLLY RAICHE : Excellente réponse.

Nous avons plusieurs personnes dans le chat qui veulent faire des commentaires ou qui veulent poser des questions. Gabriel, vous avez mis une question dans le chat. Voulez-vous la reposer maintenant ?

GABRIEL : Oui, d'accord.

La question est celle-ci : est-ce que cette centralisation qui n'est pas volontaire va augmenter les attaques du DNS ? Et cela pourrait mener

à une panne du web à grande échelle comme on l'a vu en octobre 2016.

PAUL HOFFMAN : Barry, voulez-vous répondre à cela ? Je pense que vous en avez parlé au SSAC.

BARRY LEIBA : Je vais en parler, effectivement.

À la base, quand on du DDoS, les gens qui ont ces résolveurs récursifs importants sont tout à fait conscients de ces problèmes d'attaques DDoS. Ils sont là pour atténuer ces attaques ; c'est ce qu'ils font, par exemple celui qui est géré par Cloudflare. Cloudflare est un système de livraison de contenu. Ils sont très bien préparés pour faire face à cela.

Nous avons fait beaucoup de chemin dans les deux dernières années depuis que nous avons eu ce problème de pannes. Beaucoup de personnes maintenant ont appris de ces leçons. Il y a moins de vulnérabilité pour ces attaques mais ces points peuvent être compliqués. Donc c'est un équilibre.

GABRIEL : Est-ce qu'il y a quelque chose dans le protocole qui va nous permettre de passer à un canal non chiffré ?

BARRY LEIBA : Non, pas dans le protocole. L'application en elle-même doit voir si le résolveur fait le changement.

GABRIEL : Merci.

HOLLY RAICHE : Alan, vous voulez prendre la parole ? Alan Greenberg ?

ALAN GREENBERG : Merci.

Dans cette séance et dans d'autres séances, on parle beaucoup de confiance et de protection de la vie privée. Ce qui n'est pas très clair ici, c'est qu'il ne s'agit pas vraiment de question de protocole ou de méthodologie qui soit plus fiable qu'une autre. Mais il s'agit ici de savoir en qui on peut avoir confiance.

Je dirais que le DNS ouvert traditionnel est facile, on peut le pirater. Et en même temps, le DoH ou DoT, on peut aussi les pirater par quelqu'un qui utilise le résolveur. Google et Mozilla ont des systèmes, mais il faut comprendre que tout cela est vulnérable si l'on n'a pas confiance à l'endroit dans lequel on trouve ces données. On peut toujours être suivi par quelqu'un sur le réseau. Et en même temps, les opérateurs du résolveur qui chiffrent les questions pour le résolveur ont la possibilité de suivre tout cela. Si on n'a pas confiance en eux, à ce moment-là, c'est un problème. Ici, c'est cela le problème.

BARRY LEIBA : Je voudrais répondre à cette question parce que nous en avons parlé dans ce document du SSAC.

La première chose que j'ai dite, c'est qu'il y a toute une série de problèmes et de solutions dans le domaine des activités du DNS pour les rendre plus privées. Ces solutions qui ont été proposées et exposées abordent différents aspects ici. Donc vous avez raison, cela ne rend pas tout protégé et privé mais cela présente quelques aspects de la protection de la vie privée et de la communication avec le DNS.

L'autre partie de votre commentaire concerne ce que nous avons analysé dans ce document. Dans ce document du SSAC, nous avons analysé différents points de vue, différentes perspectives en fonction de votre rôle, si vous travaillez dans un gouvernement, dans une entreprise, si vous fournissez un service, si vous êtes parent d'un enfant et que vous voulez contrôler. Vous avez peut-être différentes raisons de vouloir protéger votre vie privée. Il y a différentes parties en qui vous avez confiance ou pas. Donc ce document analyse tout cela. Il y a de nombreux problèmes ici parce qu'une personne peut filtrer son système pour éviter que ses enfants aient accès à du matériel pornographique et d'une certaine façon, c'est de la censure. Donc si vous lisez le document du SSAC, qui va bientôt sortir d'ailleurs, vous verrez tout cela.

PAUL HOFFMAN : Je voudrais répéter un petit peu ce que Barry a dit mais l'aborder d'une perspective différente.

Vous parlez de la confiance ici. C'est une question simple, mais je vais vous demander et vous reposer une autre question à propos de cela. Lorsque vous posez cette question « Qui êtes-vous ? », il y a différents « vous » dans cette question. Cela peut être la personne qui est assise devant l'ordinateur, la personne qui a écrit ce logiciel, par exemple les personnes de Mozilla pensent qu'ils ont un droit à prendre cette décision à votre place.

Ensuite, il y a aussi le fournisseur de service internet parce qu'eux savent que vous ne pensez pas suffisamment à tout cela, et donc ils le font à votre place. Si vous travaillez dans une compagnie, vous payez ces responsables du service informatique pour qu'ils réfléchissent à tout cela et pour que vous soyez libéré de cette préoccupation. Ce « vous » peut même être votre gouvernement local qui considère qu'il y a trop de personnes ici concernées et qui veut avoir l'autorité.

Donc c'est difficile de savoir qui est ce vous quand on parle de vous.

HOLLY RAICHE : Merci Barry.

Je crois qu'on a encore une trentaine de minutes. Nous n'avons pas eu le temps de vous entendre parler du document du SSAC. Hier, vous avez dit que ce document n'était pas encore sur le site du SSAC. Mais est-ce que vous pouvez nous en parler un petit peu quand même ? Merci.

BARRY LEIBA : Oui, je peux.

La première question est : « Quand ce document va être diffusé ? » Nous sommes en train de faire les dernières petites corrections dans ce document avant qu'il soit diffusé.

Je vais vous parler un petit peu de ce que l'on peut attendre de ce document. Ce document explique un petit peu ce que Paul a dit, c'est-à-dire ce que le DNS sur le DoH et sur le DoT représentent. Ce document ne passe pas beaucoup de temps là-dessus, il analyse surtout les effets de ces protocoles et les perspectives de différents groupes, de différentes parties prenantes. On parle des parents, des entreprises, des gestionnaires de réseau, des fournisseurs de service internet, de différentes parties qui peuvent utiliser ou mettre en œuvre ce protocole ou qui vont implémenter des résolveurs qui vont donner lieu à des changements de comportements et d'applications.

Donc on essaie de voir les différentes perspectives, d'analyser les différentes perspectives des différents types de parties prenantes qui vont utiliser tout cela. On essaie de voir quels seront les choix du résolveur, comment est-ce que l'application va faire ses propres choix du résolveur, comment cela va affecter différentes parties et quel est l'impact que cela aura sur les différentes décisions. L'implication aussi du nom de l'espace qui change le point de contrôle, cela va donner différents impacts sur des choix que les résolveurs vont faire. Donc c'est une chose ici dont Paul n'a pas parlé, il me semble, qui fait partie de cette explication parce que traditionnellement, lorsque vous

utilisez ce stub, ce résolveur minimum, vous utilisez toujours le même résolveur. Donc l'application qui va passer par cela va utiliser le même résolveur minimum.

Chaque application va faire son propre choix ou a la possibilité de faire son propre choix concernant le résolveur récursif qu'elle veut utiliser. Il y a différentes applications qui vont faire différents choix. Théoriquement, chaque résolveur récursif va envoyer la même information mais en pratique, ce n'est pas toujours le cas.

Par conséquent, ce document va parler de la façon dont tout cela va affecter ces fonctionnements. Une chose que le document ne fait pas, c'est d'indiquer la bonne manière de faire les choses. Nous avons regardé tout cela, nous en avons discuté, nous avons dit : « Ce sont des problèmes qui sont nouveaux et qui dépendent de perspectives, de visions. » Et il y a des personnes au sein du SSAC qui ont des visions différentes à propos de cela. Donc on essaie d'éviter de dire : « C'est faux. C'est bien. C'est mal. » On essaie de dire que c'est une nouvelle tendance, il y a de nouveaux choix, de nouveaux impacts. On essaie de dire aussi peut-être qu'une chose n'est pas meilleure que l'autre. Plus de protection, plus de chiffrement, ce n'est pas toujours meilleur.

Nos recommandations changent un petit peu. Ce que nous faisons ici, c'est que nous essayons de présenter le problème et de présenter les avantages et les inconvénients selon les différentes perspectives. Notre objectif est que nos lecteurs comprennent mieux où on en est, quelle est la situation actuelle. Voilà ce que j'avais à dire.

Suzanne Woolf est la coprésidente du groupe de travail qui a élaboré ce document. Peut-être que Suzanne a quelque chose à ajouter ? Nous allons lui demander. Suzanne ?

SUZANNE WOOLF : J'ai la possibilité de parler. Bien. Je ne savais pas si mon système audio allait fonctionner.

Je voudrais reprendre un petit peu ce que Barry a dit, ce qui a été dit dans le chat.

Je pense que tout est très complexe. On a essayé dans ce document de réduire ce niveau de complexité, de faire quelques recommandations, de présenter des principes de base. C'est difficile parce qu'il y a une grande diversité d'intérêts ici. C'est donc compliqué.

Je crois que, comme on l'a dit dans le chat, une des choses qui surgit des efforts du SSAC, c'est qu'il y a une série de solutions au niveau technique, au niveau politique qui ne prennent pas en compte la complexité des intérêts. À ce moment-là, ce type d'approche ne sera pas une approche réussie. Parce qu'on voit qu'avec l'emploi de DoH ou DoT, dans la mesure où ces technologies ont été inventées et sont utilisées, il y a des logiciels qui les utilisent, ensuite il faut voir quelles sont les politiques que l'on doit appliquer dans le cadre de ces systèmes. Et beaucoup de choses qui arrivent ici, c'est que les personnes déploient ces technologies, voient comment elles

fonctionnent, quels sont les intérêts qui sont affectés et définissent le modèle, la façon dont ils veulent configurer tout cela.

Donc avoir des personnes qui s'intéressent à cela, des utilisateurs, la cybersécurité qui s'intéresse davantage à tout cela ; c'est un petit peu ce que nous voulons faire dans ce document du SSAC. Plus les gens sont informés, plus les gens qui s'intéressent à cela et à la façon dont fonctionnent les choses comme le DNSSEC, plus les utilisateurs et les représentants des utilisateurs vont trouver la meilleure manière de naviguer dans ce monde assez complexe.

HOLLY RAICHE : Merci Suzanne, merci Barry.

Je crois qu'il y a encore beaucoup de questions. On est un petit peu sur la fin de notre séance. Rappelez-vous que ces séances sont enregistrées, qu'il y aura une transcription du contenu de ces séances et qu'il y a un chat aussi. Et si cela vous intéresse, vous pouvez revenir aussi à ces séances, les écouter à nouveau, etc.

Avant de donner la parole aux participants, est-ce que vous avez quelque chose à ajouter, Barry, Rod ou Paul ?

PAUL HOFFMAN : Je reprendrai un petit peu ce que Suzanne a dit. Il y a beaucoup de gens qui ont beaucoup réfléchi à tout cela et je ne sais pas si le fait que je vous en dise davantage va être utile. Je crois que le mieux serait de passer aux questions.

HOLLY RAICHE : Très bien, passons aux questions. Judith, allez.

JUDITH HELLERSTEIN : Merci beaucoup pour cette séance et ces présentations. Cela a été très utile. Cela répond à certaines questions je me posais.

Par exemple Firefox, quand on navigue dans certains pays, on se rend compte qu'il y a ces systèmes comme cela qui ne fonctionnent plus. Est-ce qu'il s'agit des problèmes de sécurité ou pas ? Puis cela marche mieux parfois sur d'autres navigateurs. Est-ce que c'est le problème que Firefox a avec le DoH ou est-ce que c'est autre chose ? Ou est-ce que c'est quelque chose qui s'est perdu dans la conversation que les navigateurs ont entre eux et entre les autres serveurs ? Est-ce que vous pouvez nous expliquer un petit peu ? Je sais que c'est très technique mais j'aimerais bien comprendre un peu comment cela fonctionne.

PAUL HOFFMAN : Je vais répondre.

C'est technique, oui, mais ce n'est pas complètement ou seulement technique. La réponse à votre question est que non, ce n'est pas directement lié au DoH et ce type de choses qui viennent de Firefox, mais c'est lié de manière non technique parce que cela remonte à la question de Jonathan, c'est-à-dire « En qui est-ce que vous avez confiance ? ». Lorsqu'un navigateur va vérifier un site internet pour voir s'il est fiable, il faut qu'il y ait des règles au niveau interne qui

aient été élaborées en fonction de leurs propres règles, en fonction de ce que vous faites, etc. Différents navigateurs vont élaborer ces règles de manière différente à différents moments. Par conséquent, lorsque vous rencontrez un problème sur un site internet, cela dépend du lieu et du moment où vous le trouvez. Il s'agit d'une question de problème pour le navigateur. On a vu cela avec le DNS chiffré mais lorsqu'on aura cette discussion dans 10 ou 15 ans, je pense que la réponse sera que tout cela est lié, bien sûr.

JUDITH HELLERSTEIN : Pourquoi est-ce que le même site internet, si vous sortez des États-Unis, sera différent par rapport à ce qu'il est aux États-Unis ?

PAUL HOFFMAN : Le navigateur fait un choix pour vous. Ce choix n'est pas un choix technique, c'est un choix de confiance. Donc ils vont peut-être passer sur un trajet différent. Ils vont peut-être dire : « Je sais où vous êtes et l'emplacement où vous vous trouvez a des restrictions juridiques différentes. » Il y a des millions de décisions non techniques qui ont lieu dans les coulisses. Maintenant que nous avons un DNS chiffré, les systèmes d'exploitation et les navigateurs doivent choisir quel DNS chiffré, ces résolveurs récursifs auxquels ils vont faire confiance. Ce sont des questions qui vont être sur la table pour l'avenir.

JUDITH HELLERSTEIN : Merci beaucoup.

HOLLY RAICHE : Prochaine question d'un nouvel intervenant. Pouvez-vous ouvrir votre micro s'il vous plaît ? Apparemment, non.

Nous allons donc passer la parole à [Siva].Siva, êtes-vous là ? Vous avez une question ?

[SIVA] : Est-ce que vous m'entendez ?

HOLLY RAICHE : Oui, allez-y.

[SIVA] : Je comprends la question des serveurs d'autorité DNS avec les requêtes DNS. Mais malgré tout, est-ce que le titulaire du nom de domaine a un rôle à jouer ? Si j'ai bien compris, dans l'interface web, un titulaire de domaine doit mettre en place HTTPS. S'il ne le fait pas, le domaine passe par le protocole HTTP et HTTPS n'est pas utilisé. Est-ce qu'il y a un rôle qui correspond soit aux opérateurs de registre, soit aux titulaires de noms de domaine ? Je ne suis pas techniquement aiguisé sur le sujet mais j'espère que la réponse peut m'être apportée.

PAUL HOFFMAN : Je peux répondre à votre question simplement en disant que non, ce n'est pas lié. Votre question est raisonnable quand il s'agit du DNS qui peut aider à augmenter la protection de la vie privée, mais c'est en

dehors de la discussion que nous avons maintenant sur le sujet des requêtes qui vont vers les noms de domaine existants.

HOLLY RAICHE : Merci.

Nous avons une question de Thomas de la Commission européenne une fois de plus. Allez-y Thomas.

THOMAS DE HAAN : Vous m'entendez ?

J'ai une question sur les capacités du DNS pour le filtrage. Nous avons été approchés à la Commission par de nombreuses parties prenantes, des forces d'application de la loi, des ISP. Et on nous parle...

INTERPRÈTE : L'audio est inaudible.

THOMAS DE HAAN : ... pour voir si les chaînes sont affectées. On nous a posé la question de l'atténuation au niveau local pour les résolveurs. Il faudrait des directives pour le déploiement du DoH sinon, cela risque de créer des problèmes importants.

INTERPRÈTE : Nous nous excusons, l'audio était pratiquement inaudible.

PAUL HOFFMAN : Barry, vous voulez répondre à cette question ? Nous n'aimons toujours pas répondre aux questions qui incluent le mot loi.

BARRY LEIBA : Non, allez-y Paul.

PAUL HOFFMAN : Votre question, Thomas, était difficile. Je ne dis pas que c'est compliqué, je pense que c'est difficile. Il est difficile d'y apporter une réponse parce que comme l'a dit Barry, le document SSAC a essayé d'étudier cette question avec des perspectives différentes, beaucoup plus d'ailleurs que je l'ai fait dans le document de l'ICANN.

Au niveau des perspectives juridiques, comme vous le savez très bien, elles ont lieu à des emplacements complètement différents. Encore une fois, quand on vous dit : « Un utilisateur est dans tel endroit. » et en fait, cela correspond à plusieurs emplacements. En Europe, si je comprends bien, à n'importe quel moment, vous êtes dans une ville ou une municipalité – vous avez de meilleurs mots que nous aux États-Unis – vous êtes dans une région, vous êtes dans un pays et vous êtes aussi en Europe. Il y a des valeurs changeantes au niveau du mot Europe bien sûr, donc il peut y avoir des restrictions différentes dans chacun de ces emplacements.

Votre question dit : « Comment est-ce qu'un utilisateur va faire face à cela ? » La réponse est telle : ils ne vont pas bien faire les choses. Et la

question, c'est que vous aimeriez qu'ils fassent les choses d'une meilleure manière. Mais beaucoup de personnes qui sont là dans cette réunion aimeraient qu'ils le fassent d'une meilleure manière. Mais ils n'ont pas trop de moyens pour le faire. C'est une question que nous recevons depuis le début de l'internet : « Comment faire face à ces questions ? »

Avec le DNS chiffré, cela devient un petit peu plus difficile comme ce l'était quand on a commencé à avoir les HTTPS qui étaient chiffrés il y a 25 ans. Mais une de ces restrictions est celle-ci : en tant que gouvernement, j'ai besoin de savoir ce qui se passe de façon à prendre des décisions sur les politiques. Maintenant, vous pouvez voir ce qui se passe. Ou alors, une autre raison serait : vous pouvez seulement faire les choses qui sont autorisées si vous êtes dans une de mes régions. Et vous pouvez ainsi vérifier que cela est autorisé.

Ma réponse va être assez négative sur ce sujet. La bonne nouvelle, c'est que toutes les choses qui sont réglées quand il s'agit de cette question dans n'importe quelle partie de l'internet, pas seulement dans le DNS mais aussi sur le web, ces mêmes solutions pourraient facilement être transférées sur le DNS chiffré.

Barry, est-ce que vous pensez que ce serait la réponse que vous auriez apportée si vous aviez été un peu plus brave ?

BARRY LEIBA : Je vais rajouter quelque chose. Parce que Paul a parlé d'une personne étant en même temps dans plusieurs juridictions différentes. Cela

complique les choses parce qu'on utilise des choses différentes dans différentes juridictions. Vous pouvez être un Allemand qui se trouve aussi en Europe et vous utilisez un réseau géré au Pays-Bas, un logiciel qui a été créé en France et qui a été vendu par une compagnie au Royaume-Uni, votre stockage est dans un nuage aux États-Unis. Qui est responsable de quoi ? Pourquoi ? Quelle loi gère la situation ? Cela dépasse mon entendement, du moins, cela dépasse ma mission.

HOLLY RAICHE : J'apprécie la réponse. C'est difficile.

PAUL HOFFMAN : Avant d'avancer, Holly, puisque vous et moi ne nous sommes pas rencontrés, j'ai regardé votre biographie et j'ai vu que vous enseignez la loi dans un pays qui n'était pas sur la liste de Barry. Est-ce que vous pouvez d'ailleurs adresser la question ?

HOLLY RAICHE : J'enseigne la gouvernance de l'internet et je pense que j'aurais répondu un peu comme Barry l'a fait.

Quand on a un internet global, mondial avec des morceaux un petit peu partout sur la planète, la loi s'attache à des pays. On parle de lois nationales ou de lois étatiques. Là, l'interaction est problématique et c'est bon pour nous.

Quand les choses deviennent mondial, cela devient de plus en plus compliqué. Et la première chose que je dis à mes étudiants après que

je leur explique exactement ce qu'était l'internet, je leur dis qu'il est très difficile d'adresser les réglementations mondiales car le concept que l'on a de la loi est attaché à une juridiction où il y a des processus qui sont déjà en place pour élaborer ces lois. Et cela reflète les citoyens qui sont couverts par ces lois.

Il n'y a pas de façon adéquate de passer le bâton. Est-ce que j'ai expliqué de la bonne manière ?

PAUL HOFFMAN : C'est vous la professeure. Ce n'est pas moi, ne me le demandez pas.

HOLLY RAICHE : C'est une question difficile parce qu'il y a des juridictions qui se chevauchent et cela va au-delà de l'internet. Vous allez dire, comme l'a dit Lessig : « Le code, c'est la loi et n'y touchez plus. » C'est vraiment faire passer la patate chaude comme on dit.

Paul, vous êtes parti, vous m'avez laissée.

PAUL HOFFMAN : Non, je ne vous ai pas laissée. Vous êtes encore avec moi dans la même séance.

Puisque vous étiez la personne que je voyais sur le chat, comme Thomas était concerné par tout ce qui est loi et gouvernement, je sais que vous êtes avec nous, Suzanne, Rod, nous ne sommes pas de ce monde juridique. Il y a eu des questions au préalable sur le DNS

chiffré. Ces questions portaient sur les décisions au niveau local, sur l'ISP, qui fait ça, qui fait quoi. Après, on a commencé à parler de la loi. C'était des demandes, des attentes. On nous disait : « On s'attend à ce que vous fassiez cela et cela. » et on ne le faisait pas. C'est normal, les gouvernements ont l'habitude de procéder de cette manière.

Je vois dans le chat qu'il y a Patrik Fältström, qui est aussi un membre du SSAC, qui parle de ce qu'a dit Thomas. Patrick a travaillé sur ces questions depuis plus longtemps que moi, d'ailleurs. Ce genre de questions sont raisonnables, mais on ne s'attend pas à recevoir des réponses à ce sujet de la part des « techies ».

HOLLY RAICHE : Honnêtement, quand les personnes posent des questions juridiques, je dis : « Oui, ce sont des questions complexes parce qu'il y a plusieurs lois et elles sont contradictoires la plupart du temps. » Je n'ai pas la connaissance pour vous expliquer pourquoi cela est difficile puisqu'il y a plusieurs juridictions et pourquoi à la fin il est nécessaire de comprendre le cadre de travail juridique et technique. Et cela veut dire que les réponses ne sont pas faciles. Et bien sûr, comme on le voit à la fin de cette séance, les réponses ne sont pas faciles.

Dans le document de Barry, vous verrez qu'il y a des questions et cela correspond tout à fait à la situation. Ce n'est pas une tâche facile. Vous avez tous les deux bien expliqué le fait que cette tâche n'était pas facile.

THOMAS DE HAAN : Est-ce que je peux faire une remarque ?

La réalité est différente de la réalité internet virtuelle. Il faut que les résolveurs soient aussi locaux que possible.

INTERPRÈTE : Nous nous excusons, l'audio est presqu'inaudible.

HOLLY RAICHE : Merci.

Je vois qu'il reste une main levée. D'accord. Y a-t-il d'autres questions ?

Juste un rappel pour tout le monde, Paul a publié un document. Paul a même mis dans le chat le lien pour que vous puissiez aller consulter ce document.

Rod, vous aviez promis qu'on allait pouvoir lire le document SSAC très rapidement.

ROD RASMUSSEN : L'encre sèche encore sur le PDF. Le SAC109 sera publié et soumis au Conseil d'Administration, bien sûr. Et ensuite, je l'enverrai. Je suis désolé que ce document ne soit pas encore prêt.

Nous avions aussi préparé une présentation sur cela. Il y avait un petit changement avec ce qu'a dit Paul, il y avait quelques différences. Si

Andrew ou quelqu'un qui a le lien pouvait partager ce lien de cette présentation sur le chat, cela pourrait être utile.

HOLLY RAICHE : Oui, s'il vous plaît, mettez ce lien dans le chat. Cela veut dire qu'il y aura plus d'informations pour toutes les personnes comme moi qui absorbent toutes ces informations. Nous pourrons revenir dessus, lire la présentation, le document, etc.

Nous en sommes maintenant à la fin de cette séance. Je voudrais vous remercier tous les deux. En fait, je remercie toutes les personnes qui ont mis des commentaires et posé des questions dans le chat, c'était très intéressant. Merci Paul, vous avez expliqué quelque chose qui était très complexe et vous avez simplifié les choses. Merci Barry, vous nous avez aidés à mieux comprendre les choses. Et merci à tout le monde.

Avec cela, je voudrais clore la séance avec un grand remerciement. J'espère que tout le monde va essayer de se documenter et de lire un peu plus pour avoir plus d'informations. Merci.

Cette séance est maintenant close. Merci.

[FIN DE LA TRANSCRIPTION]