SINGAPOUR – Atelier d'At-Large : cadre de référence et mécanismes alternatifs de nommage pour le DNS
Lundi 24 mars 2014 – 17h00 à 18h00
ICANN – Singapour, Singapour

EVAN LEIBOVITCH : Bonjour ou bonsoir à tous. Merci beaucoup d'être venus, je sais qu'il est tard, il est déjà 17h00 ici à Singapour et je sais que le gala est ce soir, nous serons très heureux de nous y rendre. Nous avons un sujet important dont nous devons parler. Je m'appelle Evan Leibovitch, je suis vice-président de l'ALAC basé à Toronto au Canada et je serai votre hôte aujourd'hui. Lorsque nous parlons des gTLD et des noms de domaines, parfois on ne pense pas à des approches alternatives qui permettraient d'obtenir les informations que l'on désire sur l'Internet, et cette séance est une introduction à ces mécanismes, une introduction à ces différents termes de référence.

Nous aurons deux intervenants aujourd'hui, Patrik Fältström n'est pas là car il a une journée très chargée, mais je suis très heureux que vous ayez choisi de venir ici ? Nous pourrons nous informer les uns et les autres de ces mécanismes de dénomination. Nous n'avons pas de transparents pour cette présentation mais nous avons deux présentateurs ainsi que des transparents pour la seconde présentation. Le premier intervenant vient d'Amérique du Nord, où il fait encore nuit, Dave Piscitello, vice-président pour la sécurité et la stabilité de l'ICANN, venu nous donner une petite introduction et nous parler des différents concepts, à vous Dave. Il n'y a pas de transparents pour cette présentation, veuillez simplement écouter Dave.

DAVE PISCITELLO : Merci Evan.

EVAN LEIBOVITCH : Nous vous entendons avec un peu de difficultés.

DAVE PISCITELLO : Je vais commencer par dire que je n'ai dormi que quelques heures, puisque je suis en Amérique du Nord, mais ce que j'aimerais faire, c'est commencer à parler un peu de ces noms de substitution aux DNS et revenir en 2006, pour parler de ce que la SSAC avait effectué à l'époque. J'aimerais poser des questions auxquelles vous pourriez répondre, nous ne sommes que deux personnes cet après-midi, peut-être que nous entendrons Garth Bruen. J'espère que vous apprécierez votre gala plus tard. Vous pouvez poser des questions, nous pouvons simplifier un peu la séance. Toujours Dave Piscitello au micro, vice-président de la sécurité coordination technologie de l'information et de la communication TIC.

À la base, nous avons plusieurs noms mis en contexte, et nous avons le DNS public qui permet aux personnes d'affecter des noms, et des noms d'utilisateurs qui sont plus à propos que les adresses pour les différentes ressources sur l'Internet, pour les différents serveurs. Un des besoins pour avoir ces noms, c'est qu'ils doivent être gérés, une administration globale doit être faite. Nous avons un système d'identification, des identifiants, et au niveau d'une gouvernance mondiale, cela pose de grands problèmes. Nous avons eu beaucoup de différents systèmes de noms de domaines, depuis les années 70, nous

avons eu différents systèmes d'opération [Technet ? SNA ? Zeroxpark ? XNS ?].

Tous ces noms d'espaces n'étaient pas obligatoirement utilisés, mais il y avait certains critères pour l'utilisation de ces noms de domaines, pour ces différents scénarios, et lorsqu'on a commencé à utiliser le DNS au milieu des années 1980, nous avons établi un système de délégation des noms. Nous avions ces noms de domaines génériques, comme nous les appelons, et nous avons identifié ensuite des différents noms d'espaces utilisés par des pays, les ccTLD. D'ici la fin des années 90, des personnes avaient des noms internationalisés et la racine a connu une grande expansion dans le cadre des nouveaux TLD, donc aux environs des années 2000. En 2006 j'ai fait un rapport pour la SSAC, le rapport 0009 de la SSAC sur ces noms de substitution possibles aux DNS. La SSAC a parlé de ce concept.

Pourquoi utiliser des noms autres que les DNS ? C'étaient des mécanismes de dénomination différents qui permettaient d'éviter les collisions de noms qui existent parfois sur l'Internet. Ce qu'on essaye de résoudre comme problèmes, c'est un véritable désir de changer le contrôle administratif. Si vous regardez SSAC 009 vous avez des alternatives commerciales. Certains étaient pratiquement en signe de protestation politique. Il y a environ huit ou neuf ans, on utilisait des systèmes un peu similaires. Pourquoi avoir aujourd'hui des noms de substitution aux DNS ? Peut-être pour éviter ces collisions de noms, pour avoir un peu plus de possibilités administratives pour gérer ces noms de domaines, [Ces gels ?] d'étiquetage de noms de domaines pour les gTLD. Vous pouvez résoudre certains problèmes avec cette

approche, lorsque vous allez écouter Garth et que nous allons passer aux questions.

Quels sont les problèmes que vous allez essayer de résoudre ? Quelles sont les conséquences, les avantages de ce système alternatif ? En 2006 on pensait que dans certains cas il y avait un sacrifice qui était fait. Il y avait moins de capacité et de fonctionnalité, c'était parfois moins pratique, ça dépendait des navigateurs et des applications qu'on utilisait. Lorsqu'on crée des noms d'espaces, une certaine balkanisation se produit lorsqu'on sacrifie cela. Un autre aspect important, lorsque vous êtes dans le DNS public, vous allez faire des suppositions. Quel impact allez-vous avoir et quelles conséquences non anticipées allez-vous obtenir si vous ne pouvez pas contrôler et avoir une séparation totale des noms de domaines dans une organisation ?

Une autre supposition que vous allez faire dans le cadre des termes de référence, quelle protection allez-vous obtenir avec les termes de référence et quelles raisons vont être, pour les connexions avec différences hautes ? Par exemple quand il y a un système de cryptage. C'est une dernière chose dont j'aimerais parler, parce que moi je fais partie de l'équipe sécurité et j'ai certaines inquiétudes au niveau du système actuel du DNS et de son utilisation par des cybercriminels. Il me semble qu'il faut prendre en compte ces inquiétudes qui existent et les changements DNS. Il va y avoir d'autres utilisateurs et d'autres applications à l'avenir.

Quelle sera la visibilité de tout cela ? C'est tout à fait essentiel. Je crois que l'évolution de l'utilisation de l'Internet va être très marquée dans les années à venir. À une époque, nous n'avions pas le DNS, demain

nous aurons autre chose. Nous avons adapté nos produits et je crois que le DNS ne va plus suffire et sera peut-être moins important demain. Ce sont des questions que j'aimerais lancer pour le débat, et je vais redonner la parole à Garth.

EVAN LEIBOVITCH : Oui, nous allons donner la parole à Garth Bruen qui est Président du NARALO et membre de l'ALAC, qui travaille avec acharnement aux questions de conformité qui se posent. Des transparents vont être projetés, j'espère que nous allons pouvoir les voir.

GARTH BRUEN : Merci Gisella. Premier transparent : Pourquoi cette séance ? On a déjà eu des informations intéressantes de Dave Piscitello. Pourquoi cette séance ? Cela prête déjà à confusion. Je suis Garth Bruen, Président du NARALO. J'ai demandé à ce qu'on fasse une séance de ce type parce qu'on en parle pas assez à l'ICANN. Il y a des systèmes dont on ne parle pas assez à l'ICANN parce que les structures dont nous parlons aujourd'hui ne sont pas opérationnellement du domaine de l'ICANN. Il y a plusieurs raisons pour cela, on peut en parler. Il est important de savoir que ces autres systèmes existent, qu'ils ne font pas partie des contrats de l'ICANN. Ce n'est pas bon ou mauvais mais ce sont des faits que j'aimerais présenter.

Nous devons créer des politiques solides et nous devons prendre des décisions à former. Nous devons savoir qu'il y a des centaines de systèmes de noms de domaines et de systèmes de dénomination qui existent. Des personnes pensent que ce sont des menaces, que nous

devons les ignorer, on peut parler de cela. Si on voit un besoin pour d'autres systèmes, l'ICANN devrait-elle l'ignorer ou essayer d'atteindre tout le monde ? Conceptuellement, voilà à quoi cela ressemble. Le DNS, c'est là où travaille l'ICANN, ce n'est pas tout l'Internet, c'est une toute petite partie d' l'Internet. Vous avez tout un espace de l'Internet et des Protocoles Internet et vous avez une petite partie avec du contenu encore plus petit intégré aux DNS, vous voyez à quoi cela ressemble.

Qu'est-ce qui se passe dans tout cet espace protocole Internet ? Il est intéressant de se poser la question. Trois points : d'autres structures, des domaines sans point et des domaines Tor. Nous avons d'autres systèmes de racines, il existe plus de 400 TLD qui ne sont pas ICANN, il pourrait y en avoir plus, ce sont les seuls que je connaisse. Ils ont été publiés, ils ont été découverts, on en a parlé, on a analysé cela. Deux personnes ou un groupe de personnes peuvent créer leur propre TLD et avoir leur propre protocole pour se parler, personne ne le saura mais ça peut se faire. Ça peut exister, par exemple la racine Cesidian plus de 100 TLD, space.name plus de 90 TLD. New.net, je ne sais pas le statut de cette procédure judiciaire contre l'ICANN, il y a New Nations, OpenNIC, il y avait des anciens qui n'existent plus : eDNS, [Dipperdome ?], AlterNIC, Open RSC.

Les différentes raisons pour ces systèmes de noms de domaines alternatifs. Il y avait plusieurs raisons, pour point-space, c'était la concurrence, pour les consommateurs qui se sentaient restreints par l'ICANN, point-Cesidio pour l'indépendance politique, c'est une entité souveraine qui va avoir son propre nom de domaine et ne répondre à personne, point-bit c'est économique, c'est le Bitcoin, utilisé pour les payements par Bitcoins, cette monnaie virtuelle alternative, point-jack,

c'était en mesure de protestation lorsqu'ils ont lu le travail qui avait été fait par le groupe de travail sur le réseau, en 2000 on nous a parlé de racines alternatives, et point-jack a alors dit qu'ils se lançaient. Nous avons point-pirate qui est interdit, qui a été créé pour effectuer des téléchargements sans censure.

La SSAC a parlé de cela, des noms de domaines sans point. C'est bien ce que ça veut dire, un domaine qui n'a pas d'extension, qui n'a pas de point, comme .net. « Comment ça peut marcher ? Il faut ce point », allez-vous me dire. Eh bien, une table, une adresse Internet protocole, il n'y a pas besoin de point. Les nodes de l'ARPANET n'avaient pas de point, les noms existaient avant qu'on ne lance ce système de noms de domaines avec des points. Les « domaines » Tor, ce n'est pas exactement un DNS, Tor n'est pas un système de nom de domaine, c'est différent. Ce sont des identificateurs de sites uniques qui sont appelés des domaines mais qui ne peuvent pas être atteints par le DNS, par le système de nom de domaine. Ce sont des services cachés, en quelque sorte.

Par exemple point-onion, qui peut être utilisé seulement depuis un navigateur Tor. C'est comme à l'ancienne avec ces fichiers hôtes que nous avions. Tor ce n'est pas pour la dénomination, Tor est un système qui permet d'ajouter des couches pour le routage, pour l'obscurité du trafic, pour l'anonymat, on ne voit pas l'origine, on ne voit pas la destination dans l'Internet, on trouve la voie la plus rapide possible, Tor au contraire ce sont des déviations très nombreuses. Voilà à quoi ressemble le routage par Tor, voilà comment Tor fonctionne, cela crée des routes beaucoup plus longues afin de cacher les différents points et la manière dont on va d'un point à un autre et vous pouvez imaginer, ça

ne va pas très vite, c'est très lent. C'est très obscur, c'est anonyme, mais ce n'est pas rapide, comme notre DNS que nous connaissons.

La question qui se pose est de savoir si c'est seulement pour les criminels, on parle beaucoup de cela. On parle du « marché noir », de la « route de la soie », là en effet, on utilise souvent cela dans la communauté Tor mais Tor n'est pas utilisé que par des criminels, loin de là, les criminels utilisent également très souvent les DNS. Des journalistes, des activistes, des victimes, des personnels des forces de l'ordre voulant être anonymes utilisent Tor. Tor est un logiciel et une collectivité, une communauté. J'ai rencontré des personnes du projet Tor et je leur ai demandé ce qu'ils pensaient. Ce que je peux dire c'est que c'est une communauté, avec des personnes, il y a un logiciel, un réseau, des donations, des bénévoles et ils n'ont pas l'intention de remplacer le DNS, mais ils veulent utiliser des logiciels libres et beaucoup d'anonymat, pour différentes raisons.

Les problèmes que cela pose, ceci est un aperçu très rapide de Tor, mais c'est vraiment très complexe. Des problèmes se posent. Cela prête à confusion pour les consommateurs, des collisions de noms peuvent exister lorsque nous avons les TLD, les noms de domaines qui sont similaires, parfois c'est l'utilisateur qui a un problème, ou il y a un problème technique, des problèmes juridiques. Je crois qu'il y a eu des poursuites judiciaires à ce niveau et la création de système alternatif avec leurs propres extensions TLD. Ils nous disent que les gTLD violent des noms Tor, donc il est question de poursuites judiciaires contre l'ICANN. Des questions de sécurité et de gouvernance se posent.

Est-ce que ces systèmes alternatifs sont une force ou une faiblesse ? Avec ces systèmes alternatifs, il n'y a pas d'échange d'argent, tout est gratuit. Il n'y a pas de coût pour ces domaines, comme par exemple avec le routeur de *The Onion*. Il n'y a pas d'archivage des propriétaires. Cela peut être inquiétant pour les personnes voulant lutter contre la criminalité, mais ils peuvent avoir leur propre système Whois s'ils le désirent. Il y a la question de responsabilité : Qui est responsable ? Est-ce qu'il y a une résilience dans ce système ? Est-ce qu'il y a des questions de sécurité qui peuvent se poser ? Nous avons des problèmes complexes au niveau du DNS, dans notre DNS officiel, mais au moins nous avons des entités, un forum où l'on parle à l'ICANN, et cela n'existe pas obligatoirement dans les systèmes alternatifs.

La grande question qui se pose est : « Un monde, un seul Internet. » Est-ce que c'est vrai ? Est-ce que nous pouvons arrêter ces systèmes alternatifs ? Je crois que ce sont des questions qu'il faut se poser. Est-ce qu'il serait nécessaire, et même possible d'arrêter un système alternatif ? Est-ce que c'est innovant, est-ce que ce sont des imitations ? Qu'en sera-t-il dans dix ans, est ce que ces domaines compterons ? On ne le sait pas. Seront-ils remplacés par une couche supplémentaire, plus efficace pour les utilisateurs finaux ? Toutes ces questions se posent. Est-ce qu'ils vont rester, dans plusieurs années, ces systèmes du style Tor ? C'est la question que je voudrais lancer.

EVAN LEIBOVITCH : Merci beaucoup Garth pour cette présentation intéressante. Nous allons à présent passer aux questions et réponses, veuillez s'il vous plait vous identifier lorsque vous prenez la parole, et parler lentement et

clairement. Nous sommes interprétés en trois langues et si vous voulez parler en Chinois, en Français ou en Espagnol, c'est tout à fait possible. Il y a des casques, émetteurs et récepteurs à votre disposition, du matériel pour l'interprétation simultanée. J'aimerais commencer par poser une question. Personnellement, ce que j'aimerais savoir concerne l'accessibilité. On a entendu parler de problèmes de gTLD non accessibles avec certains navigateurs. Est-ce que ça peut être plus difficile d'utiliser ces systèmes alternatifs ? Est-ce qu'ils limitent l'accessibilité à certains sites ? Sont-ils difficiles d'utilisation ?

GARTH BRUEN : Tout dépend de la configuration des logiciels, mais certains des packages d'Internet qui existent accèdent à tous les systèmes, c'est intéressant.

DAVE PISCITELLO : Une des choses qui a été découverte il y a sept ans, c'est que la façon dont la plupart des systèmes fonctionne dans le DNS, requiert une pré-configuration, une sorte de requête au niveau du DNS. Je pense que dans tous les cas que j'ai examinés, nous n'avons pas ce type d'arrangement que tous les systèmes qui fonctionnent de manière commerciale au sein d'IANA en terme de coordination dans le système opératif la façon dont ce système commence.

ALAN GREENBERG : Deux commentaires. D'abord pour répondre à la dernière question de Garth, pour savoir ce qui sera là dans dix ans avec le système de DNS actuel, il y a une période qui peut être longue au niveau des

changements technologiques. Le temps que cela prend de démontrer quelque chose dans un laboratoire, par exemple. C'est une question d'années, il y a des choses qui apparaissent plus rapidement, mais ce n'est pas le cas de beaucoup de choses. Cela signifie que lorsqu'on essaye de prédire ce que seront les choses dans cinq ou six ans, on peut dire que ces choses fonctionnent déjà, et ce qu'il faut savoir, c'est qu'est-ce qui va continuer à fonctionner. Je ne sais pas si le DNS sera encore en fonctionnement dans cinq ou six ans, le monde est beaucoup trop complexe et c'est difficile de prédire, il y a trop de variables qui entrent en jeu.

Pour analyser certaines choses qui ont leur propre fonctionnement, il suffit de regarder Tor, mais il y a aussi Skype. Une fois que Microsoft l'a repris, il a été utilisé sur le système de mobile et il a commencé à avoir sa propre évolution, son propre développement. Skype a eu la possibilité de passer d'un réseau à l'autre et il a utilisé son propre système de nommage à l'intérieur du DNS. Une chose courante qu'on utilise tous mais qui ne représente pas une menace pour nous, c'est Skype. Beaucoup de choses dans ce monde sont potentiellement dangereuses et si tout le monde essaye de construire son propre système Skype et arrête d'utiliser le DNS, nous allons avoir de gros problèmes. Mais certaines personnes le font, soigneusement et sans trop d'erreurs et à ce moment-là ça fonctionne.

EVAN LEIBOVITCH : Allez-y Dave.

DAVE PISCITELLO : Il me semble que l'on considère la façon dont les noms de domaines étaient utilisés dans les années 90-99, si on regarde maintenant comment nous les utilisons sur des appareils portables et systèmes mobiles, nous utilisons la voix, et qui permettent de faire des recherches. Par exemple en cliquant sur ICANN sur un appareil mobile, on peut dire que nous avons déjà un moteur de recherche, que nous avions déjà ce moteur de recherche et qu'il utilise une langue naturelle. Un nom de domaine peut paraitre comme une marque et sur un appareil mobile ou sur PC aujourd'hui, on peut utiliser ces mêmes systèmes. Je pense qu'il y a ici une révolution, et il faut être sensible à certains changements qui ont eu lieu dans le marché au niveau des noms de domaines. Si on pense à ce qu'est l'Internet aujourd'hui, à son infrastructure, la chose la plus importante qui nous intéresse aujourd'hui c'est qu'il ne faut pas confondre les différents systèmes qui existent sur le Web actuellement. Une des premières choses qu'il nous faut penser c'est si c'est une discussion à propos de ce qu'est le nom de domaine et de ce qu'il signifie, s'il est articulé et s'il a une meilleure façon d'analyser cela, dans la mesure où le nom de domaine est de plus en plus intégré dans les différents systèmes selon le type de recherche qu'on veut faire sur Internet. Quel est le rôle que joue ICANN ou le rôle que joue la communauté multipartite dans l'administration de ce type d'espace ? Nous pouvons également nous poser cette question.

EVAN LEIBOVITCH : Bien, ensuite nous avons Eduardo.

EDUARDO DIAZ : Merci Evan. J'ai une question concernant le réseau Tor en lui-même et sur sa relation par rapport à la possibilité de faire de l'espionnage sur Internet. Peut-on faire de l'espionnage à travers le réseau Tor ?

GARTH BRUEN : Excusez-moi, j'étais en train de parler avec Gisella. Pouvez-vous répéter Eduardo ?

EDUARDO DIAZ : Oui Garth, lorsqu'on parle d'espionnage sur Internet, est-ce que le réseau Tor est inclus ?

GARTH BRUEN : Tout d'abord, ça peut inclure n'importe quoi. C'est une histoire complexe, parce que le gouvernement américain a créé Tor. Ça a été créé dans un laboratoire de l'armée, de la marine, et nous avons une réponse très spécifique.

EVAN LEIBOVITCH : Ok Alan, allez-y.

ALAN GREENBERG : Deux choses. Quand on dit que nous avons récemment découvert certaines choses. Je me souviens d'une discussion que j'ai eue avec des ingénieurs senior en 1995, il y a 19 ans de cela, de ce qu'étaient les principaux hubs aux États-Unis -MAE-East et MAE-West-, et chacun d'entre eux avait un gros câble utilisé pour capturer tout le trafic pour le gouvernement. Pour répondre à votre question spécifique, ça

fonctionne sur le réseau IP et c'est visible sur les principaux routeurs hub. La question est de savoir dans quelle mesure ça peut reconnaitre le trafic et le décoder, mais je pense que oui.

NIELS TEN OEVER : Je pense que nous devons être un peu plus précis si nous parlons de Tor. Il y a eu des diapos très explicites de la NSA qui montrent que la NSA ne peut pas suivre ce trafic et on suppose qu'il y a eu des implantations directes dans les anciennes versions de Firefox. On a essayé de cibler les utilisateurs mais ce n'était pas un groupe important, et avant que le patch n'apparaisse, l'équipe de Tor avait déjà son propre patch. L'agence de sécurité est assez lente et c'est très difficile de rompre l'action de Tor. Il y a une attaque au cours de laquelle l'agence de sécurité nationale a essayé de couvrir l'ensemble du réseau et en faisant une attaque pour voir d'où venait le trafic et pour voir s'il pouvait réduire ou situer l'endroit où se trouvait les utilisateurs. Nous ne pensons pas qu'ils aient la possibilité de le faire actuellement, donc on peut dire que si on veut être anonyme sur Internet, Tor est la meilleure option.

EVAN LEIBOVITCH : Je pense qu'il faut aussi tenir compte du fait que dans le passé il y a eu un moment où l'Agence de Sécurité Nationale nous disait qu'ils ne faisaient rien et en réalité ils faisaient quelque chose. Ce que vous dites c'est que la NSA dit qu'ils ne peuvent rien faire mais je ne suis pas sûr qu'on puisse les croire.

NIELS TEN OEVER : Je reviendrai sur ce point. L'agence de sécurité ne nous le dit pas, on l'a constaté, ce sont des fuites. Je voudrais également répondre à ce qui a été dit à propos de l'argent investit dans Tor et qui a été développé dans les laboratoires de l'armée, ça a été développé par une organisation qui est autre chose, qui n'est pas du tout créée par les militaires, ils n'avaient rien à voir dans tout ça, ça a toujours été en open-source et basé sur les protocoles de meilleures pratiques. Il ne faut pas insinuer quelque chose qui n'est pas vrai.

DAVE PISCITELLO : Je ne veux pas dire que je ne suis pas d'accord avec vous pour savoir si l'Agence de Sécurité Nationale peut ou ne peut pas décrypter Tor, mais je dirais que les services des forces de l'ordre, les gens cherchent des occasions et l'année dernière avec le FBI ils ont fait des recherches sur ce réseau Tor et ils ont trouvé un cas d'abus d'enfants et je pense qu'il y a une série de choses qui sont conflictuelles lorsqu'on parle des personnes qui surveillent Tor en temps réel, lorsqu'on parle de la possibilité de réduire ces encryptages de Tor. Puisque les communications Tor sont anonymes, il n'y a pas de processus actif pour bloquer. Il n'y a pas d'agence civile ou de forces de l'ordre qui puisse le faire. On est anonyme et tout le monde l'est, le trafic est encrypté et c'est un grand défi, il est presque impossible de le décrypter. Par ailleurs il faut s'assurer que le DNS n'est pas le seul système et théoriquement il est pratiquement impossible de le faire aujourd'hui.

EVAN LEIBOVITCH : Merci Dave. La prochaine question est posée par un monsieur qui lève la main, veuillez vous identifier s'il vous plait.

WARREN KUMARI : Je suis Warren Kumari et malheureusement je suis arrivé en retard, donc arrêtez-moi si ceci a déjà été abordé. Une des préoccupations que nous avons, c'est le DNS. Si on envoie des emails et que quelqu'un n'a pas le navigateur Tor installé, cela cause des problèmes. Un travail qu'Andrew Sullivan et moi-même avons rédigé au niveau de l'IETF afin d'essayer de trouver des solutions pour atténuer ce problème en utilisant ce qu'on appelle les noms de type DNS, et lorsque les personnes l'utilisent dans un contexte non DNS, on suggère qu'une étiquette soit réservée quand il s'agit d'un espace « Ultimate Name », on va mettre une étiquette à la fin pour montrer que c'est différent d'un contexte DNS. C'est un TLD dont ils donnent le nom, si quelqu'un veut me poser des questions sur ce point, venez me voir et je vous donnerai d'avantage de détails.

EVAN LEIBOVITCH : Si vous avez accès à Adobe Connect, vous pouvez donner la possibilité à quelqu'un de mettre ce lien sur le tchat, comme ça nous pouvons donner la possibilité aux gens d'y accéder. Nous avons à présent Garth, Bruen puis Guisella Gruber qui va lire quelque chose sur la salle Adobe Connect.

GARTH BRUEN : Juste pour revenir à un point concernant la sécurité de Tor et les questions du public : Est-ce que vous avez des préoccupations concernant la sécurité d'exit nodes ?

NIELS TEN OEVER : Il y a eu plusieurs documents théoriques qui ont été faits et également des recherches qui pouvaient être engagées à propos d'exit nodes possiblement compromis. Parmi les menaces qui existaient, il est clair que le trafic à l'intérieur du réseau Tor est encrypté entre les nodes mais n'est pas encrypté à partir du node de sortie, donc il est possible pour les forces de l'ordre de suivre ce node et de capturer par conséquent le trafic. Il serait cependant difficile de revenir à la source du trafic, donc il ne sera pas impossible d'avoir un système pour suivre ce trafic, mais il sera difficile de trouver la source de ce trafic. Il faudra utiliser un système de navigateur, c'est pour ça que le navigateur Tor rend les choses encore plus difficiles. Donc oui, c'est un problème, mais pas obligatoirement pour le DNS.

GARTH BRUEN : Pour un réseau Tor end to end de personnes, la personne qui est directement à côté de toi le sait.

EVAN LEIBOVITCH : Dave, avez-vous quelque chose à ajouter à cela ?

DAVE PISCITELLO : Non, je crois que nous avons dit plus ou moins ce que nous savions sur le Tor.

EVAN LEIBOVITCH : Ok, maintenant nous allons donner la parole à Gisella qui va lire un commentaire dans la salle Adobe d'un participant en ligne.

GISELLA GRUBER : Merci Evan. Il s'agit de Poomjit, membre de NCUC de Thailande : « Je serais curieux de savoir quelle application de tchat est actuellement la plus sure pour l'utilisateur ou pour les activistes et journalistes, notamment pour les activistes qui doivent travailler et vivre dans une crise politique tendue ? »

EVAN LEIBOVITCH : Je ne suis pas sûr que ce soit totalement applicable à ce sujet, mais si quelqu'un a une recommandation, nous pouvons mettre ça dans la salle de tchat et revoir cela. Je sais qu'l y a quelques applications qui permettent un tchat sécurisé, mais je pense que beaucoup d'autres gens en ont aussi. Si vous avez quelque chose, mettez-le sur le tchat en ligne pour nous aider. Est-ce qu'il y a d'autres questions ? Nous avons ici des gens qui sont très capables, donc c'est le moment de leur poser des questions. Je voulais juste ajouter un point personnel, et rappeler aux gens qu'il y a un groupe de paramètres gTLD créé par la GNSO pour essayer d'engager le choix des consommateurs.

Du point de vue du programme des gTLD, une des choses qu'ALAC a essayé de faire, c'était de s'assurer que les paramètres ne disait pas seulement que c'est un meilleur choix parce qu'on a une centaine de TLD au lieu d'en avoir seulement une vingtaine, mais on veut s'assurer que les paramètres tiennent compte également de la popularité du DNS et la possibilité pour cela, c'est que s'il y a une confusion des consommateurs concernant ce gTLD, ça va mener les gens vers des alternatives, le Tor ou des médias sociaux et d'autres sites. C'est quelque chose qu'il faut souligner en termes d'alternative. Je vais

revenir maintenant à mon époque d'UUCP et cette histoire de routeur onion m'a rappelé un peu nos recherches du début, lorsque nous commencions à travailler sur les TLD de premier niveau.

GARTH BRUEN : Je voudrais voir si on peut continuer à développer cette discussion. J'ai demandé à des gens du projet Tor de présenter une discussion plus étendue, lors de la prochaine réunion et on peut demander à un groupe d'étudier les DNS alternatifs, et peut-être qu'At-Large peut publier des informations à ce sujet.

EVAN LEIBOVITCH : Comme Président de cette réunion, nous avons ici des gens qui sont vraiment des experts dans ce domaine. Je vois Glenn par exemple, on peut leur demander de venir nous voir pour créer ce groupe.

GLEN MCKNIGHT : Je voulais juste reprendre ce que Garth a dit. Evan et moi allons être à la réunion du FTEI à Toronto au mois de Juin et au Mois d'Octobre, et pour nous c'est une très bonne discussion, et j'aimerais faciliter aux mois de Juin et Octobre au Canada ce type de discussions, donc venez me voir, venez voir Evan, et nous en discuterons un peu plus pour mettre cela en place.

EVAN LEIBOVITCH : Il nous reste dix minutes, et je vois ici des gens qui veulent prendre la parole. Eduardo.

EDUARDO DIAZ : Je suis curieux, j'ai entendu parler du navigateur Tor avant. Si j'utilise Tor, je peux vraiment naviguer sur Internet, mais la seule chose c'est que personne ne va savoir d'où je viens, c'est ça ?

GARTH BRUEN : C'est exactement ça.

EVAN LEIBOVITCH : Nous avons des participants à distance, veuillez parler dans le micro je vous prie.

EDUARDO DIAZ : Excusez-moi, Monsieur le Président. Puis-je reprendre sur ceci ? Si j'utilise un navigateur Tor pour naviguer sur Internet, de quel espace alternatif parle-t-on, et cela veut-il dire que je peux atteindre cet espace alternatif avec mon navigateur ?

GARTH BRUEN : L'espace est séparé du concept de Tor, le système alternatif qu'il y a est un système qu'on ne peut pas atteindre à travers un DNS, on peut le faire d'autres façons.

EDUARDO DIAZ: Pour finir on parle de deux choses. Le Tor est une chose et l'espace alternatif en est une autre ? Ok alors, merci.

NIELS TEN OEVER : C'est Niels Ten Oever d'Article 19 et NCUC. Il y a d'autres raisons d'utiliser les adresses onion, c'est la résilience de texte qui peut être faite dans le réseau Tor, donc c'est une raison autre que la censure. Ce qui est peut-être une des choses les plus intéressantes concernant le système de domaine alternatif, c'est qu'on peut interagir. Et je voudrais attirer votre attention sur un projet Tor2Web qui permet d'atteindre des adresses à travers un proxy. Ça peut être une façon de relier certains domaines.

EVAN LEIBOVITCH : Pouvez-vous mettre ce lien de nouveau Sur Adobe Connect ? Ce serait formidable. Nous arrivons à la fin de notre session. Oui Dave, Allez-y.

DAVE PISCITELLO : Si vous avez créé ce groupe, vous allez peut-être voir…

EVAN LEIBOVITCH : Nous avons de gros problèmes pour vous entendre Dave. Désolé, Dave parle de la recommandation SSAC 009, c'est bien cela ?

DAVE PISCITELLO : Oui, il me semble que ça nous permettrait d'identifier les principaux problèmes, d'essayer d'identifier cinq différentes classes de noms d'espaces alternatifs. Nous parlons ici de systèmes de noms commerciaux, de systèmes de noms politiques etc. Ce sera peut-être donc une technologie utile pour revisiter et voir les nouveaux problèmes et si ces problèmes continuent à apparaitre. C'est un premier point. Le deuxième point, c'est peut-être la façon de conclure ici cette

session, lorsqu'on parle de systèmes de noms alternatifs, je me demande ce qu'on va sacrifier, il faut voir dans quelle mesure le DNS est intégré et la façon dont ces applications vont se comporter, ainsi que nous-mêmes.

Donc le problème je pense, c'est que nous devons analyser l'évolutivité contre le contrôle du système. L'autre problème c'est les défaillances et la capacité à continuer dans un environnement de ce type. Si vous voulez contrôler l'évolution et aller au-delà d'un système de contrôle tel qu'il existe actuellement –ce système est important pour beaucoup de gens- et la balkanisation. On a un scénario dans lequel on aurait des TLD bloqués. C'est une situation à laquelle nous allons répondre et je pense que l'autre aspect dont Garth a parlé, je ne pense pas que vous ayez oublié dans cette discussion de parler de la transparence de l'espace de nom et du système de bureau d'enregistrement.

EVAN LEIBOVITCH : Bien, merci beaucoup Dave. Garth vous pouvez conclure si vous le voulez. J'aimerais continuer cette discussion dans de futures réunions ? Merci à tous. J'espère que cette session a été pour vous une source d'informations. En tout cas ça l'a été pour moi. Bonne suite de conférence. Une dernière chose, je voudrais remercier les interprètes qui sont au fond de la salle et qui ont souffert. C'est une grande fierté de savoir qu'ALAC a un service d'interprétariat, ainsi que le GAC mais je crois que nous l'avons eu les premiers. Les personnes qui sont là-bas dans le coin, le personnel d'ICANN qui a fait tout son possible et qui ont écrit des petites notes, qui ont arrangé les projecteurs, etc. Merci à vous

également, les personnes qui s'occupent de l'audio, les techniciens, bravo à vous.

GARTH BRUEN : Il y a des autocollants Tor au fond de la salle, pour ceux qui sont intéressés.