NATHALIE PEREGRINE: La conférence est maintenant enregistrée et je m'occupe de l'appel. Bonjour à tous et bienvenue à la conférence du groupe de travail At-Large chargé des technologies en ce 16 novembre 2015.

À la conférence aujourd'hui nous avons Alexis Anteliz, Harold Arcos, Lutz Donnerhacke, Klaus Stoll, Vernatius Ezeama, Carlos Quintana, Gordon Chillcott, Stuart Clark, Glenn McKnight, Maureen Hilyard, Dev Anand Teelucksingh, Alfredo Calderon, Carlos Watson.

Notre orateur invité pour les projets clés est David Goulet. Il est en ligne avec nous. Bienvenue David.

Olivier Crepin-Leblond nous a présenté ses excuses.

Pour le personnel nous avons Terri Agnew et moi-même, Nathalie Peregrine.

Je vous rappelle de bien donner votre nom avant de parler pour les besoins de la transcription. Merci beaucoup et c'est à vous Dev.

DEV ANAND TEELUCKSINGH: Merci beaucoup Nathalie. Merci de participer à cette conférence. Je sais que c'est probablement la première conférence du groupe de travail At-Large chargé des technologies pour certains d'entre vous. Je pensais donner un rapide aperçu de ce qu'est le groupe de travail At-Large chargé des technologies.

J'ai donc rassemblé quelques diapos. Le groupe de travail At-Large chargé des technologies évalue et examine la technologie de l'information et des communications (TIC) qui peut aider la communauté At-Large (l'ALAC, les RALOs, les structures At-Large) à mieux accomplir leur rôle au sein des activités de l'ICANN.

Tous ceux qui s'intéressent à la TIC et à la manière dont elle peut s'appliquer pour répondre aux besoins de l'At-Large et des autres communautés de l'ICANN sont invités à se joindre au groupe de travail At-Large chargé des technologies Vous pouvez le faire en envoyant un e-mail au personnel At-Large, à l'adresse e-mail du personnel.

Juste pour vous donner quelques (inaudible) activités réalisées entre l'ICANN 53 et l'ICANN 54, les deux réunions publiques de cette année, nous avons examiné Kavi comme outil possible de gestion de politique de projet. Nous avons étudié la technologie telle que Teamup, c'est un calendrier de groupe qui est utilisé par le sous-comité de sensibilisation et d'engagement de l'ALAC.

Nous avons également eu des discussions concernant les questions relatives à la liste de diffusion LACRALO. Nous avons également eu des discussions avec des personnes de LACNIC pour discuter de leur processus d'élaboration de politiques, et avons observé leurs outils. Nous avons également observé pour la première fois l'application mobile ICANN qui était en version bêta pour la réunion de Dublin.

Je voudrais juste dire que tout ceci est ouvert à tous les membres At-Large provenant des cinq régions ICANN : Amérique du nord, Amérique latine, Caraïbes, Afrique, Asie, Australie, Iles Pacifiques et Europe.

Pour conclure rapidement, le groupe de travail At-Large chargé des technologies a des membres venant de la communauté At-Large et d'autres membres des AC et SO. Nous avons désormais des personnes du GAC qui rejoignent le groupe de travail. Nous avons une ou deux conférences téléphoniques par mois. Il y a ici deux liens où vous pouvez trouver plus d'informations. De la documentation que nous avons établie pour la communauté At-Large en termes d'outils de traduction et ainsi de suite.

Je voudrais maintenant vous parler du pourquoi nous avons cette conférence aujourd'hui. C'est l'une des recommandations du sommet At-Large. Pour ceux qui ne savent pas, le sommet At-Large est une réunion de tous les représentants At-large qui s'est tenue pendant l'ICANN 50. Lors de cette réunion, tous les représentants At-Large ont développé (inaudible) recommandations et des observations. Il y eut en tout 43 recommandations. Vous pouvez les trouver en suivant le lien de la présentation.

Certaines de ces recommandations ont été données à la TTF en coordination avec certains autres groupes de travail pour la mise en œuvre. L'une des recommandations était la recommandation 17 qui affirme que l'ICANN doit être sensible au fait que les médias sociaux sont bloqués dans certains pays, et en lien avec des organismes techniques promouvoir des alternatives crédibles.

Nous avons examiné des services de chat comme Slack et Hipchat. Mais nous avons aussi commencé à en examiner deux qui pourraient être utilisés pour contourner les sites Internet bloqués.

Il y a eu des discussions au sein de ce groupe pour savoir si nous devrions prendre en considération le fait d'utiliser ces outils, et nous avons décidé que nous devons avoir quelques conférences téléphoniques pour vraiment comprendre certaines idées relatives à ces outils. Et l'un des outils les plus populaires est le projet Tor. C'est là où intervient notre orateur invité, David Goulet, impliqué dans le projet Tor. Il a gentiment accepté de venir à la conférence. Je voudrais maintenant donner la parole à David pour qu'il fasse sa présentation. David, vous avez la parole.

DAVID GOULET: Bonjour. Je suis David. Je viens de Montréal, donc je suis Franco-canadien, donc je m'excuse pour mon accent. Vous aurez peut-être des problèmes pour m'entendre ou me comprendre mais je vais essayer d'être le plus concis possible. Je suppose que vous avez toutes les diapos. Je ne peux pas les contrôler, je vais donc demander à quelqu'un via la ligne. Je dirai : diapo suivante.

Tout d'abord, merci beaucoup à Glenn de m'avoir invité. Je l'ai rencontré à Montréal et il m'a gentiment invité sur le projet Tor.

Nous allons commencer avec la première diapo, l'introduction. Je travaille sur le projet Tor depuis un an maintenant. J'ai été volontaire pendant trois ans avant mon travail. En tout, cela fait quatre ans que je suis sur le projet Tor. Nous avons une mission mondiale. Vous pouvez le lire ici. Je ne vais pas le relire, mais il s'agit de technologie, de défense de la vie privée. Nous faisons beaucoup de recherches. Nous avons au moins trois universités dans le monde qui font des recherches actives

avec le réseau Tor. Et nous avons beaucoup de diffusions en termes de liberté de parole, de censure, de contournement et autres.

Si vous passez à la diapo suivante, qu'est-ce que Tor ? Le projet Tor a été créé par le NRL, le laboratoire de recherche de la marine aux États-Unis. Cet homme, (inaudible), et quelqu'un d'autre, je ne me souviens pas bien.

DEV ANAND TEELUCKSINGH: On dirait que quelqu'un…continuons David. Voyons si le son (inaudible) et a été résolu.

DAVID GOULET: En gros, il a été créé pour ajouter un moyen de communiquer à travers l'Internet dans un certain anonymat pour préserver la vie privée de tout utilisateur. Bien entendu il y avait derrière ça des idées militaires et à l'heure actuelle c'est devenu un projet. Je ne connais pas les spécificités, mais Tor est maintenant un logiciel qui est utilisé pour l'anonymat en-ligne. C'est une source ouverte complète. Tout ce que nous faisons est une source ouverte. Nous n'avons rien qui est en vente ou autre. Tout notre travail est transparent sur Internet, ce qui veut dire que les listes de diffusion sont (inaudible). Nous avons des propositions ouvertes, etc.

Cette communauté a donc un peu grandi en termes de chercheurs, de développeurs, d'utilisateurs et bien entendu, d'opérateurs. Je vais maintenant passer à ce que sont les opérateurs.

Pour le moment, notre financement vient en grande partie du gouvernement américain, donc le DOD (Department of Defense) et le

DOJ (Department of Justice). Ça dépend de l'année où nous avons des subventions. À l'heure actuelle je ne connais pas les détails, mais la plupart de notre argent provient du gouvernement américain. Nous avons également des fondations.

Nous travaillons (inaudible) des sources de financement. Si vous passez à la diapo suivante qui est (inaudible) pour les personnes au sein des États-Unis. C'est un 501(c)(3), qui est pour les gens au sein des USA, c'est une organisation à but non lucratif. Aux USA nous avons un bureau à Cambridge, et notre objectif, à nouveau, est en lien avec la recherche et le développement d'un champ relatif à l'anonymat.

Voyons cela. Si vous passez à la diapo suivante, diapo quatre, nous avons cette statistique qui, la dernière fois que j'ai vérifié, estimait 2,1 millions d'utilisateurs Tor. Cela signifie que sur le réseau nous avons cette quantité d'utilisateurs à tout moment.

Si vous passez à la diapo suivante, vous avez un graphique, qui est directement connecté aux utilisateurs. C'est seulement pour 2015. Vous voyez que c'est stable autour de 2,1 peut-être 2,2 millions d'utilisateurs.

D'ailleurs, je vais utiliser plusieurs graphiques pendant la présentation et vous avez l'adresse en bas de chaque graphique qui est, je crois, metrics.torproject.org. Tous ces graphiques sont accessibles. Vous pouvez modifier les dates, télécharger PDF, etc.

Je vais maintenant passer à ce qu'est le modèle Tor dans la prochaine diapo. Avant de commencer, il va y avoir quelques parties techniques et d'autres moins techniques. Je crois que nous avons (inaudible), mais Tor est un projet énorme, donc l'objectif est vraiment de vous faire

comprendre l'ensemble du projet en termes de technologie mais aussi en termes de communauté et d'importance des utilisateurs car, en dehors de la partie technologique, il touche également les humains.

Je vais commencer par la diapo relative au modèle de menace. Tor a maintenant dix ans. Nous avions en tête ce qu'une personne malveillante peut faire lorsque vous avez ce réseau. Dans cette diapo, imaginez que le réseau d'anonymat peut être Internet (inaudible) et nous avons Alice et Bob qui sont connectés. Il y a donc plusieurs points d'attaques où la personne malveillante peut écouter ou même regarder ou attaquer un ou deux participants.

Passons à la diapo suivante, la sept. Il y a un aspect très important que vous devez comprendre avec le réseau Tor. Il s'agit d'anonymat, pas de sécurité. Ce que je veux dire c'est que nous fournissons de l'anonymat sur la couche de transport, mais le problème ensuite est que vous avez toujours la couche de l'application avec un risque de fuite lorsque vous entrez dans le réseau Tor, ou lorsque vous quittez le réseau Tor. Heureusement, lorsque vous entrez, nous réglons le problème de la fuite de contenu, mais lorsque vous sortez du réseau, c'est un autre problème.

Dans ce cas, nous voyons que l'anonymat est une question d'encodage. Nous avons « Salut Bob », « Salut Alice », bla, bla bla. C'est du charabia. Ce n'est toujours pas de l'anonymat car, comme nous le savons maintenant, merci à notre ami Snowden, c'est que beaucoup de données sur Internet sont surveillées, (inaudible) à partir de métadonnées. L'anonymat devient ici très important.

Si nous passons à la prochaine diapo, la huit, tout ceci n'est pas très réaliste en termes de technologie mais aussi en termes de loi. Si nous avons des agences gouvernementales ou des sociétés ou des gouvernements, il y a des déclarations qui affirment, « Je promets que je ne regarderai pas. Je promets que nous n'espionnons pas nos citoyens. Nous n'allons pas lire vos e-mails », ou autres. Tout ceci n'est malheureusement pas encore assez. Nous avons plein de phrases dans cette diapo qui vous disent simplement que ce n'est pas possible d'avoir de l'anonymat juste en disant qu'on peut prouver que c'était moi.

La diapo suivante, diapo numéro neuf, nous avons les différents intérêts des différents groupes d'utilisateurs. Cette question d'anonymat ne peut pas juste s'appliquer au gouvernement, qui était le premier dans la base de Tor il y a dix ans. L'objectif était de fournir un anonymat à des agents sur le terrain ou des militaires ou des officiels du gouvernement pour des entreprises étrangères.

Mais la donne a un peu changé. Aujourd'hui, nous avons des activités liées aux droits de l'homme, aux entreprises, aux citoyens privés évidemment, aux gouvernements. Ça s'est élargi à…vous pouvez voir (inaudible) ici. Les citoyens privés seraient des citoyens normaux. Tout le monde sur le terrain. Nous connaissons des agents provenant non seulement des USA mais aussi d'autres gouvernements qui l'utilisent partout dans le monde. On a besoin ici de ces quatre aspects différents, qui sont (inaudible), la sécurité du réseau, bien entendu la vie privée. C'est le vieux concept. Et le trafic (inaudible) est également un bon (inaudible). Et nous avons cela car il y a beaucoup d'ennemis, d'adversaires, qui essaient de retirer le principe de l'anonymat de Tor. C'est une sorte de course.

Si nous passons à la diapo suivante, numéro 10. C'est le plus simple design que vous pouvez voir. Je vais progresser (inaudible) expliquer ce qui vient avec ça.

Nous avons Alice et Bob qui vont sur Gmail et qui échangent. Bien entendu c'est un problème car si vous passez à la diapo suivante, la 11, il s'avère que (inaudible), ils réalisent des écoutes illicites ou autres. Également de la censure. (inaudible) un seul point de défaillance.

Heureusement, l'Internet que nous connaissons aujourd'hui est un web. C'est redondant. Nous empruntons des voies différentes, en fonction des défaillances ou non. Mais nous utilisons toujours Gmail dans notre vie quotidienne, qui est (inaudible).

Voilà donc la règle d'application. Je comprends, mais quand même, que nous comptons sur ce même réseau et ainsi de suite qui sont contrôlés par des entités seules. C'est donc un problème pour l'anonymat.

Passons maintenant à la diapo 12. Nous avons ensuite cette idée. Nous allons ajouter de multiples relais pour qu'aucun ne puisse (inaudible) Alice, dans le cas présent. Plus nous diversifions vos chemins de destination, plus nous pensons qu'il est difficile d'attaquer Alice, d'écouter Alice ou autres. La censure également (inaudible).

Tor veut dit The Onion Routeur. Il y a une raison qui explique l'idée d'oignon. Nous allons voir ça dans la diapo 13, qui montre que chaque relai…Alice va communiquer via chaque relai et ensuite (inaudible) Bob. R1 dans ce cas est donc le nœud d'entrée, et ensuite R2 le nœud du milieu, et pour finir R3 le nœud de sortie. Et il existe M3 et le milieu dans le réseau Tor qui sont des propriétés très différentes. Nous

espérons qu'ils se comportent comme les autres, comme tout autre nœud, mais ils ont toujours des rôles différents.

Dans ce cas, ce qui va se passer c'est qu'Alice va créer un chemin vers Bob, et dire « Bon, je vais prendre R1, R2 et R3 et je connais ces relais d'un document connu, « que nous appelons le consensus. Le consensus est créé par neuf répertoires d'autorités dans le réseau Tor. Malheureusement je n'ai pas de diapo pour illustrer ça. Mais nous avons à l'heure actuelle neuf serveurs autour du monde qui sont gérés par des personnes de confiance et ces serveurs sont responsables de mesurer, non pas mesurer mais créer ce que nous appelons le consensus qui est un document sur lequel tout le monde est d'accord et qui contient tous les relais du réseau Tor qui sont utilisables. En gros, le document détaille chaque relai avec leurs empreintes clés (inaudible). Cela signifie, l'importation IP. Et d'autres informations utiles.

Dans ce cas, lorsqu'Alice commence, le premier pas qu'elle fait est d'obtenir ce consensus car ce consensus est la visualisation du réseau. Si elle a déjà un consensus global, elle va essayer d'obtenir un consensus via un répertoire cache c'est-à-dire n'importe quel relai dans le réseau Tor en fonction de certaines exigences, mais presque tous les relais. Ou, si elle n'a pas de consensus, ce document, elle va demander à ces neuf répertoires. Et elle sait ça car ces répertoires d'autorités sont codés dans le code de Tor.

Il y a donc des clés publiques et également leurs adresses et d'autres choses utiles. C'est complètement codé sous R. Donc chaque client, chaque relai Tor, tout ce qui utilise le réseau Tor sait comment obtenir ces répertoires (inaudible).

Revenons à notre diapo, Alice a mis à zéro le réseau. Elle peut ensuite choisir R1, R2 et R3. En gardant ça à l'esprit, au sein du consensus, chaque relai a une clé. Une clé publique est assignée au sein du consensus. Elle sait donc qu'elle peut coder une connexion à R1 et R3.

Si vous regardez la diapo, il y a une couche très claire. Vert, jaune et bleue. La première couche est R1. R1 est la clé verte. Lorsqu'Alice code, elle aura cette ligne blanche qui correspond au contenu, et ensuite elle réalisera trois couches pour chaque (inaudible). Elle renverra ensuite (inaudible) au R1. R1 supprime la couche, sait où l'envoyer ensuite, ce qui correspond aux informations dans les paquets. L'envoyer ensuite au R2. R2 supprime la couche, la couche jaune. Et R3 supprimera la dernière couche.

R3 est donc un nœud de sortie, et R3 a accès au contenu qui a été initialement codé. Vous voyez la ligne blanche. C'est important.

On en revient à l'anonymat face à la sécurité. En tant que serveur mondial…une personne malveillante étant R1, R2 ou R3, vous ne savez pas d'où ça vient. Vous ne savez pas ce qu'il y a dans les données, au milieu. Mais la sortie sait. La sortie sait où ça va et quel est le contenu mais elle ne sait pas d'où ça vient.

Donc avec Tor vous avez vraiment besoin de sécurité et également en termes d'encodage. Que vous utilisiez SSL, OTR, PGP ou autres, la sortie ne peut pas venir fouiner dans vos données.

Si vous passez à la diapo suivante, diapo 14, c'est une jolie couche d'oignon. À chaque relai nous épluchons la couche.

Je vais garder du temps pour des questions, donc n'hésitez pas. Ça peut parfois être compliqué. Passons à la prochaine diapo, la 15.

Voici le nombre de relais que nous avons à l'heure actuelle dans le réseau Tor. Nous l'avons relevé hier soir. Je crois que nous avons autour de 6 800 relais. Cela veut dire que les gens font fonctionner les relais. Un relai est donc géré par toute personne qui désire le faire. Nous avons des volontaires tout autour du monde.

Prenez note de ça car cela donne une incroyable visualisation du réseau Tor. Vous pouvez aller sur torflow.uncharted.software. Si vous allez sur le lien, c'est une incroyable visualisation de tout notre réseau autour du monde.

Et des ponts. Nous avons 3 000 ponts. Je n'en ai pas parlé. Les ponts sont des relais qui ne sont pas affichés dans le consensus. La raison est que lorsque vous réalisez une censure auprès d'un pays ou d'une organisation ou autre, l'un des (inaudible) du réseau Tor, j'avais une diapo sur ça, est de bloquer toutes les IP relayées car elles sont connues, vous pouvez obtenir ce consensus.

Mais les ponts ne sont pas dans le consensus, il y a donc différentes manières d'obtenir des ponts. Je ne sais pas si j'ai une diapo sur ça, mais par exemple, il y a une manière d'envoyer un e-mail à une adresse e-mail spécifique et vous recevrez les ponts par e-mail. Ensuite vous prenez ces ponts, vous les insérez dans votre configuration Tor et ce sera votre point d'entrée du réseau Tor. Puisque personne ne le sait, ni pour le consensus, vous pouvez éviter la censure. Je vais revenir sur les ponts avec les attaquants actifs que nous avons.

Si nous passons maintenant à la prochaine diapo, il s'agit de la bande passante de relais totale, diapo 16. Vous pouvez tout de suite voir que pour notre bande passante affichée, c'est-à-dire chaque bande passante de relais affichée, nous avons des autorités en charge de la bande passante qui mesurent les relais et essaient de faire une estimation pour que l'on puisse faire une sélection de chemins beaucoup plus intelligente. Dans ce cas, nous avons une bande passante de 140 gigabits par seconde. Et nous pensons que cette bande passante est ce qui est utilisé. Mais c'est une estimation. Ce n'est pas si précis, mais ça nous donne une idée.

Si nous passons à la diapo suivante, numéro 17. La course aux armes, c'est important pour nous. Nous avons pas mal de (inaudible) sur Internet pour diverses raisons, surveillance, censure. Vous imaginez ce qu'un pays ou un régime peut faire lorsqu'ils piratent votre Internet.

Si nous passons à la diapo suivante, numéro 18. J'ai mentionné ce qui peut être fait pour bloquer les réseaux Tor. Il y a plusieurs façons. Tout d'abord, bien entendu, bloquer le (inaudible). Il y en a neuf. Ils sont connus. Et si vous les bloquez tous, alors personne ne peut réaliser l'amorçage car ils ne pourront pas avoir de consensus, ce document qui explique et détaille la visualisation du réseau.

Ça a été fait dans certains pays, dans plusieurs pays, mais il y a un moyen de contourner ça. C'est pourquoi (inaudible) cache existe, que chaque relai peut mettre en cache le consensus. Mais bien entendu à un moment donné vous avez besoin de réaliser le démarrage, mais vous pouvez avoir un consensus dès le départ, de quelqu'un d'autre, et

ensuite commencer le démarrage, etc. Ce n'est pas le moyen idéal. Comme je le disais, on peut aussi bloquer toutes les IP des relais.

En filtrant des aires sur l'empreinte réseau de Tor. Lorsque Tor se connecte de relais en relais, il utilise le TLS. Et au sein de cette session TLS il y a ce qu'on appelle la peau de l'oignon et les couches de l'oignon. Il y a donc beaucoup d'encodage, mais pour cette question de TLS, nous essayons d'examiner le plus possible les HTTP mais ce n'est pas toujours facile. L'autre chose est donc d'empêcher les utilisateurs de trouver le logiciel Tor.

J'ai quelques diapos à vous montrer représentant une copie écran de pages de torproject.org qui vont être détournées dans différents pays pour vous montrer comment elles empêchent les utilisateurs de faire ça.

Prochaine diapo, la 19, est un exemple d'utilisateurs connectés depuis l'Égypte. Si vous vous rappelez de l'Égypte, vous pouvez voir cette ligne baisser. Elle correspond au moment où, pendant trois jours, si je me souviens bien, ils ont complètement fermé Internet. Vous pouvez voir que cette chute a été assez significative et ces points montrent les moments de censure. C'est basé sur une estimation. Vous pouvez avoir plus d'informations (inaudible) torproject.org.

Mais c'est quelque chose d'intéressant où vous pouvez voir comment les pays essaient en fait de faire de la censure ou les mouvements qu'il y a sur Internet.

Je vais vous montrer sur la prochaine diapo, la diapo 20, qui parle de la Libye. Lorsque la guerre a commencé en Libye il y a quatre ans ou

quelque chose comme ça, vous pouvez voir cette importante baisse lorsqu'ils ont complètement chuté. Je pense qu'ils ont même fermé Internet pendant un moment. Ensuite ça recommence à monter.

Mais cette importante ligne qui monte à presque 300 utilisateurs, correspond à des périodes d'importantes activités politiques dans le pays. J'ai plusieurs graphiques. J'en ai choisi quelques uns. Mais pour le Congo, l'Ukraine, j'en avais un autre. Je ne me souviens pas du pays. Où vous pouvez voir (inaudible). Vous pouvez voir toutes ces périodes de censure ou ces évènements politiques avec une augmentation des utilisateurs Tor.

Si vous passez à la diapo suivante, la 21, il s'agit de l'Iran. L'Iran a été l'un des pays les plus actifs dans le blocage de Tor. Ils l'ont fait de plusieurs façons. Mais d'une façon ou d'une autre, en janvier 2011 ils ont trouvé comment faire et ça a chuté. Presque zéro client. Et si je me souviens bien, je vais peut être dire une bêtise, ils ont bloqué Tor à partir du TPI d'Internet et ils ont trouvé un moyen d'identifier une connexion TLF. Si ma mémoire est bonne, Tor a juste modifié un des éléments TLF et nous sommes revenus en arrière et sommes passés à travers le pare-feu de l'Iran. Vous pouvez les voir surtout avec (inaudible) toutes nos mesures. Assez impressionnant.

Le dernier graphique que j'ai maintenant est la diapo 22, la Chine. La Chine est un sacré adversaire. Ils sont assez impressionnants. Ils ont bloqué Tor de plusieurs façons. Ils ont réussi à bloquer Tor en utilisant les quatre moyens possibles de le faire. L'une des choses qu'ils ont faites est de dénombrer les ponts. Je pense qu'il y a trois ou quatre manières différentes d'obtenir un pont soit par e-mail, vous vous rendez sur le

pont torproject.org et ensuite à partir de là vous avez un pont. Il y a donc plusieurs façons. Ils (inaudible) tous et les ont tous bloqué. Il n'y a pas seulement ça, mais maintenant nous savons que lorsqu'il y a une connexion TLS qui a l'air suspecte ou autre, ils se connectent à vous pour essayer de prendre les empreintes. C'est une des manières qui est assez efficace pour bloquer Tor. Ces graphiques montrent qu'au milieu des années 2010 ils ont assez bien réussi. Celui-ci est un vieux graphique mais je pense que jusqu'à 2015 c'est à peu près la même chose.

Diapo suivante, la 23. Les deux prochaines diapos sont des pages que les gens obtiennent dans différents pays pour torproject.org. L'une des manières d'intervenir ou de censurer ou de stopper torproject.org serait juste de ne pas vous autoriser à télécharger le logiciel.

Le premier que vous voyez, les Émirats-Arabes Unis, Bahreïn. Ils ont l'air sympa. C'est un clown sympa. Pas un clown mais une femme qui vous dit juste que ce n'est pas bien et que vous devriez naviguer en toute sécurité. Ce projet Tor n'est pas bien, d'accord ?

Si vous passez à la diapo suivante, la 24, il y a des personnages sympathiques qui vous disent que c'est un problème etc. Donc lorsque les gens vont sur le projet Tor et voient cela, ils ne pensent pas que c'est de la censure. Ils pensent que c'est pour leur bien. C'est un sacré problème en fait.

Si l'on passe maintenant à la diapo 25, à quoi nous attaquons-nous ? Je vous ai un peu parlé de la Chine. Nous avons des pare-feux du gouvernement. (inaudible) contre l'Iran contre la Chine. Nous savons qu'un groupe de pays essaie de le bloquer ou (inaudible) de l'éloigner.

Même les entreprises américaines ont des logiciels dédiés qui le bloquent.

L'une des choses (inaudible) est également (inaudible) fournit une option pour leurs utilisateurs pour bloquer Tor, et je pense bien entendu qu'ils bloquent Tor en bloquant les IP ou en obtenant la signature TLS. Mais c'est toujours quelque chose qui est mis dans de plus en plus de produits commerciaux pour bloquer les utilisateurs Tor.

Si nous passons à la diapo suivante, l'Iran en 2015. Vous pouvez voir qu'ils l'ont à nouveau bloqué. À chaque fois c'est une réponse aux activités politiques ou alors ils achètent du nouveau matériel informatique, ou à un moment donné ils cherchent une manière de tout filtrer;

Cette course aux armes à laquelle nous faisons face est à l'heure actuelle une course permanente. Nous voyons ces évènements de censure se dérouler dans chaque pays à tout moment. Un groupe de pays (inaudible), mais il y a plus (inaudible).

Si vous passez à la diapo 27, tel un réseau d'anonymat, la sécurité de Tor vient de la diversité des utilisateurs. Disons que si vous êtes dans un pays, un (inaudible) pays, et que vous êtes le seul utilisateur de Tor. Vous allez vous faire fortement remarquer. C'est assez facile de voir le trafic Tor.

Donc la base de Tor et de son anonymat reposent sur la diversité tout comme le fait d'avoir le plus d'utilisateurs possible. Tant qu'il y a de l'activité, il y a de l'anonymat car ensuite vous ressemblez à tout le monde.

Le point numéro deux est que 50 000 utilisateurs en Iran signifie que la plupart d'entre eux sont des citoyens normaux d'une certaine manière car ils ont tous un trafic normal. Et plus vous avez d'utilisateurs plus il y a de chances d'anonymat car moins il y a d'utilisateurs plus ils sont faciles à repérer.

Il y a cette histoire concernant un étudiant (inaudible) qui a en réalité utilisé le réseau Tor pour envoyer un e-mail à…je ne me souviens plus s'il s'agissait de chantage ou autre chose. Mais il était tout seul sur le réseau, donc c'était facile de l'atteindre. La diversité ainsi qu'une grande quantité d'utilisateurs sont donc deux choses très importantes pour l'anonymat.

Diapo 28. C'est une pièce du puzzle. Nous avons vu avec la dernière équipe de piratage et (inaudible) fuites, qu'ils vendent des logiciels espions aux entreprises, aux gouvernements ou autres et l'un d'eux espionnait les utilisateurs de Tor. Nous supposons donc que c'est une pièce du puzzle mais ce n'est pas une preuve de solution complète car si vous avez du matériel informatique ou un logiciel qui est attaquable…un logiciel espion. Avez-vous une copie authentique de Tor ?

Pour la partie technique, (inaudible) récemment, il y a un an je crois, peut-être moins. Nous avons créé cette chose appelée la construction productive. Tor est construit à partir de différentes machines par différentes personnes et elles correspondent au même (inaudible) au final. Cela veut dire que c'est la même copie partout, ce que nous appelons la construction productive.

Nous avons cette personne géniale à Tor qui travaille sur ça et qui a crée productive-build.org ou quelque chose comme ça, et maintenant

(inaudible) a presque 80-85 % si ce n'est 100 % de leurs packages étant construits de manière productive.

C'est un gros effort pour Tor, donc lorsque nous fournissons le code binaire de Tor aux personnes autour du monde, nous savons que c'est la copie exacte.

Si nous passons à la diapo 29, c'est une diapo concernant les documents secrets de la NSA qui ont été gérés par Snowden. Ils n'aiment pas du tout Tor. C'était en 2012, donc il y a trois ans. C'est donc (inaudible). Mais oui, ça pue et ils n'aiment pas ça du tout.

Si nous passons à la diapo 30, ce logo était au sein d'une diapo et avec cette citation nous observons toujours (inaudible). Ils ont dit que (inaudible). Nous ne le pensons pas. Il y a plusieurs autres séries de réseaux qui utilisent différentes choses comme (inaudible) ou d'autres alternatives. Ce sont des modèles commerciaux différents. Ils ont différentes manières de faire de l'anonymat sur Internet. Mais au final, Tor est celui qui a été étudié par la NSA. Nous le savons grâce à ces diapos. Nous savons qu'il a de l'ampleur.

Je ne sais pas si vous le saviez, mais il y a deux ou trois jours il y a eu une histoire selon laquelle le FBI a en réalité financé une université pour (inaudible) les utilisateurs de Tor, ce que nous avons réglé en juillet dernier. Juillet il y a un an. Cette recherche sur l'anonymat des utilisateurs de Tor a abouti et ils ont donné au FBI des adresses IP pour pouvoir réaliser des condamnations.

Nous savons de fait que Tor est utilisé par de mauvaises personnes. Ça nous le savons. Mais nous pensons que ce n'est qu'une minorité. J'ai un graphique pour vous montrer cela.

La diapo 31 parle de la perception. Qu'est-ce que Tor ? Nous nous battons dans l'actualité à propos de ça (inaudible) Tor. En général lorsque quelqu'un entend parler de Tor il entend parler du côté obscur du web ou le 'web profond'. Nous essayons de ne pas utiliser ces expressions, car pour nous, Tor permet juste un accès Internet différemment mais d'une manière qui protège votre vie privée.

C'est donc un gros problème de perception envers le public et aussi envers les gouvernements ou les agences qui voient Tor comme quelque chose de mauvais.

Si nous passons à la diapo 32, il y a plusieurs façons de (inaudible) Tor de manière légale. FSI (inaudible), par exemple. Faire fonctionner un relai de sortie est très difficile pour les FSI car ils obtiennent beaucoup de (inaudible) remarques ou plaintes car le trafic n'est pas toujours très net. Donc le FSI nous hait de plus en plus. C'est malheureux. Nous nous battons toujours mais nous résolvons cela la plupart du temps. Nous avons maintenant presque 7 000 relais.

(inaudible). C'est facile. C'est toujours un processus en cours pour les gens aux USA. On ne peut pas se rendre sur healthcare.gov via Tor. C'est dommage car vouloir protéger les informations liées à sa santé sur Internet ou à son état de santé ou juste essayer d'obtenir une assurance sont des choses pour lesquelles nous devrions fournir une certaine confidentialité (inaudible) et nous n'avons pas le droit.

Diapo suivante, la 33. Vous vous souvenez tous de Snowden. À cause de (inaudible) en haut à droite, et il est également défenseur de Tor. Nous avons eu un afflux d'utilisateurs et d'intérêts de plusieurs manières car son histoire a fait le tour du monde.

Si vous passez à la diapo 34, c'est un gros travail de (inaudible) de connecter les utilisateurs. C'est également plus ou moins lié à un réseau zombie qui était actif sur Tor et nous avons quadruplé notre nombre d'utilisateurs. Nous avions plus de 5 millions d'utilisateurs. Ça c'est avec le réseau zombie, mais il y a également eu un sacré effet Snowden après quelque temps, les gens disaient « Oh mais c'est quoi Tor ? Pourquoi est-ce que cette personne l'utilise ? » Il y a eu un certain intérêt.

Juste pour vous dire que cette ligne est revenue lorsque nous avons éliminé le réseau zombie, mais il y a toujours 2 millions d'utilisateurs, pas 1 million, donc l'effet Snowden a été très fort.

Si nous passons à la diapo 35, je ne me souviens plus pourquoi je l'ai mise là. Je pense que c'était supposé être avant. Mais oui (inaudible) en connectant les utilisateurs depuis la Turquie, et juste avant septembre, c'était…je ne me souviens plus. J'avais une note, mais je pense que cette diapo est juste (inaudible), donc passons à la diapo suivante, la 36.

J'en arrive à la fin de ma présentation. Je vais juste vous parler un peu des services cachés. Les services cachés sont quelque chose dont vous avez sûrement tous entendu parler, c'est en lien direct avec le côté obscur du web, ces adresses avec .onion.

Ce n'est pas une simple recherche du DNS. Un .onion est une adresse avec laquelle vous pouvez atteindre un service sur Tor. Le positif avec

(inaudible) service c'est que les clients entrent dans les réseaux et ne les quitteront jamais. Vous atteignez un service qui est à l'intérieur du réseau Tor donc vous ne passez pas par une sortie à mesure que vos données passent pas l'Internet clair et ouvert.

Je vais maintenant rester sur cette diapo 36. Nous avons (inaudible) et Facebook. Très récemment Facebook a créé sa propre adresse oignon. C'est super car ça fait une distinction entre l'Internet ouvert et le côté obscur du web, ou ce que nous aimons appeler l'espace oignon. Aller sur (inaudible) est pratiquement la même chose car vous allez sur Facebook via un .onion ou un .com. Pour nous, aller sur un .onion est juste un moyen d'atteindre un service de manière sécurisée, mais ça ne devrait pas être vu différemment de l'Internet ouvert. Il a des mécanismes différents, mais nous avons tous des mécanismes différents pour plein de choses autour d'Internet. Donc (inaudible) Facebook. Nous essayons de préconiser d'autres services pour offrir des adresses oignon car cela permet aux utilisateurs d'atteindre Facebook ou (inaudible) en utilisant l'anonymat mais aussi de manière très sécurisée. Je vais vous expliquer pourquoi ces services sont beaucoup plus intéressants.

Si nous passons à la diapo suivante, numéro 37. Il y a une adresse en bas car vous avez six ou sept images pour les services cachés. Pour vous expliquer tout de suite les choses, j'ai juste mis un graphique, mais ça montre l'ensemble. Vous avez cette adresse en bas et vous pouvez lire à propos de ça. Je vais faire cette introduction difficile de ce qu'est (inaudible) service ou du service oignon.

Vous avez donc Alice qui veut se connecter à Bob. Disons que Bob a un service Internet. Disons Facebook. Facebook veut offrir un service via un espace oignon. Maintenant, le service de Bob va se connecter aux trois points d'introduction, IP1, IP2 et IP3 que vous voyez sur l'image. Ces points d'introduction sont juste un circuit à travers Tor. Donc trois (inaudible) circuits comme nous l'avons vu avant la présentation. Et Bob va garder ce circuit ouvert aux IP.

Maintenant, Alice va (inaudible) se connecter à Bob avec cette adresse oignon, et elle sera capable de poser des questions via cette adresse oignon. C'est en gros un système à clé publique du (inaudible) et de certaines autres informations. La raison est que celle longue adresse vous donne un endroit pour aller sur une DHT, ce que nous appelons un répertoire de service caché, qui est en gros composé de relais qui correspondent au profil qui est disponible plus de 96 heures, rapide et avec une bande passante, ou d'autres exigences comme ça.

C'est une importante DHT, et avec l'empreinte digitale du (inaudible), du relai qui a le répertoire de service caché. Donc Alice va se connecter à (inaudible) car avec l'adresse oignon elle sait quel (inaudible) se connecter. Elle va télécharger ce qu'on appelle un descripteur de service d'agent qui est un document expliquant où entrer en contact avec Bob.

Dans ce document, il y a les IP, les points d'introduction des adresses 1, 2 et 3. Donc Alice se connecterait au point d'introduction, un des (inaudible) des points d'introduction. À ce stade il y a un circuit à partir de Bob qui est (inaudible) et Alice va leur faire appel. Donc Alice va dire à Bob « Rejoins-moi à ce point de rendez-vous. »

Donc Alice se connecte à l'IP1, et peut ensuite parler à Bob via ce circuit. Ensuite Bob se connecte au point de rendez-vous. Et Alice se connecte au point de rendez-vous et ils se connectent tous les deux et nous avons alors cette connexion totale entre Alice et Bob. Tout se passe à travers le réseau. Ça n'existe pas en dehors du réseau. Ils ont de bonnes caractéristiques de confidentialité et aucun contenu n'est divulgué à l'arrivée ou à la sortie du réseau Tor.

Il s'agit donc en gros de services cachés. N'hésitez pas à poser des questions car mon travail au sein de Tor aujourd'hui concerne en grande partie les services cachés. Si nous passons à la diapo 38, j'ai bientôt fini. Il s'agit de septembre. Non attendez, avant ça. C'est juste de septembre à novembre. Nous avons des statistiques des services cachés. Nous avons deux types de statistiques différents qui sont collectés de manière anonyme et qui nous donne la quantité de trafic sur le réseau Tor.

À l'heure actuelle presque 900 mégabits par seconde sur l'ensemble du réseau Tor concernent les services cachés. Je pense que ça représente autour de 5-6 % du trafic global du réseau Tor. C'est l'une des raisons pour laquelle nous avons utilisé ce graphique lorsque nous avons réalisé ce travail pour pouvoir montrer qu'en fait Tor ne représente pas tout le mauvais trafic qui passe par les services cachés que ce soit pour le trafic d'armes ou d'autres mauvaises choses comme le trafic d'êtres humains et ainsi de suite. Ce n'est pas vrai. Nous ne savons pas quel pourcentage cela représente mais c'est un très faible pourcentage du réseau Tor.

Si nous passons à la diapo 39, il s'agit de la quantité d'adresses oignon uniques que nous voyons au sein du réseau Tor. Environ 30 000

adresses vivantes. Gardez à l'esprit que les adresses oignon sont utilisées par des services comme un serveur HTTP, un serveur mail, mais aussi toute une série d'applications. L'un d'eux s'appelle Rickoshare. On peut se rendre sur rickoshare.im qui est une application de chat qui utilise des services cachés et vous pouvez discuter sur Tor. Il créé beaucoup plus d'adresses oignon. Mais à tout moment, 30 000. C'est notre estimation.

Si on passe à la diapo 40, c'est une copie d'écran du navigateur Tor. Ça montre comment la plupart des gens utilisent Tor. Donc si vous allez sur torproject.org, vous pouvez télécharger ce pack de navigation Tor. En gros c'est Firefix enrichi par les capacités de Tor et quelques divers (inaudible) de confidentialité.

Nous avons une grande équipe chez Tor qui travaille sur ça. Ce sont des gens formidables qui font un travail formidable. C'est une mission de travail incroyable qui renforce la productivité.

Pour finir, diapo 41. Il s'agit de (inaudible) sur mobile Android. Je ne sais pas s'ils ont maintenant l'iOS, mais (inaudible) vérifier cela. Mais au moins (inaudible) très bien. Vous pouvez utiliser Tor sur votre téléphone portable. Ça prend de plus en plus d'ampleur. Nous avons quelques personnes de Mozilla dans l'équipe Firefox OS qui travaillent avec nous sur la version mobile. Tor possède également un mode privé de Firefox qui pourrait être impressionnant en termes d'utilisateurs et d'atteinte. Mais voilà en gros comment ça fonctionne.

Je vais m'arrêter là. Merci beaucoup. J'en suis à 41 minutes cela veut dire que vous avez 20 minutes. Vous pouvez me poser autant de questions que vous voulez tant que je peux y répondre. Merci.

DEV ANAND TEELUCKSINGH: Merci, David. Merci pour cette présentation très instructive. Il y a quelques questions que les participants vont poser. Tout d'abord, Glenn. Glenn vous avez la parole.

GLENN MCKNIGHT: Merci. Et merci encore David pour votre présentation. Je voudrais lire quelques questions qui viennent du chat. Je voudrais revenir. Nous avons une question d'Alfredo Calderon de Puerto Rico. Il fait partie de l'ISOC de Puerto Rico. Sa question concerne…

Sa question concerne dot.dot.go. Il demande, « Est-il vrai que cela fait l'objet de publicité pour les écoles et les groupes privés ? »

DAVID GOULET: Donc dot.dot.go en tant que service, nous l'annonçons comme une solution pour Google face aux améliorations relatives à la vie privée. Car ils ne conservent pas de journal, ou les demandes de recherche. Oui c'est vrai. Si je comprends bien la question, oui c'est une amélioration par rapport à Google. C'est l'une des raisons pour laquelle nous avons en fait ajouté assez tôt une adresse oignon, pour que les gens puissent se joindre via un réseau anonyme et une certaine confidentialité. J'espère avoir répondu à votre question.

GLENN MCKNIGHT: Deuxième question du chat. Avis à tous, David n'est pas sur Adobe Connect, donc je prends la liberté de lire les questions qui sont posées.

La deuxième question est de Satish en Inde. Je crois qu'il vient de (inaudible). Il vous a posé une question David. Il est un grand fan et utilisateur de Tor depuis plusieurs années. Je pense que c'est très précieux et que ça sauve des vies. Vous avez mentionné la semaine dernière que SMU/SEI agissent conjointement avec le respect des lois. Tor parait plus vulnérable. Est-ce que c'est une pente glissante ?

DAVID GOULET: Question très intéressante. À l'heure actuelle, tout le travail réalisé chez Tor est une source ouverte. C'est notre meilleur effort. Nous avons des développeurs, des chercheurs. Je fais ça depuis des années. Je pense que nous faisons de notre mieux. Nous pensons que nos utilisateurs sont la chose la plus importante. La sécurité de nos utilisateurs est très très importante. C'est pourquoi tous nos processus de développement, nos processus de recherche, sont toujours basés sur la sécurité de nos utilisateurs, et le tout sans compromettre l'anonymat.

Nous aurons toujours à faire face à des menaces autour du monde, que ce soit au sein des agences gouvernementales américaines ou des universités qui essaient d'éliminer Tor car il vend beaucoup de papiers. Mais il améliore également la sécurité de Tor.

Nous devrions donc continuer à utiliser Tor. C'est certain. Plus nous obtenons de financement, plus notre organisation aura de la stabilité. Mieux nous arrivons à répondre à ces questions, plus nous pouvons améliorer les services.

Juste pour vous donner un exemple, je sais que nous avons une nouvelle génération de services cachés, une nouvelle proposition de

services cachés qui a été créée il y a trois ans, et les attaques face au FBI et à la CMU (Carnegie Mellon University) ne seraient pas possibles car nous sommes au courant de ces questions. Nous voulons toujours les régler, mais il faut un certain nombre d'efforts d'ingénierie et de recherches.

Je ne dirais pas que c'est vulnérable car nous, chez Tor, sommes très actifs quant aux dernières recherches, répondant aux menaces et faiblesses et nous faisons durer les informations pour le public avec notre blog et notre liste de diffusion et un nouveau logiciel.

Je ne dirais pas que vous êtes vulnérable mais gardez en tête que ce n'est pas une solution miracle. C'est le cas de n'importe quel logiciel.

DEV ANAND TEELUCKSINGH: Merci, David. Merci Glenn et merci David. Prochain orateur, Lutz Donnehacke. Lutz, vous avez la parole. Allez-y.

LUTZ DONNEHACKE: Merci. Merci pour cette super présentation. Je vois que beaucoup de services de l'ICANN vont exiger une identification et de vrais noms pour utiliser le service. Par exemple, la nouvelle plate-forme d'apprentissage demande à ce que vous donniez votre nom complet de façon à voir une simple vidéo d'introduction.

Ma question est, est-ce que nous avons de bons arguments pour dire aux gens au sein de l'ICANN d'arrêter de stopper l'anonymat des utilisateurs pour arrêter de chercher qui utilise tel ou tel service. Est-ce que nous avons un argument solide quant à la manière dont utiliser la

plate-forme d'apprentissage sans savoir qui accède aux fichiers individuels ? Merci.

DAVID GOULET: OK. C'est une question compliquée. Il y a beaucoup de raisons pour lesquelles vous pourriez soit vous connecter avec un vrai non ou pas. Peut-être sont-elles bonnes, peut-être pas. Mais vous devez garder à l'esprit que c'est plus un service de connexion avec de vrais noms, il créé une piste numérique de ce que la personne a fait ou est en train de faire. Ce sont des métadonnées qui sont très utiles dans la réalité de nos jours puisque nous sommes (inaudible) surveillance partout.

Maintenant si vous avez les données, cela veut dire que vous pouvez les rapporter à n'importe quelle agence qui a un mandat légitime ou autre. Mais les lois sont différentes aux quatre coins du monde. Ce n'est pas quelque chose de très stable. Cela veut dire que si, à un moment, vous avez des informations, elles ne seront peut-être pas utiles à un autre endroit du monde. Elles pourraient, ou non, être utilisées contre les utilisateurs.

Je dirais que s'il n'y a pas de réel besoin d'ajouter les noms mis à part un besoin statistique, par exemple, ou mieux de diffusion publicitaire, nous ne devrions pas le faire car nous pourrions perdre un peu de confidentialité. Et de plus, nous ne savons pas quelle sera l'utilisation peut-être dans le futur après quelques mois ou années. Ce serait également un argument en faveur de l'utilisation de vrais noms. Par exemple, si vous voulez parler sur le forum. Je veux savoir si je parle à Glenn ou pas. Mais ça dépend. J'utiliserai toujours cet argument de 'aucune donnée' (inaudible).

DEV ANAND TEELUCKSINGH: Merci David. Je vais regarder s'il y a d'autres questions. J'ai une question David. Vous en parliez plus tôt. Une grande partie de cela semble avoir été destiné aux ordinateurs de bureau. Mais à l'heure actuelle (inaudible) de plus en plus d'accès Internet se font sur les appareils mobiles. OK. Donc vous avez Android comme plate-forme de soutien, mais est-ce que Tor peut être installé au niveau d'un routeur pour que tous les appareils qui sont connectés à ce routeur puissent utiliser Tor ?

DAVID GOULET: Votre question est donc en rapport au fait d'avoir des routeurs. Alors, tous les appareils connectés à ce routeur pourraient-ils passer par Tor ? C'est bien la question ?

DEV ANAND TEELUCKSINGH: Oui.

DAVID GOULET: Oui c'est tout à fait possible. Il y a plusieurs façons de faire. Pour rappel, Tor fonctionne sur une couche de transport. En gros sur le TCP, ça fonctionne de façon à ce que vous soyez anonyme. Le problème est que chacune des applications, lorsqu'elles sont conçues aujourd'hui, divulguent une grande quantité d'informations vous concernant.

Ce qui veut dire que si vous avez dix appareils et que vous passez par un routeur, et que tout passe par Tor, alors tous ces appareils vont divulguer quelque chose de particulier sur vous via les nœuds de sortie.

Ça n'a pas été un modèle (inaudible). Ce fut un modèle (inaudible), mais ce n'était pas aussi sérieux qu'aujourd'hui, car nous savons aujourd'hui qu'il y a (inaudible) mondial sur Internet. Ce qui veut dire que lorsque vous avez (inaudible) mondial du réseau, c'est beaucoup plus difficile pour un réseau d'anonymat de fonctionner d'une manière telle que nous avons un pourcentage garanti que vous êtes complètement anonyme. Dans ce cas, si vous avez plusieurs appareils passant par Tor, tous divulguent quelque chose sur vous lors des nœuds de sortie car il faut bien que vous sortiez du réseau à un moment donné.

Gardez à l'esprit qu'il s'agit de quelque chose qui pourrait vous démarquer. C'est pourquoi le navigateur de Tor par exemple, essaie de vous faire ressembler à n'importe quel utilisateur, pour qu'on ne puisse pas prendre vos empreintes.

DEV ANAND TEELUCKSINGH: OK. Merci David. Je vois que Glenn a levé la main. Glenn ?

GLENN MCKNIGHT: Bonjour. J'ai une autre question de Satish Babu. Sa question est, « À quel point Tor est-il évolutif ? Si beaucoup plus d'utilisateurs commencent à l'utiliser, et que le nombre de nœuds reste sensiblement le même, est-ce que la performance sera atteinte ? De plus, est-ce qu'il y a une solution possible (inaudible) pour résoudre cette situation ? »

DAVID GOULET: Très bonne question. Nous avons toujours à l'esprit cette idée d'évolution. À l'heure actuelle nous travaillons activement sur

l'évolution des services (inaudible). Si vous vous souvenez de cette présentation, se connecter à un service caché est en réalité très intense sur le réseau et également en cryptographie. Vous construisez trois circuits différents. Ensuite vous vous connectez à cette autre personne. Il est question de beaucoup de cryptographie et beaucoup de bandes passantes sont utilisées juste pour la connexion.

Nous essayons de réduire cela de plusieurs façons. Nous avons créé un équilibre des oignons en dehors du (inaudible) programme de confidentialité, qui est en gros un programme GSOC, (Google Summer of Code). Et des services (inaudible) équilibre des oignons. Facebook est très intéressé par ça, et ils l'utilisent, ils testent la version bêta. Un faible équilibre est une adresse oignon via de multiples coordonnés.

Mais si on se dirige vers la partie réseau, si les relais restent les mêmes, si vous regardez le graphique sur les mesures, nous avons toujours une sorte d'écart entre ce qui est utilisé et ce qui est (inaudible) à utiliser, c'est toujours un problème.

Si, disons, nous atteignons 4 millions d'utilisateurs avec ces 6 000 relais, il y a des chances que la performance de Tor se dégrade. Il est très important, à mesure que nous obtenons plus d'utilisateurs, que nous ayons plus de relais rapides qui permettent de passer d'un point d'entrée à un point de sortie beaucoup plus vite.

Donc l'évolution est une question très importante pour nous. Chaque fois que nous ajoutons des éléments de sécurité à Tor, par exemple nous essayons d'ajouter du remplissage/une marge intérieure sur le réseau Tor. La corrélation du trafic ou les attaques de confirmation du trafic observent deux parties différentes du réseau et disent, « Oh tu es

David. » Ça devient beaucoup plus difficile. Mais ensuite on ajoute du poids au réseau. C'est donc toujours dans nos processus de recherche et développement. Est-ce que le réseau Tor peut évoluer avec ce que nous ajoutons ? À l'heure actuelle je ne peux pas vous dire oui ou non, nous évoluons ou pas. C'est un processus continu constant. Merci.

DEV ANAND TEELUCKSINGH: Merci, David. Je regarde juste s'il n'y a pas d'autres questions. Permettez-moi de faire un rapide sondage auprès de nos participants. Combien d'entre-vous utilisent Tor ? Vous pouvez utiliser votre AC pour répondre oui ou non. Allez-y David. Je soupçonne que vous soyez un important utilisateur de Tor.

DAVID GOULET: La question est donc, combien de personnes utilisent Tor ?

DEV ANAND TEELUCKSINGH: C'est plus un sondage pour le public. Mais vous pouvez répondre à la question pendant que les gens nous répondent.

DAVID GOULET: Ah, pour le public. OK.

DEV ANAND TEELUCKSINGH: Je vois que deux personnes ont indiqué utiliser Tor. Il y a environ 14 ou 15 personnes qui participent à l'appel. Je vois trois personnes

maintenant. Excellent. D'accord, voyons s'il y a d'autres commentaires ou questions. Une, deux. OK.

Et merci encore David pour votre présentation. Ce fut très instructif. Je pense que nous allons mettre les diapos sur le wiki et continuer à suivre les questions. Via Glenn, nous pourrions peut-être vous relayer ces questions s'il y a un suivi des questions. Et peut-être que si le groupe de travail At-Large chargé des technologies a davantage de questions nous pourrions vous recontacter. Restons en contact.

DAVID GOULET: Oui faites-le.

DEV ANAND TEELUCKSINGH: Merci beaucoup.

DAVID GOULET: Posez des questions, rendez-les publiques. C'est un plaisir pour moi.

DEV ANAND TEELUCKSINGH: Très bien. Merci beaucoup, David. Il nous reste quatre minutes pour terminer à l'heure. Nous avions d'autres éléments à l'ordre du jour. Je vais peut-être demander cinq minutes de plus pour parler rapidement des éléments de travail immédiats possibles, des objectifs, des politiques entre maintenant et la prochaine réunion de l'ICANN.

Nous allons envisager des solutions de conférence. Comme vous vous en souvenez peut-être, le groupe de travail At-Large chargé des

technologies a été (inaudible) réunir des solutions qui a démarré en 2013 lorsque l'ICANN a envisagé de passer d'Adobe Connect comme solution de conférence vers quelque chose appelée réunion Lucid. Les discussions ont ensuite porté sur le fait que s'ils changeaient, nous devrions avoir notre mot à dire quant au type de solution de conférence que nous voulons.

Le processus a commencé lorsque nous avons commencé à examiner les solutions de conférence. Lorsque l'ICANN a semblé faire un pas en arrière nous avons également arrêté d'examiner les solutions de conférence. Mais je dois dire que lors de la réunion de Dublin…et peut-être que vous pourriez en parler Glenn car vous avez eu une conversation avec le personnel de l'ICANN à ce sujet.

Certains membres du personnel de l'ICANN ont discuté du fait que nous utilisons Adobe Connect mais nous cherchons des alternatives, Glenn, est-ce que j'ai bien résumé la chose ?

GLENN MCKNIGHT: Bien sûr. Ouais. J'ai en effet parlé avec Paul Hoffman et il sera présent à notre conférence en janvier ou février et sera axé sur la comparaison des meilleures pratiques. Nous avons eu une conférence téléphonique la semaine dernière et ça a été un vrai succès avec les participants. S'il y a un outil de conférence que la communauté peut recommander c'est de quitter Adobe et de chercher d'autres alternatives. Merci de nous donner une solution. Nous serions heureux d'organiser une conférence séparée qui présenterait des alternatives. Nous voulons être sûrs que l'accessibilité fonctionne. Les gens sur toutes les plate-formes, Linux,

DSD, mobile. Nous voulons être sûrs que ça fonctionne dans des pays avec une bande passante lente. Nous avons donc quelques défis.

S'il vous plaît, si vous avez des solutions, dites-le nous. Nous avons une comparaison entre différents outils et j'ai également une présentation diaporama qui est un peu datée maintenant mais c'est un outil toujours précieux qui a été développé avec l'IEEE.

À vous Dev.

DEV ANAND TEELUCKSINGH: Merci Glenn. Je voudrais juste répondre à une question disant que de passer de quelque chose à (inaudible) pas Adobe serait bien. Nous avons une sorte de tableau comparatif. Nous proposons un ensemble de caractéristiques que nous voudrions voir dans les solutions de conférence. Nous n'avons probablement pas le temps de passer en revue chaque caractéristique, mais je vais mettre quelques liens sur la liste du groupe de travail At-Large chargé des technologies, montrer ce que sont les caractéristiques de base que nous recherchons, la question de la multi-plateforme, de l'accessibilité comme mentionné par Glenn, ce type de caractéristique. Il faut pouvoir voir les participants, être capable de lever la main pour avoir une file d'attente et ainsi de suite.

Nous avons bien une liste de caractéristiques que nous cherchons. À nouveau, merci de mettre sur le chat ou sur la liste du groupe de travail At-Large chargé des technologies, quelques idées que nous souhaitons examiner. C'est l'une des choses sur laquelle nous voulons nous concentrer entre maintenant et l'ICANN 55, qui aura lieu à Marrakech

en mars. Nous sommes à la mi-novembre, donc c'est vraiment décembre, janvier et février.

Autres choses que nous voulons examiner : nous avons deux projets qui ont été inspirés par le travail du TTF et il s'agit du livre électronique et du sous-titrage. Peut-être pouvons-nous porter plus d'attention à ces projets. Ces projets ont été approuvés par l'ICANN et il s'agit maintenant de deux projets officiels qui ont été adoptés depuis Dublin.

Glenn, voulez-vous rapidement parler de l'idée du livre électronique ?

GLENN MCKNIGHT: Bien sûr. Maureen et moi avons durement travaillé pour trouver des outils différents du livre écrit au (inaudible) et en utilisant Caliber pour la conversation. Nous sommes en train de le tester sur Kindle et iPad. Nous aurons bientôt en démonstration deux livres électroniques. Nous allons faire un des (inaudible) avec un pilote de sous-titrage lors d'une de nos conférences. Ça a été un projet très intéressant car nous avions l'habitude de réaliser des séminaires web avec le renforcement des capacités mais c'est tout. Peu de gens y participent. Cela va au-delà du séminaire web. L'idée est de le fournir à tous les éco-espaces. Ce sera un petit séminaire web très intéressant.

DEV ANAND TEELUCKSINGH: D'accord, bien. Donc merci, Glenn. C'est peut-être la deuxième partie de ce que nous avons à observer. Je pense qu'il va y avoir quelques étapes à venir quant à la mise en œuvre de l'ATLAS II et à la manière dont nous allons traiter ces recommandations car beaucoup de travail a été fait

par le groupe de travail At-Large chargé des technologies et d'autres groupes à propos de ces recommandations.

Nous allons probablement les étudier à nouveau et (inaudible) voir quelque intérêt …voir d'autres mécanismes de participation qui était l'une des recommandations.

L'une des recommandations qui a été faite est d'examiner des choses telles que Liquid Feedback, etc. Nous n'avons pas eu l'occasion de vraiment examiner ça sous cette forme. Je sais que Jimmy a eu quelques expériences avec Liquid Feedback et je crois qu'il a recommandé que nous ne l'utilisions pas. Je pense que c'était peut-être l'une des recommandations. Mais nous devons au moins comprendre la chose pour pouvoir dire, « Voilà les raisons pour lesquelles nous ne pouvons pas l'utiliser. »

Nous n'avons peut-être pas besoin de travailler beaucoup plus sur la recommandation de l'ATLAS II car je pense que nous l'avons déjà bien en mains, mais il est évident que toute personne au sein du groupe peut ne pas être d'accord et suggérer que nous nous penchions plus sur la question.

Une autre idée pour le TTF ? Une, deux.

Il y a une autre question que j'aimerais aborder. Nous voulons également lister certaines des questions liées à la technologie soulevées par la communauté At-Large. Nous avons essayé de développer cela sur notre espace de travail du groupe At-Large chargé des technologies pour suivre les questions liées à la technologie.

Par exemple, pour Adobe Connect, il y a eu une question concernant les e-mails venant principalement des utilisateurs qui utilisent des adresses yahoo.com. Ils ont été renvoyés de la liste de diffusion. Je veux donc suivre ces types de questions provenant de la communauté et les soulever face au personnel pour que nous puissions essayer de voir si nous pouvons identifier les problèmes, et arriver avec des solutions notamment en coordination avec le personnel de l'ICANN. Voilà un nouvel élément de travail immédiat pour le TTF entre maintenant et l'ICANN 55.

Une dernière chose. Je voudrais passer trois ou quatre minutes. D'autres temps de conférences pour le groupe de travail At-Large chargé des technologies. En général le groupe de travail At-Large chargé des technologies se réunit le lundi, le troisième lundi de chaque mois à 15 h 00 UTC. Certaines personnes, principalement venant de la région Asie-Pacifique, ont déclaré que c'était un horaire très inapproprié pour assister aux appels du groupe de travail At-Large chargé des technologies.

Je voulais juste vous faire part de cette remarque. Pourrions-nous avoir un horaire alternatif pour les conférences du groupe de travail At-Large chargé des technologies ? Est-ce que nous voulons, à titre d'essai, trouver une alternative aux horaires ? Lorsque je parle d'un horaire alternatif, j'essaie de me souvenir quelle était la proposition. Je crois qu'il s'agissait de quelque chose comme 21 h 00 ou 22 h 00 UTC. Cela veut dire tôt le matin pour la région Asie-Pacifique. Est-ce que quelqu'un a un commentaire ou une idée sur ça, sur un horaire alternatif ?

Je vois quelqu'un taper sur le chat. Je vois également Maureen en train d'écrire sur le chat. D'accord, essayons un horaire alternatif. Maureen écrit. Pendant qu'ils tapent quelque chose, Glenn, allez-y. Vous avez la parole.

GLENN MCKNIGHT: Ouais. Nous avons également parlé du peu de personnes présentes et j'apprécie vraiment que Maureen soit là aujourd'hui. Nous savons tous qu'il doit être environ 3 h 00 du matin pour elle. Nous essayons d'atteindre l'APRALO et avoir une conférence à une heure qui leur convient. Dev ou moi-même, je serais heureux de présider la réunion. Nous avons besoin d'un co-président pour cette conférence dans la zone de l'APRALO. Nous aimerions assister à la prochaine conférence APRALO pour pouvoir soulever cette question. Mais je pense qu'il y a beaucoup de choses à propos desquelles les personnes au sein de l'APRALO peuvent participer. Nous serions heureux de pouvoir nous adapter à d'autres zones horaires. À vous Dev.

DEV ANAND TEELUCKSINGH: Très bien. Merci Glenn. (inaudible) ce que vous dites. Je pense que nous serons vraiment ouverts à une modification des horaires. Peut-être en réalisant des rotations. Nous pourrions inclure plus de personnes, en particulier venant de la région Asie-Pacifique. Nous avons beaucoup de personnes sur la liste de la région Asie-Pacifique, mais ils ne sont pas présents à la conférence. Peut-être qu'en modifiant l'horaire, nous aurions plus de personnes présentes.

Nous pouvons peut-être soulever la question à l'APRALO. Nous pourrions ensuite avoir un sondage Doodle pour choisir un horaire approprié. Pour Maureen là il est 5 h 00 du matin.

D'autres commentaires ou d'autres remarques ?

En ce qui concerne l'interprétation, en général il faut trois personnes voire plus pour l'interprétation avant une session, et nous devons les prévenir au moins 72 heures voire trois jours avant la séance, car il faut du temps pour organiser la chose et voir si les interprètes sont disponibles pour telle date à telle heure. Donc nous avons besoin qu'au moins trois personnes demandent une traduction et pour une langue particulière. Il faut garder ça à l'esprit.

Je crois qu'il y a eu un commentaire provenant d'Internauta Venezuela disant que cette séance aurait dû être interprétée. Mais ce que nous allons faire c'est traduire les transcriptions de cette conférence pour que vous puissiez lire la séance en Espagnol et en Français.

Je ne vois pas d'autres commentaires ou questions. Et je sais que nous avons dépassé de 18 minutes. Ce fut vraiment une séance instructive. Merci à nouveau à David pour cette présentation des projets Tor.

Je voudrais remercier tout le monde. N'hésitez pas à échanger avec nous sur la liste de diffusion et la séance est maintenant levée. Merci et passez une bonne journée, soirée, matinée. Au revoir.

TERRI AGNEW: Cette séance a été levée. Merci à tous de nous avoir rejoints. Merci de bien déconnecter toutes les lignes et passez une bonne journée.

[FIN DE LA TRANSCRIPTION]