Mesdames et messieurs, nous allons commencer notre programme d'ici peu. J'aimerais vous présenter Steve Crocker, Vice-président du board de l'ICANN.

STEVE CROCKER : Merci. Je suis très heureux d'être ici. Nous allons avoir quelques interventions ce matin. Nous allons parler d'allocation et d'affectation des adresses. C'est peut-être moins excitant que les affectations des adresses IPB4 pour la dernière fois mais nous avons un excellent panel, une table ronde de haut niveau sur le sujet des abus dans le domaine DNS. Et je vais tenter de ne pas prendre trop de temps. Vous avez la liste des personnes qui sont ici présentes : Richard Boscovich de Microsoft, on va l'appeler Bosco ; nous avons Joe St. Sauver de l'Université de l'Oregon, je vais l'appeler Joe tout simplement ; Michael Moral d'Interpol ; Robert Flaim, on va l'appeler Bobby du FBI ; Glenn Watson de l'Administration américaine qui s'occupe de l'alimentation, drogues et médicaments ; et Terri Stumme de l'USDEA.

Donc, nous allons sans plus attendre donner la parole à – je vais vous demander de limiter votre temps de parole puisque nous sommes nombreux, à limiter, donc, votre temps de parole. Je peux être dur, vous savez, attention. J'espère que je n'aurais pas être dur avec vous. Bosco, allez-y.

RICHARD BOSCOVICH : Eh bien, merci de m'avoir invité tout d'abord. Oui, c'est difficile d'être concis dans ce type de domaine, de lutte, on par le de lutte contre le crime numérique. Je travaille à Microsoft, un groupe qui essaye de limiter, justement, cette criminalité informatique. On voit les menaces qui existent contre les consommateurs. Nous essayons de faire quelque chose d'une manière agressive, de voir les tendances qui se dessinent et je travaille avec beaucoup de développeurs informatiques. Les logiciels malveillants, nous les étudiants de près. On parle beaucoup de botnet. Nous avons compris ces dernières années que botnet c'est une

infrastructure criminelle qui est utilisée pour les activités illégales sur l'Internet, le spam, l'hameçonnage, les loteries qui sont fausses. Donc, le botnet, véritablement, c'est ce qu'on doit attaquer selon nous sur l'Internet. Il y a de cela un an, nous avons essayé d'être agressif contre les botnet et que ce ne soit illégal également, de le faire de manière tout à fait légale. Il y a une poursuite judiciaire en février dernier, l'opération B49, contre le botnet Waledac et en octobre 27 2010 Microsoft a donc eu un ordre par défaut contre 277 domaines qui étaient utilisés par le botnet de Waledec.

Donc, ce que nous avons réussi à réaliser avec cette opération c'était de couper entre 70 000 et 90 000 ordinateurs du botnet. Donc, tous ces domaines arrivaient vers nous avec les adresses IP et maintenant nous sommes en mesure dans tout le pays de notifier ces personnes et de nettoyer les ordinateurs, les disques durs des ordinateurs. Donc, c'était ce qu'on appelle l'opération MARS, la Réponse Active de Microsoft pour la Sécurité. On a beaucoup appris avec cette opération B49, qui est une théorie tout à fait légale, qui soutient la défense du DNS.

On est très limité aux Etats-Unis, il faut que vous le sachiez. Pour décapiter un botnet, nous avons dû prouver que nous étions dans notre droit. La loi américaine nous oblige à passer par la justice. Pour avoir ces autorisations, on doit suivre ces procédures standards, légales, juridiques et on doit indiquer aux personnes qui ont ces domaines, uniquement indiqué pour les C&C. C'était difficile, donc, à réaliser. Ce qu'on a fait c'est trouver des solutions légales avec un ordre de limitation temporaire, un TRO, c'est vraiment un remède absolument extraordinaire et très rare. Nous avons donc dû utiliser ces procédures légales. Selon les lois de la procédure, on avait 14 jours pour agir.

La situation qui existait c'est qu'on avait, comme vous pouvez le voir sur l'écran, ce type de structure. C'était nouveau pour moi lorsque je suis arrivé à Microsoft. J'ai dû me former à ce sujet. Nous devions déterminer – est-ce que l'on fait le processus UDRP ? Comment est-ce que l'on peut s'assurer qu'il y a le processus juridique des Etats-Unis qui soit suivi, même si c'est possible dans certaines situations, dans la

plupart des litiges commerciaux, après les périodes de temps, ça prend 45 jours, si on a la possibilité de faire cela, si c'est acceptable. Mais, lorsque vous avez un domaine qui est utilisé uniquement pour une malfaisance, eh bien, la personne qui a enregistré ce domaine va devoir bouger ce domaine. Le problème c'est qu'il y a un change de domaine. Donc, la question qui se pose c'est jusqu'à quel point on peut s'attaquer à cette personne qui bouge d'un domaine à un autre.

Donc, plutôt que de s'attaquer aux registrants, nous avons décidé de regarder au niveau du registraire. Au niveau légal, le problème qui se posait c'est qu'on était une fois limité par la loi américaine. Et dans ce cas, ils étaient à l'étranger. Donc, on n'avait pas de juridiction, les cours américaines ne pouvaient pas avoir juridiction sur, vu l'endroit où était ce registraire. Mais, étant donné que la plupart des domaines – on a trouvé un angle juridique pour s'attaquer puisqu'ils étaient des points com, on a passé par Verisign, basé aux Etats-Unis, par l'intermédiaire de VeriSign on a été en mesure de s'attaquer à ce « .com ».

Donc, les obstacles, j'en ai mentionnés certains. Ce qu'on a appris c'est que tous les domaines dans cette affaire juridique étaient basés en Chine par des registraires chinois et des informations étaient fausses, c'était des informations erronées qui étaient données. Donc, il n'y avait aucun processus ICANN en place. Chacun était un faux. Le processus d'enregistrement n'avait pas été respecté – c'était frauduleux, les informations étaient fausses et la seule bonne information qu'on a pu déterminer c'était deux adresses email. Et on connaissait ces adresses email, qui existaient, qui étaient à des personnes parce que quelqu'un a ouvert et lu, n'a jamais répondu, mais ouvert et lu. Nous courriels ont été lus. Donc, le problème c'est qu'il risquait toujours de se déplacer d'un domaine à un autre, ces malfaiteurs.

Donc, l'enregistrement des domaines. Au niveau légal, si vous ne pouvez pas identifier qui a enregistré ce domaine, ça va être très difficile de faire quoi que ce soit au niveau légal ou de lancer une action en justice.

Donc, il y a des traités internationaux aussi qui posent des problèmes, ça prend beaucoup de temps, c'est très long. On a utilisé la Convention de la Haye. Ça aurait pris des mois pour s'attaquer à ces registres qui étaient en Chine. Et en fait, on avait arrêté certains – il y a certains qui ont coopéré. Mais, ça vous montre bien à quel point c'est complexe, à quel point nous sommes dans une situation difficile dans le cas de l'abus des DNS. Nous sommes dans une situation où on tire profit du processus d'inscription d'enregistrement et les botnet savent qu'ils ont l'anonymité et l'immunité en quelque sort parce qu'ils sont le temps de changer, de se déplacer.

Donc, ça c'était une des premières opérations.

Nous avons fait une autre opération à Microsoft. Ce qu'on a vu c'est qu'on a un différent type d'abus de DNS. On a vu des botnet qui utilisent non seulement des faux enregistrements mais également des codes, des algorithmes qui sont utilisés dans le botnet, par exemple vous pouvez générer 15 ou 16 domaines par jour avec certains codes. Par exemple, ça peut être un Protocole Internet, il peut y avoir un mécanisme codé, ou si on n'atteint pas cette adresse Internet, eh bien, dans le logiciel malveillant ça vous envoie à un mode secondaire et la génération d'un nouveau domaine, un nouveau nom, et on sais quels domaines vont être libérés au quotidien et ces nouveaux domaines sont affectés par l'intermédiaire de ce logiciel malveillant. Donc, ça c'est avec des codes ce que cela est réalisé. C'est alphanumérique. Mais, on se demande qui enregistre cela et pourquoi. Est-ce que quelqu'un se pose des questions – qu'est-ce qui est enregistré ? Est-ce que quelqu'un suit cela de près ?

Ça c'est les problèmes que nous avons notés lorsque nous avons fait notre opération B49. Et je crois que cela montre bien ce qui doit être fait à tous les niveaux. Peut-être il y a un logiciel malveillant, s'il y a un problème de sécurité, s'il y a des allégations, il y a peut-être une période de 24 heures de l'ICANN ou du registraire qui pourrait permettre – voir si les personnes répondent ou pas, s'il y a bien quelqu'un derrière cette adresse, derrière ce domaine.

Donc, voilà quelques points que je voulais soulever aujourd'hui, qui sont tout à fait crucial. C'est dont les menaces de botnet qui sont en hausse. Je crois qu'il faut être absolument conscient de la manière dont ils utilisent cela, les criminels utilisent les botnet pour faire de la fraude sur l'Internet.

STEVE CROCKER : Merci beaucoup. Merci beaucoup. C'est absolument fascinant. Rapidement, je vais donner la parole à Joe, maintenant.

JOE ST. SAUVER : Oui, merci beaucoup.

Donc, je crois que nous avons des transparents également. Nous avons des…

Alors, selon moi, une des questions les plus importantes qui se pose – les spammers, quel infrastructure utilisent-ils ? Quels sont les ressources qu'ils utilisent ? Eh bien, clairement, ce sont les noms de domaine. Alors, quels sont les registraires qui sont des victimes de ces personnes criminelles ?

Nous pensons que dans la plupart des cas, il faut avoir un ombre limité de registraires qui vont être des victimes selon les violations de leur ligne de conduite qu'ils notent. Moi, je crois que dans beaucoup de cas, ces registraires sont des victimes comme nous lorsque l'on reçoit du spam, des pourriels. Donc, certains ne prennent pas de mesure dans ce cas, rien ne se fait, rien n'avance. Donc, j'ai étudié cela pour MAAWG en février 2008 et j'avais 60 transparents et il y a des gens qui m'ont dit que c'était un petit peu trop long ce type de discours, je n'aurais pas le temps aujourd'hui de vous passer ces 60 transparents, donc je vais faire une version condensée, simplifiée du matériel que j'avais à l'époque.

MAAWG, vous ne connaissez peut-être pas cette association. C'est un groupe de travail pour lutter contre les messages abusifs. Ça représente

un milliard de boîtes postales Internet. Il y a des vendeurs, des prestataires de services, des registraires qui participent également dans ces activités. Et ce que je voulais dire c'est que si ça vous intéresse, si vous voulez participer à MAAWG, si vous êtes un registraire, ce serait une bonne idée. J'aimerais également vous dire que je suis un conseiller technique auprès d'eux.

Donc, si vous essayez de déterminer quels sont les registraires qui sont abusés, eh bien, quels sont les domaines qui pointent à la surface ? Eh bien, comment le spam fonctionne-t-il, par exemple ? Nous avons une liste qui s'appelle SURBL, qui a entre 500 à 600 000 domaines de listé et pour donner une idée de l'impact de cela, si vous allez voir un message, s'ils ont une liste de domaines, vous voyez entre 0,122 et 4,449 points de chaque zone. Là, on parle de spam assassin. Donc, c'est une situation où il y a un impact fort, il y a beaucoup de confiance de la part de la collectivité.

Vous avez besoin également de faire l'adressage des noms de domaine vers les registraires. Vous pouvez vous baser sur les registres, savoir qui est le registrant, le registraire. Je dis en général parce qu'il y a des exceptions à la règle. Il y a certains ccTLD qui n'offrent pas ce service WHOIS ou qui vont le limiter, ou bien il y a d'autres facteurs qui rentrent en ligne de compte. On ne peut pas trouver facilement cette information, on va trouver une manière d'être plus efficace mais pour le moment vous n'avez pas toujours accès à toutes les informations.

Donc, qu'est-ce que nous observons ? Quels sont les TLD ? Ce que nous voyons le plus souvent dans la liste SURBL de février 2011 – 40 % des domaines sont des « .info », il y a un problème avec « .info ». « .info » a pourtant une bonne réputation. Ils sont attaqués souvent mais ils répondent rapidement. Donc, ça c'est une chose qui est très claire. « .com » en second, ça j'ai l'expérience de cela. « .ru » pour la Russie, en troisième position. Ça ne m'a pas trop surpris non plus. Donc, il y a une concentration assez forte. Ils nous disent ils vont utiliser un domaine de Gibraltar ou d'Andorre, c'est assez obscur. Non, ce n'est pas vrai. On ne le voit pas actuellement sur cette liste.

Donc, là on ne voit pas le volume de données. On a une situation où les spammers utilisent un domaine et font du spamming. Donc, il faut bien reconnaître que ces données ne sont pas compensées. Donc, quels sont les registraires que nous voyons le plus souvent sur notre liste SURBL ? Go Daddy, qui a des réponses rapides. Ce ne sont pas des données une nouvelle fois qui sont mises en rapport avec la part de marché. Il y a des domaines qui n'existent déjà plus. C'est ce que l'on retrouve – domaine non trouvé. Donc, il faut qu'il n'y ait pas d'impact opérationnel sur le serveur WHOIS.

Donc, c'est une situation où nous voyons des domaines qui disparaissent très rapidement. Il y a des registraires également qui sont associés avec différents ccTLD. Mais, on peut se baser avec des données par registraire. Donc, là vous voyez – je ne sais pas si c'est très utile, mais je vous montre la liste sur mes transparents.

Alors, qu'est-ce que l'ont peut ajuster par rapport à la part de marché du registraire ? Si on pense à cela, par exemple, si on voit Go Daddy ou d'autres des plus grands, ce n'est pas juste de ne pas les informer. Il y a, donc, des registraires qui ont une part de marché très forte. Donc, vous avez un ratio d'environ 1 sur 1, deux tiers ou trois quarts sont listés. Et ça représente peut-être 1 ou 2 %. Donc néanmoins, je ne crois pas que on devrait laisser ces personnes tranquilles, leur dire que 1 % c'est acceptable, non. Même si 1 % est abusé, c'est un nombre important de noms de domaine et c'est une véritable souffrance pour l'Internet.

Donc, on ne peut pas arriver à zéro, c'est impossible. C'est irréaliste d'arriver. Mais, 0,5 là ce serait acceptable pour, par exemple, Go Daddy. Ça représenterait 10 000 – 20 000 noms de domaine qui sont abusés, ça serait dans cet ordre d'idée.

Donc, je ne m'attends pas à ce qu'il y ait des miracles mais je crois qu'il faut vraiment qu'il y ait moins d'abus à ce niveau.

Donc, en conclusion, quelques étapes qui seront possibles. Il y a encore beaucoup de choses que l'on peut faire. C'est un exemple très simple de

cette analyse. Selon le volume de spam, on peut lister les domaines, faire une liste de priorités et également fournir des dossiers quotidiens, des fichiers quotidiens. Bon, ce n'est pas si important que d'obtenir très rapidement les données WHOIS mais il faut le faire au moins fréquemment. Pour les ccTLD, il y a des ccTLD qui ne donnent pas d'informations. Il faut plus de transparence, donc, et il faut que les ccTLD diffusent des informations lorsqu'on les demande. Il faut qu'on ait des cibles, donc. Il faut, comme j'ai dit, qu'on ait un seuil également.

STEVE CROCKER : Merci, Joe. Michael Moran d'Interpol.

MICHAEL MORAN : Je m'appelle Michael Moran ou Moran, comme vous le dites aux Etats-Unis. Je suis membre de la Police Nationale Irlandais et je participe à Interpol également. Très rapidement, je voulais vous présenter Interpol et essayer de nous éloigner un peu de l'impression que vous avez à Hollywood d'Interpol. On ne saute pas des hélicoptères, par exemple. Ce n'est pas notre boulot. Nos fonctions principales sont communication, opération, soutien et formation. On dit politiquement correct c'est le transfert de compétence. Communication c'est-à-dire assurer 198 pays par leur bureau central. Chacun de vos bureaux a un bureau central et ce bureau central normalement est assez haut dans la hiérarchie de la police. Les bases de données comme la base de données des empreintes digitales, des objets volés ou perdus, des objets d'art et des automobiles volés. Et moi, j'ai la responsabilité de la base de données sur l'exploitation et abus des enfants. Il y a des sous-groupes sur les stupéfiants, crimes organisés, trafique des êtres humains. Les crimes contre les enfants fait partie de mes fonctions.

J'ai pressé le mauvais bouton, excusez-moi.

Voilà, je vous donne une vue générale maintenant de deux opérations qui sont liées, deux opérations, tous les deux basées sur le web, sur internet et les deux qui concernent DNS. Avant de commencer, je ne

vais utiliser des mots comme « pornographie enfants », moi j'appelle ça « le matériel d'abus des enfants ». Tout ce matériel ne peut pas être produit sans qu'un enfant soit abusé. « Pornographie » implique le consentement social et on ne peut pas dire cela lorsqu'il s'agit de l'abus des enfants. C'est très important de ne pas oublier que comme agent de police et de la force de l'ordre, lorsqu'on parle de ce matériel c'est pas des photos des enfants, des filles sur la plage. On parle des petits enfants, avant la puberté, souvent sous l'âge de 10 ans. C'est très important de vous rappeler de cela parce que on n'est pas des puritains qui ne veulent pas que vous regardez des pornographies. Nous sommes des agents de police qui travaillent dans un environnement international à essayer d'identifier les enfants et ceux qui les exploitent et mettre fin à ces abus.

Opération Flicker, Tornad et Myosis, trois opérations qui ont eu lieu contre le même groupe criminel en 2006-2007. Aux Etats-Unis, il y avait le FBI, il y avait l'équipe COS au Département de la Justice, Interpol a été impliqué également. Il y avait le Ministère de l'Intérieur en Biélorussie et puis il y avait la police de Londres.

Il s'agissait d'une opération criminelle qui avait des sites Internet qui vendaient du matériel de l'abus des enfants sur Internet en utilisant des cartes de crédit simples. Vous entrez en ligne et éventuellement vous arrivez au site, vous payez et vous mettez toutes vos informations sur la carte de crédit et je peux parler toute la journée de pourquoi des gens font ça. Mais, c'est une autre conversation. Mais, ils mettent toutes les informations et on vous donne accès à ces abus d'enfants en grand volume, en utilisant un om de code. Et ça a changé dans l'opération plus tard. M ais essentiellement l'opération Flicker component était – ça c'est le FBI, ils sont suivi une autre voie. L'opération Tornado - c'était l'opération Biélorussie. Ici il s'agissait plutôt de blanchiment d'argent pas des abus des enfants. Ils gagnaient énormément d'argent de cette opération. Opération Mysosis – c'était la police de Londres qui a eu position d'une liste de clients, les « idiots » comme on le dit, qui ont donné leur nom de crédit, leur nom, leur code postal, date de

naissance, adresse, tout ça est entré dans l'ordinateur, ils sont payé pour avoir accès à ces sites pour les abus des enfants.

ICE et le FBI aux Etats-Unis ont suivi – les agents à Paypal normalement. Et quand j'ai dit avant qu'ils payaient avec les cartes de crédit Visa mais plus tard ils ont utilisé Paypal. Et donc, il y avait une opération de blanchiment d'argent également. Le résultat final de toues ces opérations est qu'on a pu suivre vers 140 pays et que les gens avaient envoyé toutes les informations de paiement.

Donc, certains pays ont réagi, d'autres pays n'ont pas réagi lorsqu'ils ont reçu ces informations. Les Biélorusses ont éliminé le gang criminel, ils sont maintenant en prison pour 9-10 ans pour blanchiment d'argent. Mais, l'idée centrale ici est que c'était un gang criminel organisé et vendait des enfants mais ils auraient pu vendre n'importe quoi comme produit. Bon, la fin de ce gang était basée en Ukraine et ce gang est devenu l'objet de l'opération Basket. Ils sont pris – on a pris du contenu et ils ont mis ça en ligne mais ils ont opéré de manière plus sophistiquée. Ils avaient un système d'abus de DNS beaucoup plus sophistiqué. Chacune de ces opérations auraient eu au moins 2 000 noms de domaine. Et beaucoup, dans l'opération Basket, une des manières de cacher leurs opérations – eh bien, ce qu'on a parlé tout à l'heure. Il y avait des noms de domaine aléatoires, par hasard. Tous ces 2 000 noms de domaine avaient beaucoup d'informations très précises et attachées, n'étaient pas payés par les cartes de crédit avec ces soi-disant « idiots ». En fait, tous ces noms de domaine étaient payés par des cartes de crédit volés et deuxièmement toute l'information était de valeur zéro. Un nom a été utilisé pour registrer, un autre nom était utilisé – disons que les noms, les numéros de téléphone étaient justes, les noms étaient justes mais c'est simplement de l'information que ce groupe criminel avait trouvé sur Internet.

Si vous coupez un nom de domaine, on obtenait une page qui disait que le compte était terminé. Puisque le gang était de l'Ukraine, on ne pouvait pas trouver des résultats si on le cherchait de l'Ukraine. Si la police ukrainienne faisait une recherche sur ce gang, on ne pouvait pas

obtenir des renseignements. Le message qui apparaissait sur l'écran était « compte terminé ». Ils utilisaient la méthode d'injection directe où ils utilisaient des machines qui étaient compromises, c'est-à-dire vous entrez dans un nom de domaine, nom de domaine innocent mais le contenu venait d'ailleurs. Et cet ailleurs était des serveurs dans des pays d'Amérique du Sud, l'Amérique Centrale et là-dedans on trouvait simplement un seul fichier. Ce fichier était redirigé, réorienté vers un autre serveur. A la fin, on n'obtenait aucun renseignement utile. Voilà, ça c'est le genre de détail parce que ce sont de vrais experts qui organisent ces gangs.

Du matériel des abus des enfants sur Internet, on ne voit pas autant de volume qu'il y a quelques années. Ludvigsen d'Interpol, de la police criminelle de la Norvège, il est aussi aujourd'hui et il va vous parler plus tard du système de blocage en place dans certains pays de l'Europe, surtout en Scandinavie. Mais le résultat de tout cela a été la réduction du matériel des abus des enfants sur Internet à cause, justement, des opérations de la police à l'échelle mondiale. Opération Basket, par exemple, on a pu démonter le gang, on a pu arrêter des gens et ils sont en prison en Ukraine maintenant. Donc, ce gang-là a été totalement démonté. Donc, bloquer, on fait ça souvent en Europe. Augmenter la capacité de la capacité de la police dans le monde est une autre technique. Ça amène à la réduction de cette activité sur l'Internet.

Il y a un bureau à Washington, que vous connaissez peut-être, une coalition des gens qui font des paiements comme American Express, Visa, Paypal. Ils s'assoient avec la police et les ONG aussi, comme le Centre International pour les Enfants Perdus. On se met à eux, à table dans la même salle et si on leur dit que leur système de paiement est utilisé pour payer pour l'abus des enfants, ils terminent les comptes. Une fois qu'on les avise de cette activité, les payeurs arrêtent de traiter avec ces clients. Les associations de service fournisseur Internet eux aussi ils reçoivent les notifications pour démonter. Ils ont des techniques pour, justement, réduire la quantité de ce contenu sur Internet. D'autres groupes, comme ceux qui luttent contre le spam,

limitent aussi accès à ce genre de matériel. Mais, DNS est le trou ; DNS et les registraires, il y a un manque d'effort, un manque de bon sens qui pourrait être mis en place. Moi, je crois qu'on pourrait le mettre en place pour mieux contrôler ce matériel.

J'appelle les registraires à accepter leur responsabilité et que j'aimerais voir une coalition des DNS où on pourrait avoir des procédures, justement, pour essayer de mettre fin à cette activité criminelle. Il faut avoir un processus mis en place pour mettre fin immédiatement à un domaine pendant le temps que l'enquête ait lieu. Il y a une liste de blocages en Europe, les critères sont très strictes mais le matériel qui est absolument illégal dans nos pays. Ces 400 domaines, on ne parle pas d'un million de domaines, on parle de 400-500 domaines, point final. Ceux qui ont vraiment du matériel très mauvais, des enfants trop jeunes dans les actes sexuels, qui sont abusés. Ces domaines on aimerait les voir, on aimerait voir un système automatique de notification chez ICANN ou je ne sais pas quelles est l'instance qui a le pouvoir de faire ça.

Un autre élément précise WHOIS, on ne le reçoit jamais, même si on le reçoit, on voit quelque chose qui nous donne une indication, c'est toujours un cul de sac, c'est toujours une perte de temps. Quel est pour moi la base de données de WHOIS ? Quelqu'un doit être responsable pour cette base de données. Pour al personne qui est responsable, s'il vous plaît, acceptez vous responsabilités parce que c'est une base de données qui est absolument inutile.

On voit les TLD qui sont impliqués dans les crimes contre les enfants. Souvent, ils sont notifiés et il y a une réaction immédiate. Je vous garantis que dans les petits pays où il n'y a pas un système de registrement qui est hors de contrôle, ça n'existe pas.

Et communication. Nous sommes là parce que nous voulons tendre la main à ICANN et ICANN a tendu la main à nous et on ne peut toujours pas communiquer. Donc, il faut qu'on commence à danser ensemble. Ça c'est ce que je vous suggère.

Merci.

STEVE CROCKER : Merci, Michael. Je vous remercie beaucoup d'être si franc, si franc avec vos propos. Et je m'excuse d'avoir mal prononcé votre nom.

Robert Flaim, je sais qu'on l'appelle Bobby.

ROBERT FLAIM : Bon, je vais permettre à mes collègues de parler avant moi. Glenn Watson et Terri Stumme.

TERRI STUMME : Je m'appelle Terri Stumme. On m'a demandé d'assister à ce panel pour parler de l'abus comme c'est lié au trafique illégal online de produits pharmaceutiques.

Je travaille dans ce domaine depuis 6 ans et dans le domaine des enquêtes contre les pharmaceutiques. Nous sommes le point de contact principal pour les enquêtes qui ciblent les organisations qui trafiquent dans des stupéfiants. Je veux saisir cette opportunité de partager avec vous le fait que les Etats-Unis, les drogues pharmaceutiques continuent à tuer beaucoup plus de personnes. 6 millions de personnes sont affectées par ces abus. En Floride, en 2008-2009, plus de 6 000 personnes sont morts d'une overdose de produits pharmaceutiques. En Caroline du Nord, une personne est morte d'une overdose. De 2005 à 2009, des overdoses dans l'état de Ohio ont augmentées de 249%. En Virginie de l'Ouest, il y a eu un problème d'overdose, une augmentation de plus de 500 %. De 2001 à 2005, plus de 32 000 personnes sont morts d'une overdose de produits pharmaceutique.

Et voilà donc des augmentations énormes. Si vous ne testez pas vos employés, considérez le fait que de 2005 à 2009, il y a eu une augmentation de 40 % dans les employés qui prend des produits pharmaceutiques illégalement.

Les produits vendus sur Internet est énorme. 14 individus ont été condamnés à un trafique de substances contrôlées. Jog Network, Inc. a distribué une énorme quantité de produits pharmaceutiques illégale. 78 million de dollars ont été gagnés et toutes ces ventes ont été facilitées par les clients qui placent des commandes sur Internet. Les résidents des Etats-Unis ont reçu des milliers de paquets contenant des énormes quantités de dosage sur une période de 16 mois. Au fur et à mesure que l'Internet devient un outil efficace pour de commerces légitimes, en même temps ça facilite une énorme variété d'activités criminelles. On voit les développeurs de sites web, des registraires et d'autres qui participent dans cette activité. On a rencontré spam, logiciel malveillant, botnet et autres, des serveurs illégaux et autres. Ça continue à empêcher nos enquêtes. Même identifier l'adresse physique d'un registraire pour donner un mandat de perquisition, d'arrestation devient difficile. Ces criminels utilisent des milliers et des milliers de noms de domaine et changent de noms de domaine et changent de serveur. Ils changent l'information sur WHOIS et ils transfèrent des services et de noms de domaine sans difficulté.

En 2009, les Etats-Unis ont adopté une loi dans la matière et ajouté deux crimes à la loi sur l'abus des substances contrôlées. Un est lié à la distribution sur Internet de ces substances contrôlées, c'est illégale pour toute personne de livrer, distribuer, dispenser une substance contrôlée par la voie de l'Internet. Les exemples des activités sont livrer, distribuer, dispenser une substance contrôlée sur Internet par une pharmacie qui n'est pas inscrite. Et je voudrais souligner partie (c) « servir comme agent intermédiaire aux autres entités qui fait que l'Internet soit utilisée pour mettre un vendeur et un acheteur ensemble pour acheter et vendre ces substances contrôlées ».

Les forces de l'ordre ont des recommandations à l'ICANN basées sur des enquêtes dans le monde réel aux Etats-Unis et à l'échelle internationale. L'intention de ces recommandations est de dissuader le cyber crime avec la mise en œuvre des noms de domaine internationalisés, de noms de domaine de première linéaux, et l'Internet qui va s'élargir par des

milliards de fois. Il faut absolument augmenter les contrôles. Les statistiques démontre : la santé et la sécurité publiques est à risque et il faut une action immédiate de la part de votre communauté.

STEVE CROCKER : Merci Terri. Glenn Watson de la FDA des Etats-Unis.

GLENN WATSON : Je m'appelle Glenn et je suis agent spécial pour le bureau des enquêtes criminelles de la FDA. Nous avons la responsabilité de mener les enquêtes criminelles lorsqu'il s'agit des produits réglementés par la FDA, les produits pharmaceutiques aussi. Dans un effort de ne pas répéter ce que tout le monde a déjà dit, je vais simplement ajouter quelques questions à ce que Terri a déjà dit, liées aux substances contrôlées. Même après l'adoption de la loi Ryan Haight, il y a toujours un marché énorme pour la vente des produits pharmaceutiques via Internet qui sont des faux produits. Une étude a été faite par l'OMS qui montre que 50 % de tous les produits pharmaceutiques vendus en ligne des adresses cachés sont faux, sont des contrefaçons. La plupart des gens qui travaillent dans ce domaine vont penser « bon, c'est simplement Viagra, Cialis, c'est pas important ». Mais, si on va un peu plus profondément dans le problème, c'est beaucoup plus important que ça. Il s'agit de produits pharmaceutiques qui servent à servir la vie, comme Lipitor, Plavis, Nexium, Zyprexa, les antibiotiques, insuline, des produits pour lutter contre le cancer aussi. Donc, c'est beaucoup plus important et vu de ce point de vue, le problème est beaucoup plus important. Les gens ne sont même pas au courant et ne veulent même pas l'admettre.

Les problèmes que nous avons étudiés récemment est si les services proxy sont appropriés pour des organisations qui vendent des produits réglementés, comme les produits pharmaceutiques comme si vous allez dans votre pharmacie locale ou vous allez voir votre médecin et vous avez une ordonnance pour un produit pharmaceutique, vous voulez contacter la personne qui vous fournit ces produits. Mais, quand vous

avez des organisations criminelles qui travaillent sur Internet, ils ne veulent pas, évidemment, être contactés par leurs clients. Ils utilisent donc les serveurs proxy pour essayer de tenir à distance les forces de l'ordre.

Nous avons vu d'autres problèmes récemment où les sites qui disent qu'ils vendent des produits pharmaceutiques mais lorsque le client achète il est contacté par le groupe des forces de l'ordre qui leur dit « Nous savons que vous achetez des produits pharmaceutiques en ligne. Nous travaillons pour les forces de l'ordre des Etats-Unis, ou le DEA, FBI, etc. et si vous ne nous payez pas 15 000 dollars dans les prochaines heures on va venir vous arrêter ». Donc, des produits pharmaceutiques et mêmes s'ils sont des contrefaçons sont abusés par les criminels sur Internet pour solliciter des cartes de crédit, frauder les gens, voler de l'argent.

Je vous remercie.

ROBERT FLAIM : Je m'appelle Bobby Flaim et je voulais ajouter quelques commentaires pour résumer ce que nous avons entendu. On a parlé de botnet, abus des enfants, produits pharmaceutiques faux. Ce que nous avons fait dans les forces de l'ordre, nous avons développé une série de recommandations. Nous voulons que l'ICANN s'assure que les registres et les registraires qui sont accrédités, ceux qui seront accrédités dans l'avenir soient les plus responsables, les plus transparents, les plus capables avec les meilleurs réputations. Deuxièmement, nous voulons que les registraires et les registrar aient des noms de domaines précis qui ne soient pas des criminels qui obtiennent des informations. Il y a des manières de faire ça. il faut que notre force soit à 100 %, tout le monde doit participer pour lutter contre ce fléau. C'est ce que vous avez entendu aujourd'hui. Nous travaillons avec les registrar et le registraire d'obtenir cette information. Nous voulons raffiner le processus, c'est la raison pour laquelle nous avons fait une recommandation. Nous voulons que nous nous adressions précisément aux problèmes qui

existent. Il y a tant de problèmes avec les 22 gTLD, nous ne voulons pas que le problème soit plus massif avec l'introduction des nouveaux gTLD.

Donc, le temps est très important et c'est la raison pour laquelle nous faisons une recommandation à l'ICANN et à d'autres membres de la communauté Internet, et nous pouvons réaliser nos objectifs.

Je voulais terminer avec ce souhait.

STEVE CROCKER : Merci. Nous sommes un peu en retard. C'est la période que nous avons consacrée aux question & réponses. Il n'y avait pas de question qui nous arrivent d'Internet ? Si vous avez des questions allez-y. mettez-vous devant le micro.

>> Je serais bref. De Knujon.com. J'ai une question pour la collectivité du respect des lois. Les registraires doivent obéir aux lois et je vois très souvent dans les accords de service et contrats sur les sites web que ils doivent envoyer – s'ils savent qu'il y a une activité criminelle, ils doivent envoyer aux autorités, aux FBI des informations. Est-ce que vous recevez beaucoup d'informations à ce sujet de la part des registraires ?

ROBERT FLAIM : Eh bien, comme je l'ai dit, nous avons vu des petits éléments de coopération en effet. Mais hélas, il y a un problème plus grave, plus large. Les rapports – est-ce qu'on doit travailler au cas par cas ? Nos ressources sont très faibles, donc ce n'est pas la méthode la plus efficace de travailler au cas par cas. Je ne sais pas si quelqu'un d'autre voudrait commenter, rebondir là-dessus ?

STEVE CROCKER : Paul ?

PAUL VIXIE : Paul Vixie, Internet Systems Consortium. J'aimerais vous remercier tous de dire ce qui doit être dit. On l'a dit auparavant, il faut le redire, il faut le répéter. C'est important que vous soyez ici mais on aurait dû le faire il y a de nombreuses années. Je n'entends pas beaucoup d'espoir mais beaucoup d'exaspération. Je sais que la communauté ICANN est large et vaste et en pleine croissance. Nous avons une économie et l'économie de DNS connaît une croissance très forte. Et c'est pour cela qu'on a beaucoup de fossés dans nos règles. On a très souvent la possibilité de contourner les règles, ce que l'on voit, ce que l'on observe, notamment. Donc, il me semble que je redoublerais d'effort pour vous aider, pour nous assurer que la situation s'améliore. Et j'aurais voulu que tous la salle de vous faire quelque chose, nous devons réagir, nous devons agir. Il y a d'autres sphères technologiques mis à part le DNS où l'on gère avec un système de réputation. Plutôt qu'il y a des problèmes, on indique les personnes qui ont une mauvaise réputation et qui travaillent en dehors ses systèmes de régulation et des règlements. Moi, je crois que je suis l'auteur d'un tel système pour le DNS. Ça vient d'être ajouté à BIND et à d'autres produits, je l'espère.

Je crois que si la communauté ne peut pas vraiment être responsable de ses actions, c'est un véritable chaos qui risque de s'ensuivre au niveau du DNS. Donc, je préférerais travailler de votre manière.

Merci beaucoup de vous être exprimés avec force.

RICK WESSON : Merci. Rick Wesson. J'apprécie beaucoup tous les commentaires que j'ai entendus ce matin, ou en ce début d'après-midi. C'est un travail difficile que vous effectuez. En 2003, c'était au moment de la réunion de Beijing, moi j'ai lancé un service pour les registraires de domaines pour vérifier le WHOIS, c'est un système de vérification que j'essayais de vendre aux registraires pour qu'ils puissent vérifier chaque entrée avant de faire une délégation. Et le coût allait être de quelques centimes par

nom de domaine. Et on aurait pu couvrir 209 pays pour vérifier le WHOIS, numéros de téléphone et ainsi de suite, contacts. Et j'ai fait une erreur – c'est de le bâtir d'abord et ensuite essayer de le vendre. J'aurais dû le vendre et ensuite le bâtir. Mais, je crois que c'est faisable. Il y a des services aujourd'hui que l'on peut acheter, qui coûtent 25 cents peut-être par nom de domaine. C'est faisable. Mais, il n'y a pas de volonté de le faire. Donc, si ce n'est pas une loi, règlement ICANN, ça ne se fera pas, je crois. Je crois qu'on peut faire beaucoup plus et éviter qu'il y ait des noms de domaine qui ne soient pas en rapport avec une véritable personne, une véritable entité.

Donc, moi je me ferais l'avocat que ICANN mette en place un mécanisme pour que la population, le grand public puisse beaucoup mieux suivre le processus et être au courant de tous les problèmes qui existent d'adresses Internet et de protocole Internet. Je crois que des universitaires pourraient nous aider dans cet effort. Je crois que l'ICANN devrait ouvrir la porte pour que les communautés comprennent mieux le problème. Ce sera très utile.

Merci.

STEVE CROCKER : Merci.

DON BLUMENTHAL : Oui. Don Blumenthal de Public Interest Registry. Donc, j'ai passé un tiers de ma carrière dans le domaine des lois qui régissent l'Internet. Je ne suis pas quelqu'un qui remet en question ce qui a été dit mais l'exemple de Finsen (ph), service financier, donc, de respect de lois financières, pour mettre cela en perspective, si – je crois que c'est monsieur Moran qui en parlait, si vous êtes venus me voir en tant que registraire disant qu'il y a des personnes qui se mêlent des activités frauduleuses, est-ce que vous m'auriez les preuves ou est-ce que vous m'auriez indiqué qui était cette personne ?

MICHAEL MORAN : Vous voyez, les personnes qui travaillent à ce problème, ils ont des critères très stricts. Donc, ils ajoutent ce la à des listes et c'est disponible par l'intermédiaire de votre bureau national, si vous êtes du BFA ou du Botswana vous avez un bureau central avec une liste, avec un protocole d'accord. Vous pouvez avoir accès à cela sans aucun problème. Les preuves sont là.

Bon, on est à Lyon en France, l'Interpol, mais vous pouvez absolument obtenir des exemplaires de tout cela. Tout est disponible, toutes les preuves sont là, sont disponibles.

Ce que nous demandons c'est que nous mettions en place des protocoles pour bâtir la confiance et moi j'y crois personnellement. Je crois que l'on peut mettre en place des processus qui permettront qu'il y ait la confiance qui règne pour que nous puissions faire des enquêtes rapides et prendre des actions rapides. Je crois que c'est tout à fait possible. Lorsque l'on parle de la sécurité du public, lorsque l'on parle de crime contre les enfants, que je vois au quotidien, il est important de faire quelque chose et d'agir. Mais, on ne cache rien. Notre travail est là, documenté, disponible, ouvert et transparent.

DON BLUMENTHAL : Oui, brièvement. Je ne suis pas sûr que tout le monde travaille de cette manière au niveau du respect des lois, au niveau des autorités de respect des lois et des polices. Donc, je crois que, en effet, il faut qu'il y ait une confiance, il faut qu'il y ait une relation de confiance. Il faut que l'on puisse établir une relation de confiance avec des autorités policières en qui on a confiance, qu'on soit à l'aise. Et qu'en effet on puisse obtenir des preuves, qu'il y a des problèmes. J'espère qu'il y aura des mécanismes.

GLENN WATSON : Moi, ce que j'ajouterais à cela c'est que de la part de la FDA ces dernières années on a été proactifs pour les registraires. On leur a donné beaucoup de documentations, on leur a indiqué quelles sont les lois qui sont violées par les registrants ou les sites web.

Les allégations qu'on a reçues récemment, il y a des domaines qui sont suspendus mais très vite ils se retrouvent avec des registraires qui sont en dehors des Etats-Unis. Donc, par exemple, pour les ventes de faux médicaments ou de médicaments, si c'est basé aux Etats-Unis, eh bien, très vite le domaine va être libéré et ça va être repris par quelqu'un qui ne se trouve aux Etats-Unis, on aura du mal à le poursuivre. C'est ce qui se passe.

STEVE CROCKER : Moi, j'aimerais interrompre cet excellent échange parce que nous avons de moins en moins de temps. Je suis désolé, Alex. C'est vraiment un excellent échange. Les problèmes sont importants, les problèmes d'équité, les problèmes de procédure juste et équitable. Je crois qu'on doit poursuivre le dialogue. Je crois que vous avez tous fait un excellent travail. Vous nous avez fait prendre conscience des problèmes qui existent à ce niveau. On a pris un peu la température et je crois que vous nous êtes très utiles. Merci beaucoup. J'aimerais qu'on vous applaudisse et que nous passions au point suivant.

Vous êtes prêts à vous lancer ? Avec un micro peut-être, monsieur Ram Mohan de Afilias.

RAM MOHAN : Alors, merci de m'avoir invité. Je voulais vous parler précisément – oui merci, c'est excellent. J'aimerais vous parler d'un concept qui s'appelle démontage du site et blocage du site. Donc, comme on l'a entendu auparavant, clairement, on a parlé de botnet. Par exemple, il y a beaucoup de parties qui sont à sens unique et d'autres à double sens. Donc, voyons un peu ce qu'on a fait, quelle est notre expérience.

Donc, par exemple retirer un site « .info », par exemple, il y a une ligne de conduite anti abus qui est en effet depuis octobre 2009 en collaboration avec les registraires. Donc, on a eu le processus ICANN, système de commentaire public. Et avec cette méthode, ce que nous avons fait, c'est que les registraires font des analyses et la dissémination. Il y a des relations avec la communauté de la sécurité, avec la communauté des registraires. Mais, la méthode que nous avons utilisée c'est que les problèmes sont envoyés aux registraires. Et donc, les registraires vont retirer le site web s'il est possible. Le registraire a une relation avec le registrant et donc en bonne position pour faire régner les règles du contrat. Dans le cas des registres que nous avons, il y a des – attendez, j'ai pas le bon transparent, oui. Les données que nous avons, très souvent ne sont pas aussi fiables que celles du registraire. C'est ça le problème.

Ce que nous avons vu entre octobre 2008 au jour d'aujourd'hui, mars 2001, il y a plus de 500 000 domaines « .info » qui ont été indiqués aux registraires et si nécessaire on peut retirer ces sites.

Dans notre ligne de conduite anti abus, que nous avons pour « .info », il y a la possibilité d'agir, indépendamment si nécessaire. Donc, en termes de principes et de principes de succès, ça marche. C'est take-downs ont retiré des sites, ça marche. C'est une réponse spécifique, directe. Le problème c'est que très souvent, vous jouez à un niveau très faible et non pas sur une grande échelle. Il y a des éléments criminels qui utilisent une grande variété de tactiques et qui peuvent se cacher. Donc, il faut travailler au cas par cas, nom par nom, c'est difficile, ça prend du temps également.

Donc, le blocage de DNS, qu'est-ce que c'est ? Comment le définir ? Qu'est-ce que je veux dire par là ? Eh bien, c'est une manière de ne pas permettre des demandes de renseignements, par exemple, à un niveau à un autre, une couche à une autre, du DNS. C'est différent de suspendre un domaine en le retirant de la zone. Donc, dans le blocage il y a des méthodologies qui nous permettent que les demandes ne soient pas effectuées et qu'on ne puisse pas y répondre. Donc, ça peut être

une réponse disproportionnée par rapport au problème. Pra exemple, pour le spam, nous avons des filtres email qui sont faits à plusieurs niveaux mais, comme il a été dit, il y a des listes noires qu'on peut utiliser pour le DNS. Tout dépend, pas seulement au niveau des sites web mais ça va plus loin que les sites web, les sites c'est l'élément le plus visible. Il y a des questions qui se posent – est-ce que le blocage, véritablement, vaut la peine ? Selon moi, au niveau de l'ISP ça peut être un problème parce que ça va avoir des conséquences qui n'étaient pas attendues, qui n'étaient pas voulues ; ça peut créer la confusion pour les utilisateurs de l'Internet. On se demande qui est responsable, qu'est-ce que l'on peut faire ? Auprès de qui allez-vous vous adresser pour régler le problème ? Donc, au niveau de la compatibilité avec le DNSSEC, cela requiert que les serveurs, entre parenthèses, mentent. Donc, il y a la question de confiance qui se pose, l'interprétation des données. Ça, donc, brise la chaîne de la confiance qui s'était instaurée et une fois qu'il y a un blocage, ça peut être difficile de corriger cela, de repartir en arrière. Donc, il peut y avoir des dommages.

Donc, Steve, je vous redonne le micro.

STEVE CROCKER : Je vous remercie. Oui, Christine ? Christine Jones du groupe Go Daddy.

CHRISTINE JONE : Oui, merci. Merci, Steve. Je m'appelle Christine Jones, je suis de Go Daddy et on travaille au niveau des abus des DNS au quotidien. Et, j'aimerais dire que les noms de domaine ne commettent pas de crime. C'est clair. Les personnes qui enregistrent des noms de domaine sont parfois des criminels et on ne veut pas – je vais vous mettre – excusez-moi, j'ai du mal à vous voir. Donc, j'ai des problèmes de lunettes. Vous êtes quand même très bien, je vous vois mal. J'ai simplement des lunettes de soleil que je peux mettre.

Donc, on travaille avec la FDA, avec l'Interpol au quotidien, avec la police irlandaise, avec les personnes du monde entier parce qu'il y a des

malfaiteurs partout dans le monde. Que ce soit du spam, que ce soit de l'hameçonnage, que ce ça soit des logiciels malveillants, de la pornographie ou bien de l'abus d'enfants, ce n'est pas de la pornographie infantile, c'est de l'abus d'enfants. Eh bien, nous avons une approche une approche agressive par rapport à d'autres registraires mais nous enregistrons un nom de domaine par second, et même plus. J'ai 100 personnes seulement qui travaillent 24 heures sur 24, 7 jours sur 7. Et ça, dans cet écosystème c'est vraiment unique. Il y a peu de registraires qui ont 100 personnes pour lutter contre ce crime informatique. Donc, il faut dire quelle est véritablement l'envergure de ce registraire, qu'est-ce qu'ils sont en mesure de faire, quels sont leurs moyens, leurs ressources, quelles est leur taille ? Ce n'est pas qu'ils ne devraient pas le faire. Je crois que chaque que chaque registraire qui est un bon citoyen, qui est ici dans cette salle, qui vient à l'ICANN devrait indiquer « Vous devez faire quelque chose, agir, vous battre contre les malfaiteurs ». Mais, on ne peut pas tous vous répondre en 1 heure, parfois c'est impossible. Ça dépend des moyens.

Donc, ce que l'on trouve c'est que nous avons une approche hybride pour l'abus DNS dans différents contextes. Ce que je veux dire par là c'est que nous avons soutenu, ciblé des textes législatifs que nous utilisons pour que les activités qui soit bien illégales, très clairement illégales, et que les autorités policières puissent trouver ces malfaiteurs, les stopper. On ne fait pas de jugement. Il faut qu'on ait, donc, des textes très clairs qui nous indiquent lorsqu'il y a un crime d'effectué. Mais nous avons besoin d'une collaboration volontaire du secteur parce que, en effet, comme je vous le disais, si nous n'avons pas les ressources d'aller chercher les spammers qui vont utiliser un nom de domaine à 9 dollars. Ça ce sont des ressources que l'on n'a pas tout simplement. Donc, s'il y a quelqu'un, qu'Interpol dit qu'il y a quelqu'un, ou l'a police irlandaise nous dit qu'il y a un problème avec quelqu'un, est-ce que nous allons tout de suite bloquer le site ou pas ? Les questions se posent. Donc, aux Etats-Unis, nous avons travaillé étroitement également et avec beaucoup de succès avec des agences n'étant pas des agences policières, propriétés intellectuelles, par exemple, la

Maison Blanche, FTC, des autorités américaines, des agences américaines, ce ne sont pas des personnes qui puissent poursuivre les criminels mais qui travaillent quand même au niveau principalement légal.

En ce qui concerne les botnet, le spam, les médicaments – faux médicaments, de contrefaçon, tout ce dont on a parlé auparavant, on ne veut pas aider des personnes à commettre des crimes sur l'Internet, ce n'est pas la raison de notre existence. Mais, uniquement le jour où tous les registraires ont un haut niveau, un standard à respecter, des normes à respecter, et qu'on les forcera à retirer les malfaiteurs de leur systèmes, même si on fait le maximum à Go Daddy, eh bien, vous n'allez jamais réussir à résoudre le problème parce qu'il y aura toujours quelqu'un qui abritera ces malfaiteurs. Un mauvais registraire qui permettra d'enregistrer des noms de domaine fraudulaires et d'avoir des activités criminelles.

Voilà ce que je voulais dire ce matin.

STEVE CROCKER : Oui, merci Christine. C'était très bien dit. Je vois que Marc a la parole maintenant.

MARC ROTENBERG : Mark Rotenberg. Je suis du Consultatif At-Large. Moi, je travaille dans la journée en tant que directeur à Washington de la vie privée électronique et j'aide le congrès à prendre des décisions, d'autres organisations internationales également, sur les problèmes de droits civils et de vie privée. Donc, les abus de DNS c'est important pour la communauté des utilisateurs. On a soutenu le SECDNS. On a dit qu'il était important de beaucoup agir dans ce domaine. Je crois qu'il faut bien comprendre qu'il y a des points supplémentaires à prendre en compte. Un qui a été mentionné plusieurs fois a trait à l'équité ou au processus juridique, vous savez lorsqu'il y a une autorité policière qui veut bloquer un site web ou bien le mettre à bas, eh bien, il faut savoir

si cette décision policière est justifiée, légale, correcte. Et pour s'attaquer à ces problèmes le gouvernement devient de plus en plus agressif pour poursuivre en justice ces abus de DNS. On ne met pas dans le même sac les bons et les méchants. Et je crois que c'est Christine qui le disait, les participants doivent bien comprendre quelles sont les règles. Il faut leur indiquer comment ils sont en mesure de répondre et quelles sont, en effet, les réponses appropriées. Moi, je crois que c'est un domaine où la loi apportera une grande clarté. Je dirais qu'on pousse également l'attribution en ligne. On a parlé d'avoir une meilleure authentification des domaines. Je crois que c'est un pas dans la bonne direction mais il y a également dans les collectivités de maintien de l'ordre de prendre en compte les attributions des utilisateurs finaux pour retracer les activités des utilisateurs pour limiter les abus. Et maintenant que nous avons IPV6 et que nous pouvons avoir des adresses pour des objets éventuellement, eh bien, au niveau de la vie privée il me semble que ce sera important de prendre en compte les utilisateurs finaux. Il y a des attributions pour les consommateurs.

STEVE CROCKER : Oui. Merci beaucoup, Marc. Nous allons maintenant donner la parole à Bjorn. Bjorn-Erik Ludvigsen d'Interpol.

BJORN-ERIK LUDVIGSEN : Je vais vous dire Bjorn-Erik Ludvigsen. Je suis de Norvège, officier de police et je travaille à Interpol en France et je travail au blocage de domaines pour l'exploitation sexuelle des enfants.

Donc, je pense que le blocage est une bonne option – blocage de l'accès. C'est un travail de prévention, un travail de policier, de prévention. Il n'y a plus de victime. On veut protéger les droits des victimes en faisant de la prévention. Moi, je ne parle pas d'hameçonnage, de spamming, je n'y connais rien. Moi, je parle d'exploitation sexuelle des enfants. Ce sont des crimes analogiques et non pas numériques, selon moi, qui sont peut-être effectués en utilisant

des outils numériques toutefois. On veut limiter l'accès criminel, la dissolution et la procession et éviter, en effet, qu'il n'y ait pas d'exposition, donc, pour les enfants de ces images choquantes.

Donc, on a travaillé avec l'IWF au Royaume-Uni. On a commencé en Norvège en novembre 2004 avec une nouvelle législation scandinave et avec d'autres pays européens également. Donc, ce qui serait légal dans un pays sera légal dans un autre pays. Donc, ce sera inaccessible de n'importe quel pays. On continue à travailler ensemble, c'est un projet de la police européenne dans quatorze pays.

Donc, les pays qui risquent de choisir un petit peu – ça c'est la liste de blocage national de CIRCAMP. Donc, nous avons les pays scandinaves qui font partie du CIRCAMP, donc, Norvège, Suède, Danemark, Finlande. On travaille également avec d'autres autorités policières, comme la Suisse, la Nouvelle-Zélande et on partage les données avec eux. Et nous avons donc des preuves hors ligne de cela. Ils peuvent voir leur texte législatif, voir les preuves qu'on leur apporte et voir s'ils bloquent le site pour leur pays.

Donc, on avait besoin de quelque chose qui soit illégale partout. C'est pour ça qu'on a été voir Interpol et qu'on leur a proposé de faire une liste des domaines les pires. Cela a été adopté lors d'une résolution à Singapour, lors de l'assemblée générale d'Interpol en octobre 2009, adopté à l'unanimité pour combattre l'exploitation sexuelle des enfants sur l'Internet en utilisant toutes les solutions techniques, incluant le blocage de l'accès à partir des pays membres de l'Interpol. Donc, les chefs de police ont pensé que c'était une bonne idée. Et nous sommes d'accord avec eux.

Alors, voilà les critères dont on a parlés.

Donc, un enfant c'est un moins de 18 ans dans la plupart des pays. Mais, dans la moitié des pays du monde, il n'y a pas de définition des crimes sexuels contre les enfants. C'est souvent pour cela qu'on appelle cela de

la pornographie ou bien c'est tout simplement pas mentionné, pas défini.

Donc, nous avons défini qu'un enfant a moins de 13 ans. Donc, on veut bien s'assurer qu'on ait que des enfants et que ce soit de vrais enfants, que ça ne soit pas des images informatiques ; donc, qu'il y ait des abus très forts ; un acte sexuel défini par le code pénal ; ou qu'on le se concentre sur les parties génitales de l'enfant. Donc, comme je l'ai dit, comme on l'a dit, il ne s'agit pas de photos douces, soft, de pornographie douce. Donc, il faut que cela soit doublement vérifié par au moins deux pays ou organisations. Et il faut que ça soit en ligne depuis les trois derniers mois. On le garde en ligne pendant au moins trois mois, on vérifie que ces images ne réapparaissent pas sous une autre forme sur l'Internet.

On a une liste de 386 domaines. Donc, c'est pas tout l'Internet. Il y a moins de 400 sites de ce type. Mais, il y a une croissance quand même très forte. Il y a de nouveaux domaines que l'on voit depuis 2010-2011, ça a doublé entre 2010 et 2011.

Donc, cette liste est disponible gratuitement, si vous êtes un fournisseur de service Internet, ISP, RSP, eh bien, vous pouvez, si vous donnez l'accès à l'Internet, avoir gratuitement cette liste pour pouvoir agir. On ne demande pas de données statistiques. Vous pouvez voir le bureau Interpol de votre pays et donc leur demander d'avoir accès à cela.

On aura une page d'arrêt, stop page, de disponible mais pas obligatoire, que vous pouvez montrer. Plutôt qu'on ait accès aux sites web, on aura accès à une page indiquant quelque chose.

Voilà les types de domaine que nous avons sur la liste. Donc, vous reconnaissez peut-être des points dont vous êtes responsable. Je ne dis pas que certains sont pires que d'autres – « .com » c'est plus gros, donc c'est le plus grave. Nous avons des abus de nom de pays et donc là on peut travailler avec les bureaux Interpol du pays. Mais, il faut qu'on

prenne compte tout ce que vous voyez mais qui sont des domaines de premier niveau, pas de pays.

Donc, le problème – j'en ai assez d'expliquer ce que c'était. Mike a fait un excellent travail pour expliquer cela, comme on le voit. Donc, on nous parle de mauvais acteur, mauvais contenu. Pour nous, ça se sont des enfants qui sont abusés sexuellement et c'est distribué – vendu sur l'Internet. Simplement parfois pour le plaisir que certains en retirent. C'est des personnes qui ont des fantaisies par rapport à ces enfants, des fantasmes sexuels. Donc, vous n'allez rien voir mais vous voyez les sites, la diversité de ces sites. C'est absolument incroyable. Tout ça, ça a été retiré il y a une semaine. Donc, là vous pouvez voir cela sur leur format originel. On peut vous montrer ces preuves. Là, vous avez une petite Américaine de 4 ans. Son père l'a abusée, violée et il y a des images terribles. Et on a essayé de la protéger au maximum pour arrêter la distribution.

Alors, la solution partielle c'est le blocage selon moi et selon nous, Interpol. Si met à bas le site, ils reviennent, ils réussissent à repartir et à retrouver de nouveaux domaines. Donc, les effacer, les effacer, ça ne marche pas toujours. Le blocage, à mon avis, c'est mieux. Plutôt que de voir – vous avez vu ? Voilà. Vous avez une page avec marqué Interpol, sens interdit et une explication de quelques paragraphes. On explique ce qui s'est passé et il y a un lien par rapport aux textes de loi, un lien vers Interpol et si vous êtes un propriétaire de domaine vous pouvez déposer une demande.

Alors, en ce qui concerne les WHOIS, est-ce que cela est efficace ? Est-ce qu'on peut faire confiance aux données WHOIS ? Je vais vous donner quelques exemples. Voilà le WHOIS de ce site d'abus d'enfants. Voilà. Alors, on donne un contact administratif, on dit que c'est quelqu'un qui fait une assurance, qui a un travail, qui est en Californie. Voilà sa maison, c'est supposé être sa maison, son adresse, son numéro de téléphone. Ça va à un centre médical en Californie, hein. Un numéro qui existe. Et on n'a jamais utilisé son email sur l'Internet. Donc, ça ne sert à rien le WHOIS, aucune information – tout est faux, aucune crédibilité.

Donc, cette personne a eu droit à un nom de domaine, c'est enregistré parce que les informations qui ont été communiquées sont totalement fausses, totalement erronées, totalement inventées. Rien n'a été vérifié. Il faut trouver un système automatique. Si vous obtenez un fax plutôt qu'un numéro de téléphone, ça c'est déjà une indication. Nous avons vérifié que toutes les informations sont fausses sur ces sites. Et je crois que ce que nous devons prendre en compte c'est que les cartes de crédit sont souvent volés pour enregistrer les noms de domaine. Et il y a des banques qui sont un petit peu complices de cela.

Il faut suspendre davantage de domaines. Avoir un domaine sur Internet ce n'est pas un droit de l'homme. S'ils ne gèrent pas l'affaire comme il faut, il faut les suspendre. S'ils n'ont pas un courriel qui fonctionne – on ne peut pas dire ce que je voulais dire mais vous les éliminez et s'ils ont un problème, vous pouvez résoudre le problème une fois qu'ils vous ont données les réelles informations. Il faut qu'il y ait de plus de préalables, plus d'exigences. Pour ceux qui redistribuent les domaines, si vous avez un domaine de premier niveau qui fait ça, il faut les suspendre.

Il ne faut pas permettre ces gens de continuer à faire cette activité. Nous pensons revoir tous le matériel, faire une liste que nous pouvons offrir à ceux qui font l'hébergement des sites pour qu'ils puissent très rapidement suspendre tous ces utilisateurs qui donnent ces fausses informations ou qui ne donnent pas des informations. Nous pensons que si vous ne n'acceptez pas dans al vie réelle, pourquoi accepter ça sur Internet ? Il faut suivre les mêmes règles. L'Internet est simplement une partie de la vie. C'est comme le courant électrique, l'eau. Il faut suivre les règles comme dans le monde réel.

Je vous remercie de m'avoir écouté.

STEVE CROCKER : Merci. Il nous reste un peu de temps pour des questions. Si vous voulez bien approcher le micro.

RAM MOHAN : Tout de suite une question pour clarifier. Sur les points antécédents considérés, vous avez dit suspendre les TLD sur la liste des pires. J'espère que vous voulez dire les – pas les domaines de premier niveau mais de deuxième niveau.

BJORN-ERICK LUDVIGSEN : Je suis un simple flic. Donc, je me suis trompé sur la terminologie, pardonnez-moi. Si vous avez un site qui est utilisé pour…

STEVE CROCKER : Mais, vous ne voulez pas suspendre tous les « .com ».

BJORN-ERIK LUDVIGSEN : Non, non. Pas tous les « .com ». Non, non, non. Ça ce n'est pas ce que je veux dire. J'utilise moi-même des sites « .com ». Non, c'était, justement, au deuxième niveau.

BEN WILSON : Je m'appelle Ben Wilson et j'ai une question. On me dit qu'il y a des contrats de vieux registres avec ICANN qui ne permettent pas à l'ICANN de les contrôler ou changer le cadre selon lequel ces registres fonctionnent. Est-ce que c'est vrai ?

MARGIE MILAM : Moi, je peux répondre à cette question. Oui, ils fonctionnent sous un accord standard que le registraire signe. Mais, c'est mis à jour de temps en temps et le conseil étudie comment les mettre à jour. Il y a beaucoup de discussions et il y a une possibilité de les changer. Mais, le processus est difficile, c'est vrai.

STEVE CROCKER : Steve ?

STEVE METALITZ : Steve Metalitz de la Coalition pour la responsabilité online. Merci à vous et à l'autre groupe. Christine Jones a parlé d'une approche hybride. Il y a une bonne approche pour les forces de l'ordre nationale et internationale. Il y a un rôle aussi pour l'action volontaire dans le secteur privé. Et la question difficile – quel sera le rôle d'ICANN ? Une chose que Christine a dit ce matin, si tout le monde n'est pas impliqué, il y aura toujours un problème. Et le véhicule est ICANN et par le processus d'accréditation et leur accord avec les registraires. Nous avons donc besoin d'une règlementation plus forte pour l'accréditation. Il faut un meilleur accord signé avec les registraires. Et il faut plus d'application des lois et de la règlementation par ICANN. ICANN peut faire une contribution.

STEVE CROCKER : Je vais mettre l'accent sur vous qui êtes à droite.

MALCOLM HUTTY : Je représente les Européen et les fournisseurs de services. Il y a des organisations qui représentent les registraires et les registres. Moi, je perçois des questions communes liées aux intermédiaires lorsque les forces de l'ordre voient des crimes et veulent que les intermédiaires agissent contre ces malfaiteurs. Nous avons les mêmes problèmes. Ça a été une session excellente et j'aimerais féliciter ceux qui ont participé dans ces sessions. Cependant, nous avons entendu des arguments puissants. En même temps, les intermédiaires doivent faire face au quotidien, qui font des choses contre les intérêts des consommateurs. Il faut des sauvegardes puissantes contre l'enlèvement de certains service et si retirer certains services pourrait faire du mal aux registrants ou pour nous, le client.

Ma question, donc, pour le panel est – comment trouver un équilibre ? Quels commentaires faites-vous concernant le besoin de rapidité et le besoin de la confidentialité dans la relation entre l'intermédiaire et les forces de l'ordre ? Est-ce qu'on peut équilibrer ça avec le besoin d'avoir un contrôle de la demande pour être sûr que l'intérêt du registraire et le client soit protégé ? Quels sont les sauvegardes croyez-vous qui doivent être mises en places pour protéger les intérêts du registrant et s'il s'agit de nier le service à un client ?

CHRISTINE JONES : Je vais essayer de répondre. Nous sommes un registraire important mais nous sommes également un grand prestataire de services d'Internet. Donc, nous voyons ces problèmes concernant le contenu, les intérêts. Je serais heureuse d'envoyer une copie de notre règlementation standard et j'aimerais que chaque fournisseur d'hébergement ait ça pour nous féliciter un petit peu.

La réponse à votre question est qu'il faut avoir – vos organisations membre doivent avoir une série de procédures qui répond à la question avant que vous voyez les problèmes. Il faut être en mesure d'avoir la réponse avant que vous ayez la question. Il y a certaines choses qui sont automatiquement illégales. Vous pouvez voir les images qu'on vous a montrées ce matin. Et vous savez, il y a quelque chose qui est mauvais – s'il n'y a pas un problème. C'est pas une question. Mais, en cet équilibre entre la position défaut est toujours laisser le contenu. Il faut avoir quelque chose, une règle qui permet de retirer l'image, surtout s'il s'agit de retirer un nom de domaine quand on ne contrôle pas le contenu. C'est une situation assez extrême. On réoriente le DNS. C'est important ça. Donc, il faut trouver un équilibre. Si je suis un petit registraire, dites-moi qui vous êtes, dites-moi qu'il y a une violation de la règle et donnez-moi une raison pour retirer le site. Je suis assez franche. Je prends peut-être plus de risques que d'autres. Je suis plutôt prête à démonter, à retirer certains des sites. Mais, pour les gens qui n'ont pas beaucoup de personnes dans le personnel qui font cette analyse des sites tous les

jours, il faut les aider – il faut les aider à vous a aider. Donnez-le un peu de couverture, c'est tout ce que je voulais vous dire.

MARC ROTENBERG : Je voulais lancer une idée. J'ai remarqué que vous avez eu beaucoup de sessions sur l'abus DNS et je pense que nous allons entendre parler davantage dans les années à venir. Il me semble qu'on pourrait utiliser plus de données. Si les registraires pourraient accumuler des données, le nombre de notifications pour retirer des sites, est-ce que c'était lié aux abus des enfants ? Est-ce que c'est lié aux violations des droits de la protection de propriétés intellectuelles ? Ça ne pourrait pas gêner nos enquêtes. C'est simplement des statistiques qui pourraient être très utiles à communauté parce que ça vous donnerait un sens de géographiquement comment les registraires répondent à ce problème. Donc, collecter les données, si on pourrait. Je connais cette pratique le domaine des écoutes téléphoniques. Nous avons des données qui remontent à 30 ans. Elles nous disent comment certaines organisations répondent à nos demandes pour des écoutes téléphoniques. Ça pourrait être utilise d'avoir un nombre, une idée du numéro de demandes.

STEVE CROCKER : Bon, pas seulement le nombre de demandes mais même des évaluations d'erreur 2, d'erreur 1. Est-ce que c'était correct ou incorrect ? Quand je parle de retirer les sites.

MARC ROTENBERG : Je vais être assez objectif que possible. Simplement pour savoir les numéros de sites, comment le problème a été traité. On peut faire ça dans les statistiques.

STEVE CROCKER : Je ne vais pas occuper le micro. Je vais continuer avec les questions. Ram ?

RAM MOHAN : Je tiens à ajouter une chose. On aurait pensé que ça serait facile si on gère une activité ou si on offre un service. Mais, c'est étonnant que tous les jours, au quotidien, on ne voit pas ceci. Lorsqu'on veut aller parler aux fournisseurs et leur demander de retirer certains sites ou faire une enquête, vous êtes choqués par le nombre de fois où on ne peut pas trouver un numéro de téléphone, on ne peut pas trouver une adresse de courriel. Et parfois, on envoie des messages et ce qu'on reçoit en retour c'est un message générique « On est en vacances ». C'est un abus. C'est un abus. Il faut avoir du personnel surplace, il faut avoir en place des mesures de base parce que c'est des prestataires de services – lorsqu'il y a un problème il faut que les services doivent fournis pour nous dans l'écosystème c'est absolument fondamental et ça n'existe pas encore.

STEVE CROCKER : Paul.

PAUL VIXIE : Merci, Steve. Comme opérateur d'un système de courriel, ça s'appelait « maps ». Beaucoup de gens qui ont fait des poursuites judiciaires contre moi m'ont dit que c'était trop cher pour eux de suspendre les clients avec la première plainte, c'était trop cher pour eux de vérifier la réputation des clients avant de faire signer les contrats. Donc, fondamentalement, c'était une méthode pour d'externaliser leurs problèmes, c'est naturel. La communauté a une réaction naturelle aussi. Je suis d'accord avec Ram. Blocking c'est terrible. On ne devrait pas le faire. Je suis là pour vous dire que ça se fait et ça sera fait beaucoup plus si Internet se multiplie par des milliards d'adresses.

Il y a peut-être seulement une chose à faire, un changement draconien, qu'ICANN pourrait faire au niveau règlementaire. Je termine en disant que j'étais, pour une certaine période de temps, le Président de PAIX et lorsqu'une chose était faite qui était mauvaise, je les déconnectais. Ça n'a pas entravé ou baissé mon niveau de rentabilité.

BILL SMITH : Je fais partie de WHOIS. Je veux faire l'écho à certains commentaires de la qualité des panels – excellent.

En ce qui concerne blocage, nous soutenons de ne pas le faire. Nous ne voulons pas faire de blocage. Nous sommes préoccupés par les 10 ans qu'il nous a fallu pour arriver à DNSSEC et l'impact très négatif du blocage sur la fiabilité et la confiance dans le système dans sa globalité. Il est important, donc, d'être très prudent lorsque vous parlez de bloquer.

Un autre commentaire sur la pornographie et l'abus des enfants. C'est une honte pour nous, la communauté, que nous permettons ce matériel de continuer d'être sur Internet. Et encore pire, que nous avons déployé des systèmes, nous écrivons des politiques et ils sont tellement inefficaces ce que ça soit pratiquement impossible de contacter les personnes responsables.

J'ai été très heureux d'entendre Go Daddy qui parlent de leur désir de ne pas faire partie – ils ne veulent pas avoir les criminels chez eux. Ça c'est très louable. Je vous félicite. Mais, Go Daddy et les autres grands registraires, que faites-vous en ce moment pour changer le système ? Que faites-vous maintenant pour améliorer le système ? Pour augmenter la précision des données que nous avons sur les clients pour savoir qui sont ces personnes ?

CHRISTINE JONES : Moi, je crois que c'est une question qui m'a été posée. Juste, je devine. Bon peut-être – je pourrais vous parler pendant des heures de ce que

fait Go Daddy. Je ne vais pas faire la publicité pour Go Daddy. Mais, je peux vous dire que je dépense plus d'argent que n'importe quel autre registraire, même plus que Paypal. Je vais devant le congrès pour les convaincre à faire adopter de bonnes lois dans la matière ; je passe beaucoup plus de temps avec les forces de l'ordre pour les aider à poursuivre en justice les malfaiteurs ; je travaille avec votre personnel et les autres personnes pour essayer de mettre fin à ces crimes. C'est difficile de payer pour la pornographie des enfants avec Paypal. Vous avez été convaincus et ça fonctionne. Nous faisons beaucoup de choses surtout avec WHOIS. Vous avez parlé dans cette salle de mauvaises informations offertes par WHOIS depuis 10 ans. Chaque fois que je fais une intervention dans une université ou devant une entreprise, là où ICANN n'est pas présent, je dis aux gens « Si vous pouvez trouver une façon pour nous de vérifier de façon légitime les données, vous allez devenir milliardaire parce que tout le monde dans cette salle va l'acheter et va l'utiliser ».

Le monsieur d'Interpol vous a donné un exemple parfait pourquoi vérifier les données dans la manière dont ça a été vérifié dans ce cas là est une mauvaise idée parce que ce que cela a fait il a suivi des bonnes données mais c'était l'information de quelqu'un d'autre. C'est pas ça la bonne réponse.

J'aimerais être aussi intelligente pour pouvoir vous donner la bonne réponse. J'aimerais que ce groupe de personnes très intelligentes trouve la réponse. Vous ne l'avez pas trouvé depuis 10 ans. Vous êtes la personne peut-être à répondre.

BILL SMITH : Avec beaucoup de respect, ce n'est pas notre travail comme équipe de révision. Nous révisons la politique existante pour voir si c'est efficace. Ça c'est notre tâche. Si vous nous demandez d'élaborer la politique, ce n'est pas nous. Je serais heureux de faire la politique. Mais, en tant que membre de l'équipe de révision ce n'est pas ma tâche.

Donc, la question que j'ai posée est que faites-vous individuel et collectivement ? Comme registrant, que faites-vous ? Parce que ce que je vois est que les registrants, collectivement, vous résistez les changements qui pourraient améliorer la précision de WHOIS.

STEVE CROCKER : Bon, je vais intervenir ici. C'est sans doute une des questions les plus difficiles qui existe dans cet environnement depuis très longtemps. Et je viens de démissionner comme Président du groupe qui concerne la sécurité. On observe ce problème depuis très longtemps et c'est frustrant de voir le manque de progrès dans le domaine et la qualité de l'inscription. On ne va pas résoudre ce problème ici mais je me soucie beaucoup pour ce problème mais je veux progresser. Nous devons peut-être organiser une autre session pour parler, justement, de ceci et s'il y a un blocage ici dans cet environnement il faut trouver une solution.

Et qui d'autre ? Tout le monde s'est assis. Est-ce qu'il y a d'autres questions ?

Bon, on va donc féliciter les différents panels. Ça a été excellent. Et surtout pour Margie Milam. Applaudissons Margie Milam qui a organisé cette session. Félicitations, Margie !

((Fin de l'enregistrement))