Nous allons commencer j'aimerais vous rappeler d'obtenir des écouteurs parce que nous aurons un panéliste qui s'exprimera en Français. Merci d'être venus, j'aimerais introduire Nii Quaynor qui sera notre modérateur pour ce forum sur l'abus de DNS. Nous avons des questions pour les panélistes et si vous avez des questions veuillez décliner votre nom pour les interprètes et les scribes merci.

NII QUAYNOR: Merci et bienvenue, comme je l'ai bien compris ce qu'on pensait est qu'avoir ne serait-ce qu'uniquement les noms pour nous rappeler. Faire notre travail internet devient de plus en plus compliqué parce que d'autres personnes trouvent des manières de ne pas l'utiliser de la bonne manière. Cela crée des différents abus, des défis à relever et il est important pour nous de prendre un peu de temps et de réfléchir surtout sur un environnement en plein développement que nous avons. Il y a des observations particulières ou des défis que nous découvrons qui pour donner des exemples d'abus au sujet des abus du système DNS. Pour nous aider à lancer notre discussion sur les DNS nous avons des panélistes très différents et il y a deux sessions, la première qui va tenter de passer en revue les dernières manifestations de la lutte contre les abus DNS et ensuite nous allons plus tard avoir une session sur les problèmes de l'évolution des noms de domaines, des pannes, des attaques, et nous allons donner aux panélistes la possibilité de faire leurs commentaires. Ensuite ce sera à nous autres de contribuer et parfois demander aux panélistes de répondre pour que ce soit un petit peu plus interactif et intéressant. Pour la première session les derniers déroulements dans la lutte contre les abus DNS nous avons un panel avec Lanre Ajayi, Frederick Gaudreau, Gary Kibby et Pierre Dandjinou. Je suis sûr qu'il est occupé mais il est en chemin, on va demander à Lanre Ajayi de commencer et si vous voulez des détails additionnels en termes de biographie et d'informations additionnelles sur leurs antécédents

professionnels ils figurent sur leur site web donc Lanre vous avez le micro.

LANRE AJAYI: Bonjour tout le monde mon commentaire sera sous forme d'une étude de cas ici au Nigéria. Je vais montrer quelques défis à relever au Nigéria et comment nous essayons de les gérer et je vais vous montrer une liste affichée sur l'écran des défis communs auxquels nous sommes confrontés. Ce n'est pas propre au Nigéria mais ce sont des défis qui existent sur l'internet le phishing, les pourriels, les emails de piège, le vol d'identité, les refus de service, les accès non autorisés, le cyber terrorisme, les virus et programmes malveillants. Il existe la perception que le Nigéria est le centre de cyber crime du monde ; regardez bien, je dis la perception du monde mais ce n'est pas tout à fait vrai. Je suppose que cette perception existe à travers le monde, je dois admettre que nous sommes coupables de certains d'entre eux mais pas de tous les crimes. Par exemple les spams, les pourriels, c'est vrai le Nigéria envoie des pourriels et c'et vrai nous sommes coupables, nous envoyons des emails de piège et d'hameçonnage, des activités d'hameçonnage et de vol d'identité. C'est vrai il y a des vol d'identité mais je n'accepterais pas et nous ne sommes pas coupables pour les attaques de refus de service, nous ne le faisons pas. Nous ne faisons pas de hacking même si vous le faites, nous n'avons pas la technologie pour faire du piratage et nous ne faisons pas de cyber terrorisme donc nous ne sommes pas coupables. Nous n'envoyons pas de virus parce qu'on ne sait pas comment écrire le code donc j'aimerais dire que nous sommes coupables des 4 premiers chefs d'accusation mais pas des 4 derniers. Nous sommes pénalisés sérieusement. Vous, vous avez arrêté de faire des affaires avec nous sur internet, ça c'est très dur comme pénalité parfois vous avez bloqué les IPs nigérianes et nous ne pouvons pas accéder à certains de vos sites et nos cartes de crédit ne sont pas acceptées dans certains cas. Et le sujet de discussion c'est ce qu'on appelle les escroqueries, ce que nous appelons 409 et que nous trouvons très embarrassant donc voici quelques conséquences de ces pénalités sur l'internet. Une fois quelques années auparavant une personne âgée citoyenne de la communauté européenne qui est arrivée au Nigéria a perdu toutes ses

économies. Il est parti voir l'ambassadeur pour se plaindre ils ont fait ce qu'ils pouvaient faire mais ils n'ont pas trouvé les escrocs. Il est allé voir l'ambassadeur nigérian dans son pays et il l'a tué, c'était très grave. Comme pays on a des options la première option est de déclarer la guerre contre ce pays pour avoir tué notre ambassadeur, l'autre option est de permettre à ce pays, à la justice de suivre son cours et pour nous de nous attacher à résoudre le problème. Ce pays A s'est fait justice et nous devons lutter contre le cyber crime dans notre pays. Le président pour cela a mis sur pied un groupe de travail cybercrime et j'ai la chance d'y participer. Le groupe travaille très dur et nous avons trouvé plusieurs solutions, des tentatives pour essayer de réduire cette menace. La première c'est que nous avons analysé du point de vue de l'angle technique, juridique et politique. Du point de vue juridique on s'est rendus compte que notre loi, notre législation est très faible sur les cybercrimes. Par exemple s'il n'y a pas de loi sur les pourriels, s'il n'y a aucune loi en cas d'emails d'escroquerie s'il n'y a aucune loi qui dit que vous avez commis un crime. Donc nous avons passé des projets de loi et pour résoudre certains de ces questions et le projet a été formulé par le groupe de travail sur me cybercrime et a bien résolu le problème de pourriel. C'est devenu maintenant législation, quand le parlement l'aura approuvé ce sera aux forces de l'ordre d'intervenir. Lors des transactions de télécommunication, la preuve électronique n'était pas encore la, ca n'existe toujours pas. Et jusqu'à ce que la loi soit passée ca demeure un défi, quelques personnes ont été arrêtées mais n'ont pas pu être inculpées en raison du fait que la seule preuve disponible pour cybercrime était une preuve électronique. Nous pensons que les opérateurs qui fournissaient les services, nous les encourageons et nous demandons que ce soit obligatoire pour eux qu'ils trouvent un parcours de comportement qui sera obligatoire pour les tous les membres. Ensuite, les gens qui n'appliquent pas les implications ne vont pas accepter cette implication pour l'économie nationale. Il faut être deux pour danser un tango, il faut un criminel pour et un complice à l'extérieur également pour le faire. Mais ce n'est pas bon pour l'image du pays, pour l'économie, et cela le public général doit être averti et on augmente les campagnes de sensibilisation et d'information du public. Cela dit la discussion se rapporte aux noms de domaine, nous avons

remarqué que la plupart des crimes, la plupart des cybercrimes listés que j'ai mentionnés auparavant ne peuvent être faits sans avoir utilisé un nom de domaine sous une forme ou une autre. Dans la plupart des cas ces criminels clonent les sites web du gouvernement nigérian et c'est facile à faire parce qu'au Nigéria la plupart des ministres départements et agences au Nigéria ont un nom de domaine de première priorité de premier niveau. Donc c'était très pratique pour le criminel de prendre un.com et que cela soit très similaire aux sites web des agences du gouvernement et le cloner pour commettre toutes sortes de crimes donc on félicite le gouvernement pour l'utilisation de.ng qui est obligatoire. Je pense que cela a été fait maintenant. Maintenant, veuillez faire des affaires avec nous arrêtez de bloquer nos IP, merci beaucoup.

NII QUAYNOR: Merci beaucoup, en réalité je me souviens que le nom en lui-même était une action contre le vol d'identité donc c'est une histoire qui existe depuis longtemps. Oui tout a fait, maintenant je voudrais avoir un petit peu de perspective je voudrais inviter Pierre Danjinou.

PIERRE DANJINOU: Merci beaucoup, je suis un petit peu en retard je m'en excuse et bien du Bénin. Je vais présenter la situation au Bénin et mon collègue a bien dit nous sommes en train d'améliorer les choses, nous essayons de voir ce qu'il se passe au Nigéria et voir si cela peut avoir un impact sur ce qui se passe au Bénin au Togo dans le reste des pays d'Afrique. Le cas du bénin va être un rapport assez bref concernant ce qui a été fait en Afrique pour combattre ce phénomène. Nous voyons vraiment qu'en Afrique en tout cas, les décideurs sont très intéressés par ces questions. Ils ont remarqué que l'internet devient de plus en plus grand et l'abus de DNS est quelque chose qui est en train de devenir de plus en plus important. On consacre des ressources à cela pour que la mission appropriée soit conduite, ce qui est une bonne chose maintenant. Nous aurions aimé avoir des statistiques à vous présenter, un système de reconnaissance de ce qui se fait dans le secteur des sociétés en Afrique mais ces chiffres ne sont pas disponibles. Comme Lanre l'a dit ce sont des problèmes,

nous savons qu'il y a certains types d'attaque qui ont lieu a différents endroits et que parfois c'est du au problèmes d'infrastructure que nous avons dans différents endroits, parfois l'incapacité à utiliser convenablement les serveurs que nous avons et les problèmes de DNS, de DNSSEC. Je pense que nous avons vraiment besoin de considération de la part des professionnels d'Afrique et des responsables politiques aussi pour améliorer les choses. Maintenant, une fois que je vous ai présenté cet environnement, ce que nous avons fait et ce que nous avons réussi a faire: je dirais qu'il y a différentes approches ici. Nous avons l'aspect professionnel, qui ont créé des réseaux avec des formations que nous réalisons. Nous sommes invités à travers l'AfriNOG à faire ce type d'ateliers et c'est cela nous permet de faire un développement de compétences. Il y a de plus en p lus de gens qui essayent d'avoir un petit peu de diplômes pour pouvoir s'assurer qu'ils pourront répondre aux problèmes de stratégie, aux problèmes de management, aux différents problèmes qui peuvent surgir dans notre pays. Le cert Afrique est une initiative qui vise à former des compétences dans les différents pays parce que vous savez que l'Afrique est formée de 54 pays qui ont tous des situations tout a fait différentes. Au Nigéria, au Bénin, nous avons une histoire différente par rapport au Togo ou à l'Afrique du Sud. Par conséquent, en Afrique, il y a une initiative continentale qui vise plusieurs objectifs dont un est la sensibilisation des décideurs. C'est une réalité parce que dans beaucoup de pays lorsqu'il s'agit des questions de sécurité, si ce ne sont pas des questions de sécurité les gens ne comprennent pas très bien. Nous voulons donc sensibiliser les décideurs pour qu'ils prennent vraiment conscience des problèmes qui existent et qu'ils fassent des programmes pour les hommes politiques avec des cours sur la cyber sécurité. Mais aussi, nous voulons entrainer former de plus en plus de gens actuellement je pense que nous avons environ 5 pays dans lesquels fonctionne vraiment ce système de cert. Nous aimerions que ça fonctionne davantage, nous allons travailler avec les professionnels nationaux pour nous assurer qu'ils ont leur propre CERT. Le CERT Afrique doit aussi être un dépôt de ce que nous appelons les informations, les documents dont nous avons besoin pour partager tout cela. L'Afrique ne va pas travailler toute seule, elle va travailler en

partenariat avec le secteur industriel, avec les différents acteurs qui existent et qui ont leur propres programmes. Nous allons créer ces groupes de travail avec eux, nous allons intensifier les ateliers sur l'abus de DNS nous avons des plans pour le faire. Le cert Afrique essaye actuellement d'enregistrer tout cela et de devenir opérationnel en 2012. L'autre question qui a lieu ici en Afrique est le programme pour le respect de la loi, pour le service d'ordre et c'est un registre qui a établi ce programme il y a trois ou quatre ans et nous voulons qu'il soit correctement ciblé. Nous ciblons les avocats et les gouvernements pour les sensibiliser mais aussi pour leur présenter les besoins qui existent pour réviser leurs propres législations. Cet atelier est important donc comme je l'ai dit il y a de plus en plus d'intérêts qui entrent en jeu et certains d'entre vous (Inaudible). On a des élections qui sont tenues dans différentes endroits et un système de fishing dont le contenu de certains sites web a été détourné et personne ne pouvait répondre à ce problème. On a été voir le comité d'élection en leur disant « on ne sait pas que faire à ce propos ». Il y a différentes histoires qui arrivent en Afrique et il faut éduquer les gens sur ces points-là. Le dernier point c'est ce qui a été fait par Interpol. Interpol est un très actif pour travailler avec la police et créer des départements, avoir une capacité pour un développement de ces systèmes de police. Nous avons aussi un atelier très intéressant parce que la spécificité de ces ateliers était de réaliser ces missions. Nous avons un partenariat entre la police et les experts par exemple en Côte d'Ivoire, on a une symbiose entre la police et les experts. Il y a des pays où on manque de confiance, il s'agit de la sécurité nationale et c'est difficile pour ces gens d'inclure des professionnels donc nous avons besoin d'en parler avec eux, d'être sûrs qu'ils comprennent que la technologie est un enjeu important. C'était un petit peu les choses que je voulais vous raconter sur ce qui se passe en Afrique. Aujourd'hui nous sommes en train d'essayer de nous assurer que les choses évoluent rapidement je dirais que ce sont de bonnes nouvelles dans un sens, merci.

NII QUAYNOR: Merci Pierre, donc nous avons vu le cas national et maintenant nous allons voir les activités qui ont lieu au niveau général et je suis heureux

de voir que AfriNIC continue de soutenir une série d'activités qui ont été lancées. Bien, continuons et sortons du continent et apprenons des différentes perspectives qui existent ailleurs, c'est un encouragement pour nous et nous allons maintenant inviter Frederick Gaudreau, du Québec, du Canada qui va nous parler maintenant.

FREDERICK GAUDREAU: Pour ceux qui ont besoin d'une traduction je vais parler en Français. Tout d'abord je voudrais commencer par une présentation du CERT du Québec, c'est une organisation de police avec un mandat pour appliquer la loi au Québec. Nous sommes basés au Canada, le Canada est divisé en 10 provinces et la loi doit s'appliquer. Pour ceux qui connaissent la géographie et l'histoire de l'Amérique du Nord nous sommes la seule province qui soit entièrement bilingue et bien sûr pour nous il est nécessaire et important de travailler également en Français. Nous avons besoin de collaborer avec des entités de police et de gendarmerie qui parlent également Français. Maintenant après trois ans notre organisation qui a été créée avec le but de regrouper pour des objectifs d'entraînement et de capacité d'échange d'information nous avons créé Francopol. Elle ne fait pas le même travail qu'Interpol, c'est vraiment une organisation pour l'échange d'information et d'enquêtes au niveau Criminel mais Francopol est là pour échanger les informations entre officiers de police et gendarmerie qui parlent Français et auraient besoin d'informations en Français sur plusieurs sujets en particulier le cybercrime. L'image ici est en circulation depuis quelques années, je voulais vous la montrer c'est une caricature publiée dans le New Yorker en 1993, soit il y a presque 20 ans et qui pense que sur Internet vous pouvez être n'importe quoi. C'est vrai aujourd'hui et la personne ayant fait cette caricature étant un visionnaire parce que c'est pourquoi la police a de vraies difficultés. Pour savoir qui est en face du clavier vous avez besoin d'une certaine connaissance et pour l'avoir vous avez besoin d'une formation et aussi de l'assistance de différents intervenants, opérateurs de l'industrie et universités. Sur le prochain slide vous pouvez voir qu'il y a un phénomène qui existe depuis quelques années, cette présentation d'interpol est un document envoyé aux utilisateurs Internet au Québec impliquées dans une arnaque

montée en Côte d'Ivoire. Ce qui s'est passé c'est que cette personne a rencontré une ivoirienne et lorsqu'il est tombé amoureux de cette ivoirienne elle l'a convaincu de se montrer sur sa webcam. Bon alors nécessairement l'objectif du monsieur qui était tombé amoureux de l'ivoirienne c'était de pouvoir rencontrer cette personne là. Finalement le monsieur c'était aperçu qu'il y avait juste lui qui pouvait mettre ces images et il n'y avait jamais de retour. Quelques jours après avoir envoyé sur webcam des images de lui en petite tenue, il a reçu un avis d'Interpol lui disant qu'il avait commis une infraction en Côte d'Ivoire et qu'immédiatement il devait payer une amende de 5000€ sinon d'une part il était dénoncé aux autorités Canadiennes et d'autre part ces images, cette vidéo allaient être publiée sur Youtube et éventuellement sur CNN, TF1 et d'autres réseaux télé. Il était un contrevenant en Côte d'Ivoire oui, alors malheureusement ce n'est pas le seul individu qui est impliqué dans ce type de stratagème et lorsque vient le moment d'intervenir pour localiser la provenance réelle de ce message frauduleux, si on a pas la collaboration internationale au niveau des pays Ouest Africains notamment d'où proviennent ce genre de messages, il nous sera impossible de pouvoir identifier la source et éventuellement de pouvoir enrayer cette problématique. Ce qui nous amène à constater que la réalité actuelle au niveau Africain c'est qu'actuellement il y a évidemment une hausse du nombre d'internautes qui est en constante croissance. On augmente dans les prochaines années la capacité d'accès à internet avec une amélioration de la bande passante notamment au niveau du continent Africain donc nous anticipons une hausse de la cybercriminalité. C'est incontournable, c'est certain que nous on anticipe un tsunami actuellement. Les besoin en terme de formation, les besoins en terme d'outils également sont très importants et c'est pourquoi la coopération internationale est essentielle. Nous avons donc profité du forum actuelle à l'ICANN pour réunir en fait 32 policiers gendarmes et magistrats du Sénégal et pouvoir assister à un atelier de formation général sur la cybercriminalité et également être en mesure d'écouter leurs besoins dans un objectif de leur apporter un soutien ou un apport plus important. Au niveau de leurs connaissances, de la formation, ICANN nous a permis de tenir cet atelier et les commentaires issus des différents intervenants policiers

gendarmes et magistrats furent très, très intéressants et nous allons pouvoir capitaliser sur çà dans le futur. C'était l'objectif de la présentation j'espère que çà vous a démontré un peu les initiatives en cours, çà va en continuité avec ce qui était présenté auparavant par mes collègues ici à la table. Je suis disponible également pour répondre aux questions éventuellement.

NII QUAYNOR: Merci beaucoup, je pense que c'est bien d'avoir quelques initiatives et c'est bien aussi de partager avec la Côte d'Ivoire qui aborde ce problème donc c'est une bonne chose. Bien, nous allons quitter l'Amérique du Nord et nous allons passer à l'Europe et nous avons la chance d'avoir Gary Kibby, de l'agence contre le crime organisé du Royaume-Uni qui va nous adresser quelques mots, merci beaucoup.

GARY KIBBY: Je vais essayer de parler doucement pour les traducteurs et d'être le plus clair possible. Je vois ici qu'il y a deux secteurs importants: le premier c'est le travail que mon organisation fait dans le service d'ordre et le deuxième secteur est un secteur opérationnel. Je dirais pour que la communauté réfléchisse un petit peu au processus dans lequel nous nous trouvons actuellement dans le domaine de la recherche, avec des problèmes en particulier et je pense que c'est une occasion de partager ces problèmes avec vous. D'abord l'organisation contre le crime organisé est une organisation basée au Royaume-Uni. C'est une combinaison de plusieurs organes et nous avons quelques différences par rapport aux organismes traditionnels de ce type parce que nous cherchons les problèmes de criminalité. Un des domaines dans lequel nous cherchons c'est l'abus de DNS pour le crime organisé du point de vue du crime organisé et le crime, les délits grave. L'abus de DNS touche à tout donc tout ce que nous avons, les derniers chiffres, ont été basés sur des opérations, une crise opérationnelle importante. C'est un secteur dans lequel nous entrainons des gens et c'est pour ça que nous travaillons avec la communauté et nous essayons de travailler avec, nous participons aux réunions d'ICANN pour être représentés auprès d'ICANN. Nous travaillons avec les organisations qui travaillent dans le

service d'ordre et le respect de la loi à travers le monde entier et nous travaillons avec AfriNIC, nous travaillons avec les RIR pour travailler en collaboration avec les services de la loi dans toutes les régions du monde. Nous avons eu des représentants et nous avons rencontré des représentants de tous les continents et lors des réunions d'ICANN. Ce travail global que nous faisons avec la communauté d'ICANN est très important pour nous. Interpol est représenté comme observateur au sein du GAC pour continuer à mettre en place et à exprimer nos points de vue en ce qui concerne l'abus de DNS. Je suis conscient que j'ai peu de temps, il est clair que le problème est complexe et je ne rentre pas dans le détail, c'est le respect de la loi dans le domaine de l'amendement et de la RIR ce que nous avons tout ce qui concerne les différentes manières concernant la due diligence. Nous avons un officier qui travaille de mon bureau lui-même, qui travaille actuellement dans le groupe WHOIS qui est un autre secteur important pour travailler dans le domaine du respect de la loi pour la révision des processus. Nous appartenons au groupe de travail donc dans le domaine des abus de DNS ce qui nous inquiète c'est d'identifier les choses qui peuvent apparaitre et qui vont avoir un impact sur les recherches et c'est la communauté et c'est vous-même qui pouvez identifier les secteurs dans lesquels il peut y avoir des problèmes qui nous concernent actuellement. Ces problèmes comme l'IPv6, les gTLD et les nouveaux gTLD, l'IDN. Nous avons aussi deux bureaux du FBI qui s'occupent du RCMD, qui s'occupent de ce problème pour essayer de comprendre le développement de l'internet dans le futur donc ce sont des secteurs, des domaines importants parce que pour le respect de la loi il s'agit d'un défi global, d'un défi mondial. A savoir, la communauté de l'icann est un groupe minoritaire et hélas pour le respect de la loi nous sommes aussi une minorité, un groupe minoritaire. Il y a beaucoup de secteurs d'application du respect de la loi qui ne comprennent pas l'importance du travail que l'on fait au sein d'ICANN et notre représentation ici comme les service d'ordre est vraiment trop basse. Un des secteurs dans lequel nous travaillons actuellement est le problème de la distribution des malwares. Nous savons tous ce que sont les malware, nous savons que les criminels vont utiliser toutes les possibilités pour explorer les faiblesses dans les systèmes et dans les processus parce

que c'est ce que les criminels font. Ils veulent faire de l'argent donc nous n'allons pas rentrer dans les aspects techniques que je ne comprends pas finalement c'est bien au delà de mon travail. Si nous parlons des domaines des personnes qui vont utiliser le contrôle pour prendre ces domaines c'est tout ce que je voulais dire et c'est quelque chose que l'on a constaté, que l'on constate en permanence à travers les bureaux d'enregistrement. Il n'y a aucune indication mais ces domaines vont être utilisés pour prendre le contrôle et prendre le contrôle signifie que l'on va faire cela pour réaliser une attaque malveillante. Si l'on regarde cela et si vous étiez une personne qui parle anglais vous pourriez vous demander de quoi il s'agit sur cette diapo et il ne s'agit de rien du tout ce sont des opérations automatiques que l'ont fait et que font les criminels, les délinquants. Ils font ce type d'opération en permanence et ce qu'ils cherchent c'est de pouvoir essayer de rentrer dans notre système parce que le système est tel que le processus qui existe actuellement pour l'identification des activités criminelles ne traite pas ce type de problèmes. Parce qu'une fois qu'ils ont identifiés on a un processus qui va aller au bureau d'enregistrement pour contacter le registrant. S'il est clairement criminel on a 15 jours plus ou moins donc en 15 jours ces personnes ont disparu. Nous n'avons pas le solution et ce que j'essaie ici c'est de vous présenter un problème opérationnel en termes de processus. Nous disons le respect de la loi, la due diligence, regarder le registrant, pourquoi est-ce que le registrant va vouloir enregistrer cela, est-ce que cela a une valeur commerciale? Donc chacun de ces points va soutenir le WHOIS, le WHOIS s'améliore un peu en terme de lutte contre le délit mais maintenant le WHOIS demande un niveau raisonnable de due diligence pour dire cela ne fonctionne pas. Ils s'améliorent, ils apprennent parce que plus nous travaillons au niveau de la loi au niveau du secteur industriel, beaucoup de gens apprennent beaucoup et répondent de mieux en mieux en termes de problèmes de WHOIS. C'est un problème important pour la loi, l'argent aussi est un problème pour ces enregistrements, on va faire cela avec des cartes de crédit volées, avec de l'argent virtuel. Ce sont des occasions de voler, je partage cela avec la communauté parce que si quelqu'un a une idée de cela ce secteur est basé sur un problème de faiblesse, de faiblesse dans les processus. C'est ce que je voulais vous

dire, merci de m'avoir donné l'occasion de partager ces soucis, ces préoccupations avec vous.

NII QUAYNOR: Merci beaucoup. C'était une très bonne synthèse et j'ai entendu des mots importants: collaboration, éducation et construction d'une communauté. Maintenant je vois qu'il y a des défis dans le domaine du processus, bien. Je vais maintenant vous donner la parole pour les commentaires, pour les questions, pour que vous ayez la possibilité de réagir allez-y le micro est ouvert et nous avons une dizaine de minute pour les questions.

STEVE DELBIANCO: Gary, une question pour vous, est-ce que vous pourriez nous expliquer un petit peu l'amendement du RIR sur lequel vous travaillez et dans quel sens vous pensez que ce sera efficace, c'est Steve Del Bianco qui a pris la parole et posé la question.

GARY KIBBY: Je pense que la question des RAA est une question importante. Je pense que çà a été très documenté en ce qui concerne l'application de la loi et il y a eu différentes discussions entre le GNSO et le GAC, au cours desquelles les réglementations ont été faites pour que l'on traite ces problèmes concernant l'abus de DNS. Je pense que les délinquants appartiennent au processus de l'évolution tel qu'il est et quel que soit le processus que nous suivons les criminels vont regarder cela. C'est une question qu'il faut continuer à partager des deux côtés donc en termes de recommandation je dirais qu'ils sont bien documentés et je pense que ce n'est pas vraiment nécessaire de voir les recommandations spécifiques qui existent.

ANTOINETTE JOHNSON: Bien vous avez peut-être dit cela pendant la session mais dans le but d'affronter l'abus de DNS, comment est-ce qu'on peut éviter de bloquer les demandes réelles de DNS? Des fois on constate que les véritables IP

sont bloquées parce que des personnes sont en train d'essayer de faire un abus de DNS non?

NII QUAYNOR: Lanre, vous voulez répondre à cette question?

LANRE AJAYI: Je pense que la prochaine session aborde cette question, on peut laisser cela pour la session des DNS et de l'annulation ou l'élimination de DNS.

>> Je suis mary, je suis du Nigeria et je voudrais dire que les agences de respect de la loi sont vraiment est-ce qu'elles travaillent vraiment sur le cybercrime. Quelques unes de mes découvertes à cause de l'enregistrement de domaine IP, s'il y a un délit l'IP peut ne pas être du Nigéria, elle peut être de n'importe où, de Chine par exemple et la légalité de l'adresse IP est remise en question donc il est très difficile pour eux de savoir qui est derrière ce délit. Ca c'est le premier, l'autre problème est que les personnes il me semble que lorsque le problème de travail entre deux ordinateurs a été développé sur internet personne n'a pensé à voir comment mettre un visage derrière un nom de domaine ou derrière une adresse IP. Je pense que qui veut lutter contre cela que ce soit au niveau du respect de la loi ou d'autre chose nous avons besoin de lIPpv6 nous devons nous occuper de cette brèche que l'ipv4 avait c'est-à-dire quel est le visage qu'il y a derrière cela. On peut s'enregistrer de n'importe où donc il faut pas que ce soit… les spams par exemple dans le cas du Nigéria ne viennent peut-être pas tous du Nigéria. Les faits restent que on ne peut pas mettre la main sur la personne qui a enregistré l'IP ou le nom de domaine qui est abusif. Je voudrais proposer ou questionner le fait que ou dire que la communauté internet regarde çà et comment obtenir cela. Même lorsque nous parlons de la cybersecurite ou du cybercrime et lorsque nous essayons de lutter contre cela comme le dernier orateur l'a dit bloquer des adresses IP qui sont bonnes ce n'est pas juste parce que cela arrive dans ce processus de lutte contre l'abus de DNS.

ROD RASMUSSEN: J'ai l'impression, j'espère que vous ne nous demander pas de mettre des informations d'identification dans les DNS.

>>: Je suis aussi du Nigeria, je ne voulais pas parler mais je pense que j'ai besoin de parler parce que ce qui vient d'être dit est correct. Nous avons fait des recherches à l'USC et nous avons trouvé que certains des emails envoyés depuis le Nigéria ne venaient pas en fait du Nigéria. Et je donnerais l'adresse du papier qui est disponible sur Internet, certains emails ne venaient pas en fait du Nigéria merci.

>>: C'est vrai mais la façon dont vous gagnez la confiance est en travaillant localement et globalement, et il y a toujours du travail à faire au Nigéria.

ROD RASMUSSEN: J'aimerais faire un commentaire sur la question du Nigéria, je dois féliciter la police nigériane qui a travaillé dur avec la police américaine pour adresser le problème du 409. Il y a eu beaucoup de démarches en commun avec des armes lourdes. Je pense que le Nigéria s'attaque à ce problème sérieusement mais ce qu'on voit maintenant c'est que beaucoup de gens le font et que de l'autre côté de la frontière pour faire le même crime. Lorsque vous appuyez quelque part ils vont ailleurs pour commettre des crimes dans d'autres pays qui sont maintenant impliqués et ca explique pourquoi il faut que ce soit une solution globale au problème. Je voulais vraiment montrer mon soutien aux officiels nigérians pour le bon travail accompli. Je voulais les remercier pour les compliments, nous faisons beaucoup pour réduire la menace mais on devait d'abord admettre que le crime et le cybercrime, les pourriels venaient du Nigeria et le gouvernement l'a admis. Ils ont mis sur pied l'ESSC et ils collaborent avec des organisations de police par exemple du Royaume-Uni. Ils font du travail au Nigéria et les Etats-Unis également. Nous luttons et les criminels s'en vont du Nigeria qui maintenant est presque libre de tout crime grâce à nos efforts et ceux de la police.

maintenant vous êtres libres de faire des transactions et des affaires avec le Nigeria.

>>: Je suis de la fondation internet et j'avais un commentaire sur le problème présenté par Gary Kibby qui a souligné la précision du whois. En Estonie, l'année dernière nous avons élaboré une solution selon laquelle le registre de domaine avec chaque nom de domaine il y a une personne privée ou une entreprise qui est responsable de ce nom de domaine. Cette personne privée ou compagnie est également identifiée donc il n'y a pas d'anonymat, d'inscription anonyme dans le registre de domaine et nous avons beaucoup de noms de domaines, environ 64000, cette solution peut-être échelonnée a l'échelle mondiale et est basée sur FATF 40 + 9 recommandation sur le financement et selon ce groupe d'unité internet financier ce cas de travail est déjà introduit dans plus de 100 pays. Nous avons modifié le protocole IPP pour que les registrars puissent attacher des informations à ce protocole pour prouver l'identification des registrants et utiliser les informations qui améliorent cette identification du registrant avec une inscription du nom de domaine. Nous stockons ces données d'identification dans notre centre de registre.

GARY KIBBY: C'est très intéressant merci nous allons approfondir.

NII QUAYNOR: Merci beaucoup pour votre participation, nous allons passer à la seconde session et celle-ci c'est comment attaquer les comportements malicieux impliquant des noms de domaine? Cette lutte a évolué de la théorie à la pratique. L'absence d'uniformité politique pour aborder ces préoccupations, les professionnels, la police et les agences de police, les compagnies privées se basent sur une coopération volontaire ou un processus juridique pour accomplir ces luttes. Les panélistes vont explorer l'efficacité et les défis associés à cette pratique et le rôle

d'ICANN dans celle-ci. Nous avons je crois 4 présentateurs donc je demanderais à Michael Moran de Interpol de mener la discussion.

MICHAEL MORAN: Je suis Irlandais, vous avez surement peut-être deviné à mon accent et tout ce domaine de ce qu'ICANN peut faire sur les noms de domaine et de ce que n'importe qui peut faire au sujet des noms de domaine. Peut-être que les vendeurs de noms de domaine pourraient faire quelque chose, peut-être que ce serait bien d'ouvrir sur l'idée que monsieur le public, Joe Public, sa mère l'appelle Joseph mais tout le monde l'appelle Joe. Joe Public va découvrir, on lui a dit qu'il peut aller à une base de données WHOIS et il peut trouver d'où le nom de domaine provient, la personne chargée de ce nom de domaine. Finalement il se trouve à aller dans des sites web de solution de réseau parce qu'il sait comme ces compagnies qui ont vendu ces domaines et c'est ce que j'ai fait y'a environ une heure de cela. Et il essaie de trouver où sur ce site web, où il peut aller pour dire qu'il a un problème avec un produit vendu par cette compagnie et donc il voit qu'il peut acheter tout les noms de domaine ici et avoir 40% de rabais sur les certificats SSL. Il peut même aller ici et il peut acheter un domaine XXX parce que sunrise est ici, il peut avoir le site web mobile, avoir un Microsoft Exchange. Il peut aller aux petits caractères et il ne trouvera pas l'abus nulle part donc il va essayer de contacter la compagnie et là il va trouver tout au sujet des ventes et du service à la clientèle mais il ne pourra pas trouver quoi que ce soit de quoi que ce soit. Il va faire un peu de recherche additionnelle et il trouve Peter Public, son frère, et lui décide qu'il va contacter la personne avec qui il a un problème au sujet du problème qu'il avait la semaine d'après. Il va, il nomme parce que c'est eux qui ont vendu le site web problématique, il passe en vue toute la liste lorsqu'il va jusqu'en bas et il regarde toutes les jeunes jolies filles qui vendent des plugins. Il va en bas et de la page et finalement il trouve rapporter l'abus de domaine bravo ENOM très bien, donc il entre il dit je veux rapporter le fait que j'ai été victime d'un comportement malveillant de votre client et il voit qu'il ne peut pas rapporter quoi que ce soit sur la pornographie enfantine, l'hameçonnage mais il peut rapporter les pourriels. Il a reçu des spams, donc il peut rapporter des spams, au

moins il peut le faire parce que lorsqu'il a appelé son cousin Phileas c'est que Phileas Public lui avait un problème avec GoDaddy qui est une fantastique compagnie, beaucoup de gens beaux et brillants qui vendent des produits magnifiques et je ne vais jamais critiquer une entreprise qui fait de l'argent parce que c'est ce que font les compagnies, elles font de l'argent. Finalement il regarde tous les beaux gens, les belles personnes et c'est ce 9.99$ pour les nouveaux.com et il va consulter tous les onglets, non, non on peut pas rapporter les abus… ah finalement rapporter un pourriel mais c'est seulement un problème de programme malveillant. Mais au moins il peut faire un rapport, il va rapporter pourriel il rentre et il trouve qu'il peut mettre son nom, son adresse et il y a un menu déroulant est-ce qu'il peut dire qu'il y a eu un hameçonnage? Il peut voir regarder jusqu'en bas il peut rapporter Divers donc bravo GoDaddy c'est que tout simplement c'est du spam donc pourriel au début mais je peux pas parler d'hameçonnage. Je ne peux pas rapporter de documents pédo-pornographiques, je peux théoriquement mais ce que j'essaie de vous faire comprendre dans le temps qu'il me reste c'est que pourquoi est-ce que certaines entreprises ne prendront aucun rapport? C'est très difficile de trouver et d'autres ne prendront des rapports que sur des pourriels ou ils ne le montrent pas. Bien sur je peux rapporter ce que je veux parce que je suis Phileas Public, Joe Public et Peter Public et je suis une personne raisonnablement intelligente. Je sais que je peux rapporter ce matériau, même si je peux le rapporter comme document pornographique, même s'il est dit que je ne peux rapporter que du pourriel pourquoi seulement que les pourriels? Pourquoi est-ce que l'abus ne pourrait pas être rapporté de manière normale? Pourquoi le pourriel ne pourrait être rapporté de manière normale ou autre type de manière normale pareil que pourriels par les deux bons acteurs qui prendront le rapport par rapport à ceux qui ne sont même pas intéressés à recevoir les rapports? Est-ce que c'est une question d'intérêt ou bien de renier l'esprit de RFC2142 écrit par Steve Crocker, je sais pas c'est peut-être un vieil homme.

>>: C'est en fait Dave, son frère.

MICHAEL MORAN: J'imagine que Steve est quelque part, Steve a ajouté des choses aussi Steve et Dave sont deux vieux hommes qui sont en train de fumer leur pipe sur une véranda quelque part. Mais si on cherche, on va trouver le mot abus et on va voir qu'il y a plusieurs problèmes. Un étant les domaines qui devraient avoir abus@domaine.quoi_que_ce_soit. Il devrait y avoir des relations clientèle pour les comportements publics inappropriés. J'accepte que les compagnies doivent investir des ressources mais j'accepte, je m'attends qu'il y aurait de grandes quantités et pour le thé dites moi ce que je mange pour le diner vous avez plus de temps la. Pourquoi? Parce que les trois entreprises que j'ai montrées sont parmi les plus grandes et elles violent l'esprit du RFC et ils donnent vraiment beaucoup le mauvais exemple aux autres, aux acteurs inférieurs. Vous avez le haut et ensuite vous avez les vendeurs et jusqu'en bas les petits acteurs dans ce jeu et c'est le mauvais exemple qui commence jusqu'en haut. Si vous avez un problème parce que c'est vous parce que c'est certainement pas le mien et j'aimerais que cela change merci.

NII QUAYNOR: Merci c'était très clair. Maintenant je voudrais inviter Rod Rasmussen, d'un groupe de travail qui va nous donner son point de vue je suis heureux que vous soyez le suivant.

ROD RASMUSSEN: Donc, je vais vous parler de quelque chose de tout à fait différent. Je vais vous parler de quelque chose que beaucoup d'entre vous connaissent, il s'agit de l'abus du processus de suspension de résolution de l'abus de nom de domaine. Donc pour ceux qui n'ont jamais entendu parler de cela, de ce processus de révision, je vais vous parler de ces objectifs. Il y a une façon pour les gens qui travaillent dans le respect de la loi ou dans les services de l'ordre ou qui ont des noms de domaine comme des grandes banques, une compagnie, une marque importante et qui ont une façon de travailler avec les registrars d'interagir avec eux en toute confiance et qui ont un système très précis et contrôlé un

système fiable pour la suspension d'un nom de domaine. Ici, nous allons aller au cœur de la question pour savoir ce qui existe, le rôle, la façon dont les gens interagissent dans le secteur de la suspension de domaines et l'échelonnement, la meilleure façon de travailler dans le système. Cela peut être fait comme un processus qu'il doit être possible de répéter. C'est de ca que je vais parler et il s'agit strictement du cas des domaines qui sont enregistrés par des personnes délinquantes, c'est pas pour annuler des domaines qui n'ont pas qui ont des problèmes. Les sites de fishing sont dans des services de noms de domaine qui sont compromis donc on a des cas ou ce n'est pas le nom de domaine qui est éligible c'est seulement le nom de domaine qui est enregistré par des délinquants. Nous avons une série d'indicateurs concernant les détails ici, tout ce dont il faut tenir compte normalement, le processus qui est rapporté pour la suspension du nom de domaine et les différents critères utilisés. Nous avons déjà discuté de certains de ces points, quel est le risque d'intervenir avec des gens qui essaient de suspendre les noms de domaine et pour la partie qui est de l'autre côté le registrant et le registrer avec lequel il travaille, c'est un problème. Je dirais que çà peut donner beaucoup de problèmes à tout le monde, et c'est un petit peu ce qui explique notre travail. Le fondement ici, que nous voulons que ces systèmes soient remplacés et nous voulons construire un système, un modèle dans lequel on pourra maitriser les abus avec une large gamme de communauté viable et aller plus vite lorsque nos opposants s'occupent de ces questions. Actuellement nous avons des barrières qui existent entre nous alors que nous sommes du même côté, nous luttons contre les mêmes choses donc nous voulons surmonter ces barrières. Voila ici, voyez cette beta 3.1, cette présentation a été faite à Los Angeles je pense et c'était une idée brillante. Nous avions un système, nous avons regardé, il y avait une réunion qui avait eu lieu a San Diego on est allés à l'APWG avec une réunion à San Diego. On a regardé le programme, c'est un programme dans lequel on a parlé de suspension, ça nous intéressait donc on a travaillé avec notre propre groupe beta. Je vais vous expliquer un petit peu plus dans le détail cette question mais nous avons exposé des critères. Les gens connaissent ce document, il y avait beaucoup de documentation que les gens devaient remplir pour rentrer dans le programme pour s'assurer que l'on avait

une partie légitime dont les employés étaient vérifiés et qu'il s'agissait d'une organisation financière ou entrepreneuriale dont on était sûr. Tout était couvert, la personne faisait une demande si elle avait un problème avec sa demande on s'assurait que tout allait bien. Voila, c'est ce qu'un candidat va voir, il y a tout un processus pour faire une demande de candidature pour l'utilisateur du système, il y a différents rôles qui sont joués par le directeur. Il y a un comité qui va contrôler les credentials de ceux qui se présentent, se portent candidats et s'ils peuvent participer au programme. Si cette organisation à le droit de participer au programme, on va vérifier ensuite les individus qui appartiennent à cette organisation. C'est ce que ça donne pour l'intervenant lui-même, nous travaillons avec un logiciel qui nous a donné de bons résultats ces dernières années. Voila le minimum requis, voyez la demande, il faut entrer dans le domaine il faut donner le site internet il faut voir il y a des pré-requis très élevés dans le domaine des contenus malveillants et des contenus non légitimes. Vous allez signer tout cela électroniquement, ensuite je vais vous montrer à quoi ça ressemble, vous voyez et je dois donc présenter les critères et dire parce que cela permet de suivre, d'avoir une série de statistiques sur qui a demandé de suspendre. Cela donne lieu a des recherches approfondies pour voir ce qu'on va faire en tant que communauté pour résoudre ces problèmes non pas seulement du point de vue de la recherche mais aussi qu'est-ce que le registrar va pouvoir faire. On va leur faire une demande, ils vont décider ce que le processus va faire avec cette demande en particulier. Ils vont avoir cette relation avec le registrant et cela se passe sur le niveau du registrar, on ne peut rejeter cela sauf si on a besoin de davantage d'informations. Je vais vous donner une invitation, ca dure juste une minute, voila. Il y a un système de suivi pour voir un petit peu ce qui se passe des deux côtés, avoir des informations. Quel est le statut des différentes requêtes? Des différentes demandes? Voila la dernière diapo, je crois que d'une certaine façon nous avons créé un système rigoureux qui est applicable et qui peut être modifié, nous avons des membres dans notre programme. Nous avons 7 registres, des ccTLD qui sont intéressés par le programme et certains d'entre eux n'ont pas rendu cette information publique encore. Il y a des noms ici, une liste que je ne peux pas vous

montrer et j'ai déjà parlé avec différents registres au cours de ces dernières années donc si vous êtes un registre ou même un registrar, s'il vous plait n'hésitez pas à me contacter, merci.

NII QUAYNOR: Bien, on continue, on passe à DON BLUMENTHAL du registre d'internet public des Etats-Unis.

DON BLUMENTHAL: Je vous remercie, voila mes diapositives. Je suis ici pour l'intérêt public et il est clair que notre rôle ici dans le domaine de l'annulation de domaines est que nous donnons des ordres pour retirer le domaine du système. Le PIR est intéressé pour travailler avec la loi et nous aider, c'est le nom de notre organisation Registre d'Intérêt Public, ça implique cela. Nous avons un rôle concernant l'intérêt public que nous prenons tout à fait au sérieux et les personnes qui font respecter la loi sur internet n'existent plus. Il y a une espèce de conscience de faire ce qu'il faut faire j'ai travaillé pendant des années dans le domaine du service de l'ordre et je pense que c'est important d'essayer de trouver ici des mesures à prendre. On a entendu ici la suspension de domaine, on a entendu la redirection, le blocage de domaines, le filtrage de domaines et dans une série de termes qu'on utilise sur internet actuellement je pense qu'une partie du rôle que nous pouvons jouer aussi ou du rôle que je peux jouer est de suggérer que toutes les différentes techniques ont des forces et des faiblesses. Le problème ici crucial dans toutes les actions de respect de la loi sur internet est d'avoir un contenu sur le système pour s'assurer de retirer le contenu sur le système, pour s'assurer qu'il ne sera plus disponible et lorsqu'on fait une redirection, lorsqu'on retire ce n'est pas à mon avis la meilleure façon de le faire. On peut faire ce qu'on veut, on peut aller et dire fermer ce serveur, c'est facile lorsque le serveur, lorsque le juge était en Virginie et qu'on était a Washington. C'était facile, on faisait tout ça en 15 minutes ou dans un rayon de 15 kilomètres, mais ça ne marche plus et ça ne se passe plus comme çà. Les gens sont devenus trop intelligents en termes de dispersion de contenu, d'utilisation de différents domaines, de différents domaines de premier niveau, de différentes techniques pour

éviter ce type d'actions. A nouveau je dirais que chaque mesure a sa force et sa faiblesse et chaque mesure a des effets potentiels. Parfois on regarde et on dit est-ce que c'est le remède est-ce que ces effets collatéraux sont plus graves que le remède? Il y a actuellement un débat qui a lieu aux Etats-Unis concernant l'utilisation de la redirection. La redirection du traffic peut parfois être très utile dans certaines situations, mais dans d'autres situations cela ne l'est pas, notamment lorsqu'on parle de problèmes de propriété. Les gens doivent avoir un encouragement pour essayer d'éviter l'ordre du tribunal, c'est facile à faire donc ici la question qu'on peut se poser est est-ce que ça vaut vraiment la peine. D'autre part la redirection pour arrêter un problème de pourriel, un problème de spam, beaucoup de personnes vont essayer d'arrêter des délinquants qui ont des activités dans le domaine des malwares. Mais je pense qu'il faut essayer d'évaluer quel est l'objectif de ces gens là et cela avec un mécanisme d'application de la loi approprié. Je pense que les autres choses qui sont en jeu ici, on en a parlé dans d'autres sessions, c'est un service d'application de la loi dans les communautés de registrar et qu'il soit en contact les uns avec les autres. On peut espérer que en utilisant la bonne terminologie pour accomplir ce qui est nécessaire. On a eu un ordre de retrait, il n'y a pas longtemps, de retrait dans lequel on disait on vous donne seulement la moitié de l'information nécessaire pour le faire nous voulons le faire maintenant il a fallu retourner voir le procureur et lui dire écoutez nous ne pouvons pas le faire donc il y a un secteur dans lequel on doit travailler avec la loi pour essayer de mieux viser, de cibler notre activité. Il y a quelques années, il y a un domaine qui a été retiré mais parce qu'on avait de nombreux domaines qui étaient parallèles qui ont été détruits aussi qui ont été annulés aussi. Il faut vraiment identifier la meilleure façon au niveau technique de faire cela, la meilleure façon de s'assurer que les choses sont faites dans le bon ordre, correctement pour qu'elles n'aient pas d'effet secondaire dangereux, voila merci.

NII QUAYNOR: Merci beaucoup, je pense que nous allons passer à la dernière présentation qui sera de TITI AKINSAMNI de l'université de Sweet Waterstrand en Afrique du Sud.

TITI AKINSAMNI: Bonjour tout le monde, j'ai la dernière portion de la session et je vais donc faire quelques commentaires à la fin de la présentation. Je vais parler lentement pour les interprètes mais je vais passer en revue mes diapositives plus rapidement pour présenter mes quelques points que j'ai noté dans la conversation. Les attaques des noms de domaine, la violation des droits d'internet et la liberté. Je parle comme quelqu'un qui est souvent prise entre le processus de comprendre les raisons pour lesquelles les noms de domaine sont éliminés et j'ai la possibilité d'avoir accès à tout ce dont j'ai besoin et je regarde de loin où les criminels m'ont visé. Soit j'étais vraiment très importante pour 3 milliards de dollars qui doivent être déplacés d'ici à là, ou lorsqu'on parle qu'ils affirment que c'est des membres de ma famille lointaine et les cartes de crédit ont été utilisées pour faire des achats et mon identité volée. Je vais présenter différentes tendances que j'ai remarqué surtout le cas de l'Afrique du Sud que je vais mentionner. Je suis nigériane par naissance, oui, faites des affaires avec nous, nous sommes un bon peuple. Mais j'habite à Johannesburg et c'est la que j'habite depuis 8 ans. Ensuite je vais parler surtout du concept de progression, on doit respecter les droits et libertés peu importe la direction qu'ils prennent et surtout le rôle d'ICANN. George Orwell a dit en1944 que le mot « fascisme » est un mot presque sans sens. Je suis d'accord avec lui je ne sais pas combien de gens connaissent le programme ICE et surtout je parle a la lutte contre rojadirecta.com. J'adore le football et j'étais vraiment contente que Manchester City ait battu Manchester United mais parfois comme j'habite dans un pays en voie de développement je n'ai pas accès à ces parties donc je dois aller sur rojadirecta.com. J'ai consulté le site et un jour je peux voir le forum je peux avoir accès à tout cela parce que j'ai suffisamment d'informations et j'ai accès et j'ai assez de connaissances pour le faire et je comprends que ça a été mis en panne, même lorsque les tribunaux espagnols ont dit que ce site est légal, mais une autre institution, un autre gouvernement est capable de l'éliminer. Voila, il est parti pas seulement.com mais également rojadirecta.org donc, vous pouvez amener le dalaï-lama, tout ce que vous voulez, Gandhi, on va vous faire tomber, on va faire tomber et c'est fini. Ensuite y'a l'affaire Wikileaks que j'appelle l'élimination furtive. Je ne suis pas

pour ce que fait wikileaks, cette conversation est pour un autre forum, mais wikileaks n'est pas éliminé directement mais de manière furtive. J'adore James Bond les opérations James Bond ont eu lieu avec wikileaks et au cours des dernières 12 mois, même pas 12 mais 5 Julien Assange a du annoncer qu'il doit arrêter de publier parce qu'ils ont des difficultés financières. Parce que quelqu'un, quelque part, qui je sais pas, institution, gouvernement, secteur privé ou autres a réussi à bloquer leur capacité a recevoir des fonds. Même le système de base, donc c'est une façon très créatrice, très innovante, d'éliminer un site web donc l'Afrique du Sud pour ramener les choses à ce que je connais. La législation électronique en Afrique du Sud offre une protection pour la responsabilité des ISP afin qu'ils reçoivent un avis pour éliminer quelque chose et qu'ils agissent. Ils sont protégés ou ils n'ont pas agi là-dessus alors ils ne sont pas protèges et si vous êtes celui qui avez ce contenu, le contenu étant le système de DNS vous êtes protèges jusqu'à une certaine mesure. Mais si vous suivez ce que nous disons mais quelque part au milieu on revient a la conversation que j'avais eu avant pour regarder mon football et je ne peux le regarder d'aucune autre manière donc que se passe-t-il l'utilisateur final pris au milieu et par rapport à la session je voulais dire que j'aime la légitimité. J'aime avoir des informations correctes. Une des choses que je voulais avoir c'est que je suis allé sur l'association des fournisseurs de service internet pour l'Afrique du Sud, j'ai demandé des données pour les types de demandes d'élimination, on m'a demandé qui êtes vous et pourquoi voulez-vous l'information. Je suis un utilisateur internet et ca et j'ai le droit de poser cette question. C'est pas des informations classées mais « qui êtes-vous et pourquoi vous avez besoin de cette information » et j'ai dit je suis un membre d'ICANN et j'ai eu les informations donc ca vaut la peine d'être membre de l'ICANN, ça sert à quelque chose. J'ai obtenu les informations que depuis avril 2005 ils ont eu des requêtes pour 284 mises hors service et ce qui s'est passé avec ISBA qui est l'association d'Afrique du Sud. Il y a certains membres qui a une requête de mise hors service y'a aussi pas de problèmes avec goddaddy c'est l'adresse email à laquelle vous répondez pour chaque requête une fois que cela est fait il n'y aucune clarté sur le propriétaire du nom de domaine qui sera informé et vous pouvez avoir accès au nom de

domaine ce matin mais deux minutes après c'est parti. En 2010 il y a eu 148 requêtes de mises hors service parmi celles-là 80% ont été approuvées. La prochaine question de cette organisation demande est-ce que je pourrais avoir les détails des types de contenu des noms de domaine qui ont été mis hors service. Je suis optimiste, je demande et on m'a dit non on a besoin d'une reconnaissance formelle officielle de qui vous êtes, on donne plus d'informations. Finalement on m'a dit vous ne pouvez pas avoir ces informations, on a besoin d'avoir davantage d'informations sur qui vous êtes et ce que la fin. C'est ma suggestion, c'est de la je parle dans une pièce remplie de personnes informées donc je fais attention pour ne pas essayer d'aborder les mêmes problèmes sans intérêt. L'internet y'a des droits fondamentaux et vous avez des droits fondamentaux qui se répercutent sur l'internet et nous devons aborder 6 d'entre eux. L'internet est pour tout le monde alors vous devez pouvoir vous assurer que si vous allez me refuser l'accès a quelque chose dont j'ai besoin que je sois informée. Deuxièmement la liberté d'expression et d'association c'est une discussion très longue on va pas continuer mais donc il y a accès aux connaissances, à l'apprentissage, à la création et bien sûr je pense trois autres thèmes. Si vous voulez davantage sur ces droits allez à apc.org donc j'ai parlé procédure en Afrique du Sud donc c'est l'approche que je prends lors d'un cas parce que je pense qu'on nous a dit spécifiquement que nous devons parler de ce que ICANN fait en termes. Je suis la seule femme je demande la possibilité de m'exprimer.

NII QUAYNOR: On vous a entendue.

TITI AKINSAMNI: Donc la question soulevée, la première, est-ce que c'est une violation? Quel type de question est soulevé comme on pourrait qualifier d'abus et une fois que un suivi doit être préemptif, cela doit être affiché publiquement. Jusqu'à présent nous n'avons pas d'information de ICE sur on nous obéit pas on a pas d'information de ICE sur les tribunaux espagnols donc les parties doivent être informées. Troisièmement à chaque fois qu'il existe des règles intermédiaires, il faut les explorer je

ne dis pas que c'est pas dans mes mains de soulever cette question, mais si nous cherchions certaines formes de systèmes ça fonctionnerait pour les trois parties, c'est-à-dire les agences de police qui ont le droit de pouvoir s'assurer qu'on soit en ligne sans danger, également pour s'assurer que les criminels soit pris dans les délais et que ces choses soient éliminées quand c'est nécessaire jusqu'au troisième niveau lorsque les institutions, les utilisateurs finaux doivent se sentir en sécurité et sans violation. Ensuite le cout qui va payer pour cela? Deuxièmement quel système juridique mais non judiciaire peut servir de plateforme juridique pour résoudre ces problèmes ICANN doit être dans une position pour que les éliminations de noms de domaine, les mises hors service des noms de domaine sur toutes ces questions puissent être abordées, avoir une pensée collective là-dessus et empêcher les influences négatives. Je donne deux exemples, un d'une manière furtive et l'autre de manière dictatoriale, peu importe comment vous le qualifiez en étant agressif donc on doit trouver un système ou il ne peut pas y avoir d'abus faciles par les intérêts du secteur privé ou public. Donc pour conclure, j'aimerais dire ce qui suit:les mises hors service DNS sont quelque chose de complexe, l'industrie et le gouvernement qui sont en mesure d'aborder les problèmes liés a la mise hors service d'un nom de domaine le font avec un certain succès. Mais si moi en tant qu'utilisateur finale je dois pouvoir rapporter des problèmes vers qui dois-je me tourner et bien sur si la personne qui a tué l'ambassadeur nigérian avait des recours il ne l'aurait pas tué, merci.

NII QUAYNOR: Merci beaucoup, je pense que nous n'avons plus beaucoup de temps donc j'aimerais obtenir directement des commentaires du public.

DON BLUMENTHAL: Si je peux dire brièvement, c'est un bon exemple de la facilité de contourner des décisions de tribunaux. Si c'est le site a été remis en service rapidement.

BERTRAND DE LA CHAPELLE: Je suis Bertrand de la Chapelle et je suis un membre du directoire ICANN et je suis représentant du GAC Français. Je veux dire qu'au cours des un an et demi la discussion sur les défis confrontés par la police malgré tous les problèmes qui émergent actuellement, pour moi la discussion est plus factuelle. Je veux soulever deux arguments le premier est pour Michael Moran, j'ai vraiment aimé votre discussion mais si je regarde d'une autre perspective, si je veux aller au site web du registrar pour faire une plainte il faut comprendre le système et vous êtes exposé au WHOIS et qui était la personne qui s'est enregistrée au registrar, qui était le registrar, donc une des questions que je voulais poser c'est quel type de discussion est-ce qu'il y a eu pour d'autres types d'opérateurs par exemple. Je pense à des choses que les utilisateurs utilisent comme simple reflexe. Second point, c'est par rapport à ce que titi disait, je voulais formuler le problème qu'elle a décrit pour ICE par exemple comme problème de souveraineté fondamental qui est un problème de compétence aujourd'hui. C'est la question suivante, comment est-ce qu'un gouvernement national se sent lorsqu'une activité menée par un citoyen de ce pays qui est absolument légale selon ce pays sont empêches par le tribunal d'un autre pays B parce que le nom de domaine que cette personne utilise a été acheté à travers soit un registrar dans le pays B ou j'imagine même dans le registre du pays B. Est-ce qu'on peut dire donc est-ce qu'on peut dire simplement que aujourd'hui par ce que.com et.org sont des registres qui sont basés dans la compétence des tribunaux américains la juridiction américaine, les tribunaux, la législation peut être applicable sur tous les sous-domaines enregistrés dans le registre c'est une question de nature juridique.

NII QUAYNOR: Prenons, on va prendre quelques questions.

MARGIE MILAM: Je vais lire une question du chat et quelqu'un du panel, n'importe qui des panelistes peut répondre. Comment est-ce que les mises hors service des DNS vont fonctionner avec le DNS peer to peer qui sans contrôle central.

ROD RASMUSSEN: Pas aussi bien je crois, cela dépend bien sur du point de vue de l'élimination du nom de domaine de la racine d'un TLD. C'est la même chose peu importe si c'est p2p ou autre. Du point de vue du filtrage et du blocage ca dépend de où vous le faites au sein de votre propre réseau. Peu importe parce que votre résolveur de DNS c'est celui qui fait le filtrage ou le blocage de pair à pair. Il va continuer peu importe les ressources que vous protégerez derrière, il va continuer à marcher. Si le filtrage ou le blocage est upstream ca va probablement pas marcher très bien donc ca va dépendre de où vous allez faire le blocage et comment vous allez le faire.

MICHAEL MORAN: Je voulais répondre à Bertrand de la Chapelle je suis d'accord, nous dans la police et je dis nous la police parce que vraiment on est pas à la hauteur de la tâche et j'ai un sergent qui disait qu'est-ce que votre mère penserait si ma mère disait qu'elle perdait de l'argent sur ebay. Excusez-moi, n'importe quelle installation en ligne elle ne peut pas le faire c'est pas parce que nous sommes encore perdus dans la brume mais le plus grand problème que nous ayons vous avez parlé d'un navigateur. Mais les personnes des droits civiques, l'industrie, la police, l'université c'est les paramètres de mesure, les métriques on ne connait pas l'étendue du problème on ne connait pas la définition du problème donc dans un pays le cybercrime est défini différemment et les rapports sont enregistrés différemment. Parfois pas du tout et le résultat est que nous ne pouvons avoir de bonnes politiques et aborder des problèmes difficiles tels que TITI a mentionnés sans savoir la portée, l'étendue, la gravité du problème donc est-ce qu'on a besoin d'une plateforme de rapports, oui.

ALEJANDRO PISANTY: Bonjour je m'appelle ALEJANDRO PISANTY, je suis professeur de l'Université Nationale de Mexico et président de la succursale de mexico pour l'internet. Le blocage, filtrage de noms de domaine partage beaucoup de caractéristiques avec les différents formes de blocage sur

l'internet qui a été je veux dire présenter ma perspective a monsieur Moran parce que Interpol bloque mon. Je suis donc venu à Dakar et 18000kilometres de déplacement pour le dire que j'aime beaucoup son travail le problème avec le blocage que nous voyons sont fondamentaux il faut résoudre la conduite humaine et son problème qui est le crime, le délit, les abus, la pornographie infantile et toutes les ramifications qui existent dans ce domaine. Dans la session d'IGF au Kenya le mois dernier il y avait un bon exemple sur lequel on doit se focaliser. C'était un officier de la loi Australienne qui décrivait le suivi d'un crime qu'ils avaient fait, l'enquête qu'ils avaient fait. Quelqu'un qui vendait des relations sexuelles en direct avec des mineurs donc cette homme a été le père de deux petites filles et nous ne devons pas, nous ne pouvons pas améliorer ce type de problèmes en bloquant, en filtrant ce type de films, de sites en refusant, en bloquant. Nous devons continuer à nous bloquer sur les êtres humains de la société, à construire des institutions, un système d'humains pour lutter contre le crime. Nous devons créer les outils qui servent à compenser les effets de ces informations qui existent, mais nous devons nous focaliser sur la conduite et sur la façon de mettre en place les institutions. Nous avons besoin de davantage de couches, une fois que nous avons ce système de couches, une fois que nous avons ces outils ça nous permet de travailler au niveau institutionnel. Et puis on peut redescendre une petit plus bas. Un forum comme ICANN, comme la gouvernance d'internet comme, d'autres types de forums avec des parties prenantes des multiples parties prenantes qui participent. Nous devons mieux comprendre ce que l'on veut si je vous ait pris quelque chose comment je vais être puni et voir quelles sont les lois que nous partageons entre les différents pays.

WENDY SELTZER: Merci, je suis un conseiller pour le groupement d'utilisateurs non commerciaux qui a découvert les effets d'un site commercial qui représentait des menaces légales et qui a aidé les utilisateurs à comprendre que le contenu en ligne n'était pas disponible parce que des plaintes avaient été portées contre cela. Lorsque nous pensons a des outils pour annuler, pour fermer rapidement des sites qui sont dangereux c'est intéressant parce que vous représentez un outil qui

parait utile pour en tout cas dans la conversation, est-ce que vous pensez à la transparence et à la façon dont les utilisateurs d'internet, les chercheurs comme Titi peuvent trouver des raisons pour lesquelles des noms ne fonctionnent plus, qu'est-ce qui est arrivé avec leur contenu et ce que les utilisateurs peuvent faire pour récupérer cela, si il y avait un contenu légitime qui était associé a ce site mais qu'il était utilisé pour les pourriels qu'est-ce qu'on peut faire pour améliorer la transparence pour aider le public et s'assurer que tout cela est utilisé de manière légitime.

NII QUAYNOR: Un commentaire du panel?

ROD RASMUSSEN: Je vais répondre à la dernière question si vous voulez bien, je pense que c'est exactement ce que nous essayons de faire au niveau du système. Donner la capacité aux gens de savoir ce qui se passe. Nous avons un système actuellement qui n'est pas transparent, tout est un petit peu entre les gens qui se connaissent ou qui essayent de faire quelque chose qui est basé sur un rapport. L'idée qui est derrière ce système c'est qu'il y aura ce système de APWG et qu'il y aura des contenus, des statistiques qui seront publiées sur ces contenus. Nous travaillons avec des académies, nous essayons de faire des études sur différents problèmes et nous voulons aussi créer un système de redressement qui nous permette d'avoir un petit peu des commentaires des personnes qui ont fait des actions donc nous voulons reconstruire ce système. Nous avons entendu beaucoup de choses de la part de gens comme vous, des préoccupations, nous les partageons, nous ne voulons pas retirer des contenus légitimes seulement des contenus sujets à controverse. Nous sommes d'accord et nous devons lutter contre le fishing et les opérations de malwares, c'est tout sur internet.

NII QUAYNOR: Je vous propose de prendre les commentaires et les questions que vous avez et on y répondra nous allons y répondre allez-y Mouhamet.

MOUHAMET DIOP: Merci Monsieur le Président je voudrais, lorsqu'on regarde les chiffres le nombre d'acteurs qui travaillent dans le domaine des différents et de l'application de la loi pour le DNS je voudrais séparer deux cas le cas du CCTLD et le cas des GTLD des noms de domaine c'est très important pour moi. D'un autre côté je voudrais vous présenter, vous dire qu'il y a beaucoup d'acteurs en terme d'intervention et d'action des réglementations la loi en tant qu'acteur global la police les tribunaux etc. Et si on a un cas, si on regarde les exemples dans le secteur du téléphone portable parce que beaucoup de problèmes se passent là les réglementations ont fait une série d'infrastructures pour résoudre ces problèmes et je suis heureux de vous annoncer qu'une des meilleures résolutions que le monde a vu pour le marché du téléphone portable est au Nigéria. On a créé une cour pour l'industrie du portable où tout cela est traité par les acteurs du secteur, ils vont voir les plaintes et il y a un responsable pour chaque région. Les gens ont la possibilité de se plaindre et cela est résolu et les gens vont revenir deux mois après pour voir ce qui est fait et si il ya des résultats. Revenons au système des noms de domaine. Ce qui se passe c'est que je suis un registrant, lorsque les gens ont un problème la première chose c'est qu'ils ne savent pas à qui ils doivent parler. La réglementation dans notre environnement, je suis navré de devoir le dire ne s'inquiète pas pour la question d'internet. Les gens ne connaissent pas cela y'a un problème de formation, de compétences, les gens doivent être formés pour pouvoir demander aux organisations responsables de s'occuper du problème si j'ai un problème de cybercrime je peux vous dire ou vous pouvez aller voir mois après mois aller voir la police. La première chose c'est qu'on va essayer d'abord de comprendre de quoi on parle et ca va prendre des mois. Je suis sérieux ici c'est un problème de CCTLD, vous aurez peut-être un peu de la chance vous serez renvoyé au CCTLD qui n'a rien pour résoudre le problème mais qui peut vous écouter et reconnaitre qu'il s'agit d'un cas d'abus parce que la cour en elle-même, la loi des pays n'est pas faite pour s'occuper de ce type de cybercrime. Il n'y a pas de mécanisme, il n'y a pas d'interface que le registrant que l'utilisateur peut utiliser et peut aller voir dans ma suggestion pour ICANN et pour l'organisation et pour les acteurs c'est que nous devons

avoir un système, une manière de soutenir les meilleures pratiques. Les pays ont besoin de guides sur la façon de gérer ce type de problèmes, certains remettent entre les mains de la loi d'autre essayent d'organiser le marché, les différente institutions qui interviennent pour avoir des guides mais je dirais que si vous n'arrivez pas a résoudre cela, le registrant africain ou le serveur du registrant n'aura pas confiance dans le système et ne rentrera pas dans ce système. Et à la fin de la journée ne soyez pas surpris s'il y a un niveau d'introduction très bas dans le pays parce que les gens disent qu'est-ce qu'il va se passer si j'ai un problème avec mon vendeur, avec mon intégrateur, avec mon hôte web si on ne trouve pas de réponse à ces questions donc il dit je préfère être en face à face physique plutôt que de passer et de travailler au niveau virtuel.

>>: Merci, je pense qu'une partie de ma question ici a été déjà posée. Je vais reprendre un petit peu ce que miss Titi a dit. Il y a beaucoup de choses à faire, beaucoup de questions qui ont été posées. Maintenant vous devez prendre, vous fermez un site internet l'adresse est toujours là il change de nom il reviennent avec le même contenu avec le même concept et lorsqu'il s'agit de télécharger des choses le travail tout se passe de la même façon. Alors pourquoi vous ne pouvez pas aller à l'adresse IP et effacer le site, je veux dire l'effacer du web. Oui merci s'il vous plait répondez moi comme ca je pourrais répondre parce que je suis pas très technique et je viens d'Afrique et tous les délits viennent d'ici et donc qu'est-ce que vous pouvez faire pour que la législation la loi soit mieux adaptée à ce problème, voila ma question.

RAFIDAH MAT ISA: Merci je suis Rafidah je suis de la commission de communication de Malaysie. J'ai une question à vous poser, les outils que vous avez parce qu'actuellement notre commission a mis en place un blocage nous sommes plus concentrés sur le problème du fising je dirais quand même parce que nous n'avons pas de personnes qui trichent sur le site web. Nous avons des fournisseurs de service comme Google ou Yahoo quand on les contacte ils arrêtent le service, on le leur dit ils le font en

quelques minutes donc le problème que nous avons est que certains sites internet ne sont pas accueillis par ces compagnies. Des fois nous n'avons pas de réponse donc nous avons utilisé notre système nous bloquons le DNS donc si on utilise ce nouvel outil ce que vous proposez je vais l'essayer ca m'intéresse mais ce que je voulais savoir c'est quel est la rapidité du temps de réponse parce que actuellement nous avons 2 heures pour que le fournisseur de services bloque un site de fishing mais si les outils que vous proposez sont plus rapides ca m'intéresse merci.

NII QUAYNOR: Dernier commentaire.

HAMZA ABOULFETH: Oui je suis HAMZA ABOULFETH du maroc. Nous avons un web host et la question est directe je voudrais savoir en tant que compagnie marocaine quelles sont les lois que nous devrions appliquer et auxquelles nous devrions obéir. Ce sont les lois marocaines, les lois américaines, les lois canadiennes dans la mesure ou notre serveur est situé au canada et nous pouvons aussi servir en France donc est-ce que cela dépend de l'endroit où se trouve le serveur de l'endroit où nous nous trouvons? Est-ce qu'un jour un policier du Maroc peut venir et nous dire (et c'est arrivé hein) frapper à notre porte et nous demander des informations ou de retirer quelque chose de notre site internet ou des choses comme ca. Et je voudrais dire que je suis d'accord avec Mouhamet sur ce qu'il a dit concernant la possibilité d'être en Afrique et ces choses que nos usagers finaux connaissent. Le fait de pouvoir savoir qui contacter en cas de problème si vous achetez un site internet à un gars qui disparait ensuite du jour au lendemain et vous vous retrouvez avec rien sans nom de domaine sans site internet. Qui je vais pouvoir contacter pour m'aider dans un cas comme ca pour résoudre ce problème?

NII QUAYNOR: Merci beaucoup, nous avons plusieurs questions, un grand internet. Nous allons commencer par la droite, nous allons demander au panel de faire des commentaires et de s'assurer de répondre aux questions, Titi allez-y.

TITI AKINSAMNI: Je voudrais vraiment être rapide. Je suis allée sur la diffusion de notre session et je me suis rendu qu'un commentaire a été fait. Est-ce que nous avons indiqué que d'une certaine façon il y a des clichés qui ont été prononcés ici et j'allais répondre et c'est ce que doit être ma remarque finale. Nous ne devons pas nous éloigner des clichés et nous répétons les problèmes dans la mesure où ces problèmes n'ont pas été résolus et un exemple et une des questions qui est apparue ici pourquoi est-ce qu'on ne efface pas l'adresse IP? Pourquoi dans la mesure où les problèmes sont pas bien compris et où nous assumons que tout le monde le comprend nous n'allons pas avancer? Mon deuxième commentaire est que en matière de DNS fermés nous avons avancé oui, mais la proposition que nous avons devant nous, qu'est-ce que nous allons faire? Quand est-ce que nous allons au delà des blabla de ce type de panel et mettre en place des actions? J'ai présenté une série d'idées ce que nous devons faire doit être fait sinon nous allons continuer à nous demander qui c'est qui a raison l'utilisateur final, le fournisseur, etc. Merci.

DON BLUMENTHAL: Je voudrais répondre aux commentaires qui ont été faits dans cette salle. D'abord qu'est-ce qu'il faut dans quel domaine il faut être attentif. Si vous avez des serveurs au Canada vous devez faire attention aux lois Canadiennes et si vous êtes situé au Maroc vous devez vous occuper des lois marocaines. Les zones grises sont par exemple tout ce qui concerne les réglementations et là on a une série de problèmes qui apparaissent en ce qui concerne l'annulation d'une adresse IP c'est un problème grave mais notre directeur à partir du moment où nous pouvons annuler cette redirection IP je pense que il s'agissait ici d'une approche

basée sur l'IP. Ce n'est pas une boule de cristal, ce site peut être hébergé dans différents endroits et donc c'est très compliqué de le trouver pour une référence je dirais qu'on peut aller voir l'autre groupe de travail celui qui travaille sur le Fast Flux.

ROD RASMUSSEN: Je vais être très bref pour répondre à la question, le programme APWG est un programme important de suspension. Si on peut faire çà en 2 heures, gardez-le, c'est très bien. C'est le mieux qu'on puisse faire avec le projet de suspension de registre ca prendra probablement un jour avec de la chance donc c'est un projet de suspension. C'est beaucoup plus sérieux que de bloquer certaines portions d'internet et qu'on ne puisse pas voir certains contenus. Je crois que j'ai répondu a la question, merci.

NII QUAYNOR: Si vous n'avez pas de commentaire vous n'êtes pas obligés d'en faire un.

MICHAEL MORAN: Je suis d'accord avec ce qui vient d'être dit, je voudrais faire un commentaire concernant la capacité qui augmente ici pour les registrar. Nous faisons beaucoup de travail et d'efforts dans ce domaine en particulier du respect de la loi parce que le problème est global et nous avons besoin de travailler dans le plus grand nombre de pays possibles et assurez vous que ce travail réalisé c'est un processus lent qui doit se faire au niveau de la région, merci.

LANRE AJAYI: Je voudrais vous donner trois raisons principales. Il y a un problème, il faut le combattre. Deux nous avons fait une collaboration internationale qui a été confirmée dans ce panel, la collaboration a été la seule façon de résoudre ce problème avec différentes juridictions. Dans certaines juridictions on a seulement une collaboration et nous faisons cela de manière extensive et cela arrive mais nous avons aussi adopté le système de multi parties prenantes et l'engagement multi parties

prenantes puisque Mouhamet disait lorsqu'il parlait de personnes qui vont se réunir lutter contre le cybercrime et le cybrecrime diminue au Nigéria par conséquent. Merci.

PIERRE DANDJINOU: Merci, je pense que on a parlé de collaboration mais je voudrais aussi qu'on par le du développement de compétences. Lorsqu'il s'agit d'Afrique, je pense qu'il faut continuer à travailler dans ce domaine et je dirais aussi que les pays ont besoin d'avoir leur propre stratégie dans le domaine de la sécurité. Les gens des fois ne savent pas que faire et finalement les meilleures pratiques que nous devons copier en Afrique je crois que c'est quelque chose de très utile et le CERT Afrique et là pour cela.

NII QUAYNOR: Bien, je crois que vous avez fait du bon travail. Vous êtes restés avec nous ca a été une longue réunion, mais je pense que c'est une discussion approfondie je suis heureux que ça ait lieu sur le continent ici et je vous remercie pour votre participation. Merci.

[FIN]