KOBE – Session de travail des dirigeants d'At-Large : GCSC et le président du GNSO
Dimanche 10 mars 2019 – 15h15 à 16h45 JST
ICANN64 | Kobe, Japon

OLIVIER CREPIN-LEBLOND: … L'équipe d'At-Large. Et aujourd'hui nous avons le GSC, ses membres, qui sont venus se réunir avec nous et discuter du travail qu'ils ont fait dans le passé. Il s'agit de la commission mondiale de la stabilité et du cyber-espace. Nous avons un nouveau président, un nouveau co-président qui est ici.

Donc bienvenus à tous, c'est un plaisir pour nous de vous voir ici. Je voudrais remercier Wolfgang Kleinwaechter d'avoir proposé cette réunion avec ALAC. C'est la première fois que vous êtes dans ce cadre d'ICANN pour parler de votre travail. Donc nous sommes ravis. Je ne vais pas continuer à parler. Je vais donner la parole ici à ma voisine.

LATHA REDDY: Merci beaucoup Olivier.

OLIVIER CREPIN-LEBLOND: Latha va prendre la parole. Ha, on me demande ici de donner la parole aux organisateurs de la partie administrative. Gisella, du personnel de l'ICANN.

GISELLA GRUBER: Je vous rappelle que cette séance va être interprétée en espagnol et en français. Et lorsque vous allez recevoir des questions dans ces langues, vous pouvez utiliser vos écouteurs, et les interprètes traduiront. S'il vous plait donnez votre nom lorsque vous prenez la parole pour être identifié par les interprètes pour la transcription. Vous devez aussi parler à une vitesse raisonnable pour permettre aux interprètes de faire un bon travail. Merci.

OLIVIER CREPIN-LEBLOND: Merci Gisella, et je donne la parole à Latha.

LATHA REDDY: Merci beaucoup Gisella, merci Olivier de nous avoir invité à faire cette présentation. Je suis donc Latha Reddy, je suis la co-présidente de la Commission Mondiale sur la stabilité dans le cyber-espace.

Et notre mission est de développer des propositions pour les normes et les politiques pour améliorer la sécurité internationale et la stabilité internationale, et guider les États vers des comportements responsables, et les groupes qui n'appartiennent pas aux gouvernements aussi, vers des comportements responsables dans le cyber-espace. Il s'agit

d'une initiative conjointe du gouvernement des Pays-Bas, de La Haye. Et nous travaillons.

Nous sommes trois présidents : Marina, Michael et moi-même. Nous sommes présidents et co-président. Marina a été élue membre du parlement en Estonie, et donc elle a présenté sa démission comme présidente. Et donc Mickael et moi, nous sommes les présidents de cette commission.

Nous avons 25 membres dans cette commission. J'ai déjà parlé du secrétariat. Nous sommes un groupe multipartite. Nous avons des membres de la société civile, du secteur industriel, des personnes qui ont une expérience dans le domaine du gouvernement. Je suis diplomate à la retraite, Mickael est un ancien secrétaire des États-Unis de la sécurité. Nous avons un groupe consultatif de recherches. Nous avons un groupe de direction et nous sommes donc tout à fait démocratiques.

Je vais vous parler un petit peu de notre mission. Ce que nous voulons faire, c'est de formuler 8 normes dans l'espace public, et nous espérons que ces normes vont permettre aux leaders et aux responsables politiques du monde entier d'agir. Et nous contactons différentes organisations, les organisations des Nations Unies aussi. Marina est aussi membre du secrétariat des Nations Unies sur des problèmes numériques.

Et ce que nous allons faire - parce que les normes en elles-mêmes expliquent mieux que ce nous pouvons faire le type de recommandations que notre commission propose, et le rapport final, notre rapport final, quels sont les points sur lesquels le rapport final va se centrer. Tout cela vise à maintenir notre cyber-espace sûr, stable et qu'il puisse continuer à rester innovant.

Nous avons 8 normes. La première norme sera présentée par un de mes collègues de la commission. Elle vise à protéger l'activité publique principale de l'internet. Je vais demander à mes collègues de faire leur présentation. Ils ont deux minutes chacun pour la faire.

WOLFGANG KLEINWAECHTER: Merci. Lorsque nous avons commencé à discuter des normes, notre idée pour avoir une norme spéciale pour protéger l'activité principale et publique de l'internet nous a paru importante. Parce que tandis que d'un côté la stabilité de l'activité publique est garantie par ce système, tel qu'il est distribué, avec le service, l'accès au service, etc. il est difficile d'annuler l'internet, ce n'est pas possible, il y a beaucoup d'éléments qui existent au sein d'internet qui garantissent sa sécurité. Par ailleurs, comme on l'a vu ces dernières années, il y a des attaques constamment contre l'activité publique sur internet, il y a eu des piratages du DNS qui

risquent de mettre en danger la sécurité et la stabilité de l'internet comme nous le savons.

Donc jusqu'à maintenant, il y a des normes qui existent qui permettent aux acteurs gouvernementaux et non gouvernementaux de ne pas toucher d'activités publiques principales de l'internet, pour que celui-ci reste stable, et de travailler ensemble pour trouver les personnes malhonnêtes, les délinquants qui essayent de faire des choses malhonnêtes dans le domaine d'internet et des activités publiques sur internet.

Il y a des attaques contre l'activité publique sur internet qui appartiennent à des catégories de ce qu'on appelle cyber-délits, avec des systèmes juridiques. Il y a aussi des crimes qui seraient considérés comme des crimes contre l'humanité, parce que cette activité publique sur internet est tellement importante pour les activités humaines en général, cela doit correspondre à une catégorie spéciale.

Donc ici, notre compréhension de l'activité publique de l'internet est très proche de la mission d'ICANN. Parce que l'activité publique de l'internet avec le DNS, le système de nommage, le système de numéro, lorsque l'on a commencé à discuter pour savoir si nous avions quelque chose de commun avec ICANN, au niveau de notre commission mondiale, ICANN a découvert que

notre travail visait à protéger l'activité publique sur Internet et que c'était un élément clef.

Nous venons de différents points du monde, de différents secteurs. ICANN a plutôt une approche technique. Il y a des points communs, une intervention commune. Nous devons identifier les coopérations possibles dans le futur.

Nous avons une réunion avec le comité consultatif de sécurité et de stabilité aujourd'hui. Et je pense que c'est une très bonne chose d'avoir l'opinion de la communauté des utilisateurs pour savoir quelles sont les choses que l'on peut faire pour protéger l'activité publique sur internet.

LATHA REDDY: Merci Wolfgang. Je vais maintenant demander à Mariet Je Schaake de présenter la norme sur la partie de protection de l'infrastructure électorale.

MARIET JE SCHAAKE: Merci beaucoup. Je suis membre du parlement européen, je viens des Pays-Bas.

Ce que nous essayons de faire avec la norme sur laquelle nous travaillons est de l'inclure dans la juridiction criminelle. Nous

voulons construire un organe, un corps de principes juridiques de base.

Le premier point est la norme de non-interférence entre les nations. Cela appartient à la charte des Nations Unies, c'est un point clef. La Charte dit que tous les États membres ne peuvent pas utiliser des systèmes qui puissent aller contre l'équilibre des États.

Lorsque vous lisez la Déclaration universelle des droits de l'homme, vous constatez qu'il y a un droit à élire et que le gouvernement a le droit d'avoir des élections avec un vote secret.

Et il est clair que lorsque l'on regarde les processus électoraux, qu'ils soient faits avec des bulletins de vote ou de manière numérique, toutes les élections ont quand même une composante numérique et il y a beaucoup d'attention au niveau du débat public sur ces informations. Et nous nous focalisons sur la question de l'infrastructure technique.

Donc la norme que nous proposons est la suivante – vous pouvez la lire sur l'écran : « les acteurs gouvernementaux et non gouvernementaux ne peuvent pas rechercher, soutenir ou permettre des opérations cybernétiques visant à détruire les infrastructures techniques utilisées pour les élections, les référendums ou les plébiscites.

Voilà j'ai fini.

LATHA REDDY: Merci. Je pense qu'il faut aussi dire que lorsque l'on regarde ce type de problème, on regarde les infrastructures des élections, on ne regarde pas les non-informations ou le problème de contenu. Parce qu'on regarde surtout la façon dont l'infrastructure ou la stabilité de l'internet est affectée.

Au niveau de la norme, je vais demander à Bill Woodcock de la présenter. C'est une norme pour les acteurs gouvernementaux et non gouvernementaux pour éviter d'altérer des produits.

BILL WOODCOCK: Cela a été inspiré par l'attaque qui a eu lieue contre Cisco et contre les gouvernements qui visait à corrompre la chaine d'approvisionnement et d'essayer de s'introduire dans certains produits, dans le processus de la manufacture, de la fabrication. Par exemple, des compromis, des attaques contre des producteurs.

Donc nous recommandons de protéger l'ensemble des logiciels, parce qu'ils risquent, au niveau des producteurs, d'y avoir une grande portion de l'internet qui peut être ciblée et qui n'est pas protégée.

Par conséquent la norme ici est la suivante, elle est destinée à protéger les clients de la corruption des appareils et des logiciels qu'ils achètent par leur gouvernement et par les acteurs non gouvernementaux aussi. Voilà.

Donc comme vous pouvez le lire ici, les acteurs gouvernementaux et non gouvernementaux ne peuvent pas altérer des produits et des services en développement et production. Ils ne sont pas non plus autorisés à altérer et à faire des modifications substantielles dans le domaine de la stabilité du cyberespace.

Voilà, je vous rends la parole.

LATHA REDDY: Je vais passer à la prochaine norme, c'est la norme concernant les appareils et les systèmes de TIC pour les réseaux zombies.

OLAF KOLKMAN: Bonjour je travaille pour l'Internet Society. La norme précédente était sur les processus de production, cette norme porte sur les appareils qui sont ouverts, les appareils qui peuvent être utilisés de manière massive dans des attaques inspirées par l'attaque qui a eu lieu il y a quelques années, et le fait que nous avons un grand nombre d'appareils qui ne sont pas sécurisés dans différents domaines et qui peuvent être transformés en appareils dangereux et causer une certaine instabilité.

Ce n'est pas seulement cela. Si cela a lieu, les utilisateurs ou les propriétaires de ces appareils peuvent être compromis aussi, peuvent être considérés comme des personnes qui participent à des attaques. Et cela peut donner lieu à des condamnations, en tout cas parce qu'on considère que ces personnes ont participé à des opérations militaires.

Donc afin de capturer, d'introduire tout cela dans une norme, il a été dit que les acteurs gouvernementaux et non gouvernementaux ne peuvent pas réquisitionner des appareils.

Ce terme de réquisitionner veut dire qu'on ne peut pas utiliser ces appareils, et bien sûr les réseaux zombies et autres – parce que toutes les attaques ne sont pas instiguées par des réseaux zombies, il peut y avoir d'autres types d'attaques aussi, qui vont aussi capturer le DNS. Voilà.

LATHA REDDY: Merci Olaf. Nous allons maintenant donner la parole à prochaine personne qui va nous parler des normes pour que les États puissent créer un processus de principes de vulnérabilité.

CHRIS PAINTER: Ici, beaucoup de gens parlent de la possibilité pour les États d'avoir accès à des vulnérabilités qui sont connues au niveau public, et donc les conserver pour les forces de l'ordre pour des

objectifs de sécurité ou de les divulguer pour que les infrastructures soient plus sûres. Nous reconnaissons qu'il y a un défi ici important.

Certains pays ont commencé à créer une transparence procédurielle avec un cadre, avec toutes les parties prenantes en jeu, pas seulement les forces de l'ordre : les gouvernements, la partie économique et différentes organisations pour analyser ces points et pour prendre des décisions concernant la divulgation de ces problèmes.

Les États-Unis ont maintenant un processus de ce type, la Grande-Bretagne aussi, le Canada aussi le fait. Je crois que de plus en plus de pays le font. Nous ne suggérons pas que ce soit un système intégré au niveau mondial – en tout cas ça pourrait l'être dans le futur – mais je pense que plus les pays vont adopter ce type de mesures, plus nous serons sûrs par rapport à ce type de problèmes.

LATHA REDDY: Merci Chris. Nous allons passer à la prochaine norme qui vise à réduire et atténuer les vulnérabilités principales. Je vais donner la parole à Jeff Moss.

JEFF MOSS: Bonjour, merci de m'avoir invité.

C'est la première norme qui se focalise sur les producteurs, sur les fabricants, sur la société civile, sur les producteurs de technologie en général et non pas autant sur les gouvernements.

L'objectif ici est de devenir plus transparent et de reconnaitre la responsabilité que l'on a en tant que producteur, de façon à réduire les vulnérabilités qui peuvent avoir un impact sur internet.

Donc, je m'excuse, c'est une des normes les plus longues. Donc je vais juste la lire pour les personnes qui ne peuvent pas décoder.

Les développeurs et les producteurs de service doivent prioriser la sécurité et la stabilité, doivent prendre des mesures pour s'assurer que leurs produits et leurs services ne contiennent pas de vulnérabilité, prendre des mesures pour atténuer ces vulnérabilités qui seront découvertes et être transparents concernant leurs processus. Tous les acteurs ont le devoir de partager les informations sur la vulnérabilité et pour prévenir et atténuer les activités malhonnêtes dans le domaine du cyberespace.

Il y a un point ici qu'il faut souligner. Le premier est le fait qu'on reconnait ici que les vulnérabilités peuvent exister, on ne peut pas demander aux gens de créer des logiciels qui n'ont pas de vulnérabilité, on peut créer des processus pour réduire les erreurs, et les bugs. Parce qu'un bug, pour une personne, peut ne

pas être un problème, ou pour un producteur, mais ailleurs dans le monde, ce bug peut devenir très grave.

Donc comme on n'a pas une connaissance mondiale de la façon dont notre technologie peut être utilisée, il faut partir du principe que ce bug peut avoir un impact. Il faut être transparent lorsqu'on découvre ce bug et y remédier.

Cette norme est liée à la partie de l'altération, à la partie de l'hygiène aussi. C'est un petit peu au milieu et cela concerne la façon dont le secteur producteur et fabricant doit agir.

LATHA REDDY: Merci beaucoup Jeff. Nous allons passer à la norme suivante sur l'hygiène cybernétique comme défense des fondations. Je vais donner la parole à Abdul Hakeem Aijijola.

ABDUL HAKEEM AIJIJOLA: Oui, mesdames et messieurs, le succès de notre société numérique peut uniquement être atteint lorsque nous avons une plateforme cybernétique solide. Aujourd'hui les données sont à la base de ce pouvoir cybernétique pour notre survie.

Nous sommes très dépendants de la solidité de cela, et nous risquons donc de bâtir un avenir avec des capacités qui ne sont

pas exactement au niveau, notamment au niveau de leur protection.

Nous devons avoir des défenses [au niveau des fondations] fortes. Donc les normes GCSC défendent ceci et nous avons besoin de mesures au niveau des lois, au niveau des règlementations, pour nous assurer d'une excellente hygiène. Cela nous permettra d'obtenir une base pour l'adoption et la mise en place de mesures qui représentent des priorités au niveau des taches de défenses pour limiter les différents dangers du cyber-espace.

Nous pensons que cette norme sera tout à fait intéressante, ce standard, par rapport aux bureaux d'enregistrements et aux registres.

Et mesdames et messieurs, je crois que ce régime d'hygiène doit être mis en place avec des informations techniques qui seront partagées. Il doit être sujet également à un contrôle. Par exemple, il y a des aspects de pollution sur les différents courants de l'internet, avec les téléphones intelligents par exemple.

Nous créons donc plus de responsabilités et les gouvernements ne doivent pas limiter l'innovation au niveau de l'évolution de l'internet, au niveau des meilleures pratiques qui existent déjà, pour une excellente hygiène cyber-informatique.

Au niveau international, ces normes sont déjà respectées, mais nous avons besoin de plus d'étapes pour s'assurer que les dangers soient limités.

Cela peut représenter un obstacle, en raison de l'accès des utilisateurs aux différentes données.

Comme Bill Clinton l'a dit, si on pouvait tuer le sida avec de l'eau pure, et bien cela ne suffirait pas. Il faut aider chacun à combattre les fléaux.

Au Nigéria, nous avons plus de 108 millions d'habitants en ligne. Et en Inde encore plus. Mais, hélas, aujourd'hui, comme l'a dit Bill Clinton, dans le monde en développement, nous avons besoin d'avoir ces normes d'hygiène cybernétique qui vont s'appliquer au monde émergeant, aux nouvelles technologies, et aux personnes qui sont responsables de l'impact de ces technologies.

Les avancées du bien-être de l'humanité sont nécessaires si nos ressources digitales sont protégées. Il est donc essentiel mesdames et messieurs que les États aient des mesures et des règlementations pour s'assurer de cette hygiène de base pour l'internet.

LATHA REDDY: Merci beaucoup Abdul. Nous aimerions maintenant donner, pour ces normes sur les opérations par des acteurs n'étant pas des acteurs d'Etat. Frédéric Douzet vous avez la parole.

FREDERICK DOUZET: Oui, donc ça c'est une norme qui nous indique qu'il ne peut pas y avoir d'opération par des acteurs n'étant pas des États, des opérations malfaisantes.

La raison pour laquelle nous avons cette norme, ce standard, c'est parce que nous avons des entreprises privées qui essayent d'avoir des attaques cybernétiques au-delà des frontières. Et nous devons limiter cela, nous devons nous défendre par rapport à cela.

Il y a des États qui ne peuvent pas se protéger contre des attaques cybernétiques et des attaques de ce type qui peuvent être néfastes, très actives. Il y a des formes très violentes au niveau de certaines de ces attaques, que nous devons contrôler avec des pratiques.

Parfois on ignore trop ces attaques, ces cyber-attaques qui ne sont pas véritablement autorisées, qui ne sont pas véritablement analysées.

Il y a d'autres opérations offensives par des acteurs, des entreprises privées par exemple.

Et nous pensons en tant que GCSC que cette sécurité et cette stabilité du cyber-espace est absolument essentielle et qu'il peut y avoir des dégâts très forts en cas d'attaques de ce type. Ce peut être des conflits très forts au niveau juridique, au niveau des lois internationales, au niveau des principes qui existent. Il y a la souveraineté des États qui est en jeu, les droits également qui sont en jeu, les monopoles, l'utilisation de la force, les lois internationales qui sont en vigueur.

Et une des responsabilités des États c'est le principe de diligences appropriées pour l'utilisation d'actes contre l'utilisation d'attaques de ce type.

LATHA REDDY: Donc vous avez entendu nos 8 standards ou normes qui ont été présentés. Avant de conclure notre présentation, j'aimerais donner la parole à Michkael Chertoff qui va nous parler de la définition et des principes que nous suivons à la GCSC en ce qui concerne la cyber-stabilité. C'est cela qui compte. Nous sommes une commission mondiale sur la stabilité dans le cyber-espace. C'est absolument essentiel, c'est notre mission. Et Mickael Chertoff va nous donner son point de vu à ce sujet.

MICHAEL CHERTOFF: Oui, merci beaucoup. Les définitions actuelles ressemblent à cela.

La stabilité dans le cyber espace, c'est une condition où les acteurs étatiques ou non sont en confiance par rapport à leur capacité d'utiliser le cyber espace de manière sûre, où la disponibilité, l'intégrité des services est, en général, assurée.

Nous ne sommes pas ici pour dire : ne faites rien de mal sur l'internet, mais c'est une perception de stabilité qui existe.

Parfois, il y a des personnes qui n'ont pas confiance en la stabilité de l'internet, qui ont l'impression que l'internet est instable et n'est pas sûr.

Deuxièmement, nous parlons de menaces à la stabilité. Nous ne sommes pas naïfs, nous comprenons par exemple qu'il y a des raisons légitimes pour des États-Nations de cibler très précisément une partie de l'internet. Ça, ce n'est pas un problème pour la stabilité de l'internet.

Mais ce que nous avons noté, c'est qu'il y a des activités qui pourraient poser des problèmes à la stabilité de l'internet. Au niveau des protocoles, au niveau de l'infrastructure ou bien au niveau des points finaux. Si cela est compromis, et bien en réalité la stabilité de l'internet est attaquée.

Donc notre espoir c'est que ces normes seront prises en compte par les gouvernements et par le secteur privé pour créer un environnement où l'internet fonctionnera bien à l'avenir.

LATHA REDDY: Merci beaucoup Mickael. Je vais donner la parole à Olivier Crepin-Leblond, si vous voulez gérer un petit peu les différentes questions qui seront posées.

OLIVIER CREPIN-LEBLOND: Merci Latha. Nous avons des questions pour les personnes. Vous connaissez la procédure.

Nous avons je crois des micros qui sont également dans la salle pour les commentaires. Donc levez la main et Gisella vous apportera un micro pour vous exprimer et qu'on vous entende.

Je vais commencer… J'ai vu Hadia qui sera la première personne à prendre la parole et ensuite nous poursuivrons, nous alternerons avec des personnes se trouvant dans la salle.

HADIA ELMINIAWI: Mon commentaire serait par rapport à - je ne sais plus les numéros de standards - mais en ce qui concerne les produits manufacturés qui peuvent être altérés et aux différentes

législations qui arrivent, ou pour les entreprises on leur demande d'avoir des données cryptées.

Cela force des entreprises à avoir des portes d'entrée possibles par rapport à leur cryptographie. Donc ce n'est pas à un État ou un non-État qui effectuerait des attaques par certains points d'entrée, mais il y aurait une possibilité d'altérer, si vous voulez, ces produits. C'est un choix de ces fabricants.

Donc comment est-ce que votre standard répond à ce critère ?

JEFF MOSS: Deux observations d'ordre général. Je crois qu'on a passé pas mal de temps à parler de cryptographie par exemple. Il y a des entreprises et des gouvernements. Les entreprises veulent gagner de l'argent. Apple par exemple gère ce problème. Ils ne veulent pas avoir trop de juristes pour répondre à toutes ces questions.

Il y a donc des fabricants qui ont des produits, qu'ils mettent sur le marché, et qui répondent déjà à ces scénarios.

Il y a des personnes qui collectent des données, et ne collectez des données si vous ne pouvez pas protéger les données. C'est une question de transparence. Si vous êtes forcés de mettre ces portes d'entrées ou de sortie, maintenant tout le monde est au

courant de cela. Les consommateurs vont bouder certaines de ces entreprises qui vendent des produits qui ne sont pas sûrs.

Donc je ne crois pas que les gouvernements vont beaucoup se pencher là-dessus. Les entreprises doivent être compétitives, si elles ne le sont pas elles perdront des clients.

Donc je crois que nous sommes bien conscients du fait que la communauté internationale ne pousse pas beaucoup à ces concepts.

BILL WOODCOCK: Oui, je crois que… Oui, c'est bien résumé. Je crois que le problème que vous décrivez… On comprend l'approche des gouvernements qui requièrent cela des fabricants et des entreprises, mais cela est en contradiction avec l'esprit des normes au niveau de la vulnérabilité.

On n'essaye pas décrire toutes les violations possibles qui pourraient exister, c'est très large, c'est conceptuel si vous voulez comme norme. Et je crois que cela peut répondre à ces différents types d'attaque au niveau de la chaine d'approvisionnement et de la vulnérabilité de certains produits.

OLIVIER CREPIN-LEBLOND: Merci beaucoup Bill Woodcock qui vient de s'exprimer. Il faut indiquer vos noms, parce que nous avons des interprètes aussi.

Nous avons une question je crois dans la salle. Nous allons donner le micro à Ricardo Holmquist.

RICARDO HOLMQUIST: Je vais m'exprimer en espagnol si cela ne vous dérange pas. On va faire travailler nos interprètes.

Bon après-midi à toutes et à tous. Ces normes semblent très solides, mais il y a plusieurs acteurs qui sont ici, nous avons de grosses entreprises, nous avons des normes qui sont à l'écran, nous avons des gouvernements. Mais dans certains cas, en ce qui concerne les applications, c'est de petites entreprises.

Donc comment allez-vous, avec votre commission, mettre cela en place, au niveau des gouvernements, au niveau des entreprises, au niveau de la convention de Budapest sur la cyber-sécurité ? Comment allez-vous envisager les prochaines étapes ? Les normes sont solides, quelles seront les prochaines étapes. Comment allez-vous faire respecter ces normes ?

CHRISTOPHER PAINTER: C'est exactement ce sur quoi la Commission travaille. Nous avons un ensemble de normes qui viennent renforcer des normes onusiennes déjà, qui existent au niveau de la responsabilité.

Et c'est difficile de faire respecter les normes, nous le savons. Ça ne suffit pas d'avoir des normes, si personne ne les respecte, ça ne sert à rien. Ça reste des feuilles de papier.

Donc on essaye de responsabiliser les différents acteurs par rapport à ces normes.

FREDERICK DOUZER: Si vous regardez au niveau de l'accord de Paris, il y a des normes qui sont déjà respectées. Il y a une soixantaine d'États qui ont soutenu cet accord. Il y a des entreprises privées… Je crois que nous avons déjà pas mal de forces pour faire respecter ces normes.

MARIA JE SCHAAKE: Je crois que la raison pour laquelle nous sommes ici, nous sommes très heureux d'être ici. Parce que vous en tant que société civile, en tant que partie prenante, vous croyez en l'utilité de ces normes et vous allez pouvoir convaincre les gouvernements, le secteur privé, les entreprises, de commencer à accepter ces normes et à limiter les différentes violations.

Donc ce n'est pas un processus de monopole. Nous venons de différentes parties du monde, différents niveaux d'expertises et d'entité et nous avons essayé de réfléchir à ce qui serait véritablement utile pour la stabilité du cyber espace, pour que dans le monde entier on fasse plus et de plus en plus confiance au cyber espace.

OLAF KOLKMAN: On ne peut pas travailler seul. On a besoin des États, des entreprises et de tous les autres acteurs. C'est un appel que nous lançons en effet.

ABDUL-HAKEEM AJIJOLA: Pour les chrétiens, il y a les dix commandements, on ne va commettre l'adultère par exemple, vous n'avez qu'une seule femme. Moi je suis musulman, moi je peux vous dire qu'on ne doit pas commettre l'adultère non plus, mais je peux avoir 4 femmes. Donc que ce soit une petite entreprise ou une grande entreprise, les normes s'appliquent de la même manière.

OLIVIER CREPIN-LEBLOND: Et bien c'était une très intéressante analogie. Nous avons John.

JOHN LAPRISE: Je voudrais demander au comité pourquoi nous n'avons pas une infrastructure technique. Et sachant cela, je mettrais ma casquette académicienne, il y a 40 ans, aux États-Unis, pendant la guerre froide, le Comité National de Télécommunication disait que le système de télécommunication devait faire l'objet d'un contrôle et, par conséquent l'internet n'est pas tout à fait différent je dirais dans ce sens.

La question est la suivante : l'internet dépend du système électrique. Comment le protéger ?

CHRIS PAINTER: Je dirais qu'à ce propos il y a des normes, il y a un groupe d'experts des Nations Unies qui travaille sur ces points. Et je pense, nous discutons de ces normes, nous sommes en train d'en parler aussi, qu'il faille sécuriser le réseau électrique.

Et il nous faut voir quelles sont les infrastructures critiques. Certaines personnes peuvent dire qu'il s'agit d'infrastructures critiques, d'autres que non. Donc il y a un certain débat ici dans ce sens. Nous pensons que les infrastructures qui sont en danger sont nombreuses et qu'il faut les protéger bien sûr.

Cela ne veut pas dire que nous ne nous intéressons pas à ces infrastructures, mais il faut sélectionner les infrastructures.

BILL WOODCOCK: En 2017, nous avons fait une enquête concernant les infrastructures qui devaient être protégées.

Nous l'avons présenté, nous avons choisi 4 de ces infrastructures : la cryptographie, le nommage et le numéro et la partie électrique. Donc entre autres choses, qu'il fallait protéger ceci.

MICHAEL CHERTOFF: Je dirais que nous essayons de nous focaliser sur les choses qui représentent des problèmes uniques au niveau des opérations. Donc protéger des infrastructures qui sont en danger, alors qu'on a des règles qui existent déjà. Je le sais parce que je travaille dans ce domaine.

Donc nous devons nous focaliser sur de choses qui ne sont pas couvertes par contre.

OLIVIER CREPIN-LEBLOND: Je vais vous demander d'être brefs, parce que nous avons 7 ou 8 personnes ici qui veulent poser des questions.

OLAF KOLKMAN: Oui, je pense que c'est important de parler des différentes structures. Ce n'est pas seulement les infrastructures physiques c'est aussi la parie logique, les tables de routage, les normes en

général. Donc, la partie logique, c'est tout à fait nouveau, il faut réfléchir à la façon dont les structures, ces structures que nous voulons protéger, ces structures intangibles parfois.

ABDULKARIM OLOYEDE: Merci beaucoup. Je souhaite ici faire un commentaire concernant ces normes. Il y a quelque chose qui me parait important et que vous n'incluez pas dans ces normes et je voudrais savoir pourquoi vous ne l'incluez pas. C'est la question de la protection de la vie privée. Est-ce qu'il y a une raison pour laquelle vous avez laissé cela à l'extérieur de ces normes ?

[LATHA REDDY]: Je voulais juste vous dire que si vous regardez notre mission, c'est de conserver le cyber espace stable. Et les données de protection de la vie privée, c'est un problème très ample et qui n'affecte pas vraiment la façon dont internet fonctionne.

Donc, de ce point de vue, je pense que ce n'est pas ici… C'est un problème important bien sûr qui peut affecter la façon dont nous considérons internet et le cyber espace, mais je pense que cela n'a pas un impact sur la stabilité du cyber espace.

C'est une question différente. C'est de toute façon une question importante.

OLIVIER CREPIN-LEBLOND: Wolfgang, vous avez la parole.

WOLFGAND KLEINWAECHTER: Nous avons eu une discussion aujourd'hui concernant les droits de l'homme. Les droits de l'homme ont un impact sur la stabilité du cyber espace, les violations massives des droits de l'homme peuvent avoir un effet négatif sur la stabilité du cyber espace. Nous n'avons pas encore éclairci ce point-là, pour savoir comment ce point peut être traduit dans une manière concrète. Mais nous savons que cela peut affecter la stabilité du cyber espace.

OLIVIER CREPIN-LEBLOND: Seun Ojedeji, vous avez la parole.

SEUN OJEDEJI: Merci beaucoup.

Je parle en tant qu'ingénieur, puisque nous sommes ici devant un public de personnes techniques. Je voudrais savoir pourquoi les actions qui visent l'infrastructure de l'internet, pourquoi est-ce que ces actions ne sont pas reflétées dans la liste si, d'une certaine façon cela est inclus dans ces normes.

Ensuite, deuxième point, je pense que c'est une bonne chose qu'il y ait une manière de voir les effets de ces normes. Par conséquent, si vous pouviez considérer une façon de faire un suivi des effets exacts que cela peut avoir quelque part.

OLIVIER CREPIN-LEBLOND: Est-ce qu'il y a quelqu'un qui veut prendre la parole pour répondre ?

JESS MOSS: Je pensé que nous sommes tous d'accords. Si j'ai bien compris, vous parlez des gouvernements ou des pays qui, d'une certaine façon, attaquent les infrastructures de routage. Et la discussion concernant la manière d'appliquer ces normes.

Certaines peuvent… Il y a un observatoire de l'internet qui peut entrer en jeu, observatoire de normes, quels sont les pays ou compagnies qui ont ratifié ces principes. Quelles compagnies violent, ou quels pays violent ces principes.

Parce que je pense que la première chose à propos de ces normes c'est identifier les bons acteurs et les mauvais acteurs dans ce sens.

Donc nous essayons de mettre en place un partenariat ou trouver des partenaires appropriés pour créer un système d'observation qui soit opérationnel dans ce sens.

BILL WOODCOCK: Oui, je pense qu'il y a deux axes ici, deux approches. La première est le fait qu'un pays ou une organisation a exprimé la possibilité d'adopter une norme, et l'autre approche serait la conformité. Par conséquent, je pense que l'on peut faire un suivi de ces deux choses.

C'est facile de dire qui a dit que cette norme représente une de leurs conduites, qui correspond. La plupart des pays de l'Union Européenne ou les États-Unis…

Donc nous devons analyser la façon dont les pays font certaines choses qui violent ces normes, parce que quelqu'un peut avoir dit qu'il soutenait cette norme, mais les militaires ou les services secrets peuvent avoir violé ces normes.

OLIVIER CREPIN-LEBLOND: Merci Bill. Je crois qu'il nous reste encore 4 personnes donc il faudrait être un peu plus bref. Eliot Noss, vous avez la parole.

ELIOT NOSS: Je voudrais vous féliciter tous pour ce travail que vous avez réalisé.

Je dirais que j'espérais qu'il y ait un processus multipartite sur la cybersécurité, et je trouve que c'est un petit peu la genèse dans ce domaine de cette organisation. Donc je vous encourage à faire une série de choses.

D'abord assurez-vous que vous restez séparé de ce processus. Et quand je dis cela, je veux dire que ICANN a une responsabilité particulière. Vous avez la vôtre et je pense que les deux sont importantes, doivent être séparées et le multipartisme va augmenter si on respecte cela.

Ensuite, pour tirer profit de ce travail, je pense que vous pouvez le faire de manière différente, en venant à nos réunions, de manière régulière. Un bénéfice que vous pourriez obtenir de votre présence ici à ces réunions, c'est qu'il y a une présence importante des forces de l'ordre ici du monde entier. Et c'est un groupe qui, en fonction de votre diagramme, ne participe pas à votre processus multipartite.

Et je pense que pour que vous puissiez mettre en œuvre un effet réel et pour que votre responsabilité augmente dans le temps, vous devriez travailler avec les forces de l'ordre qui seraient comme une partie nécessaire.

Les forces de l'ordre peuvent être, pour vous, en termes de cyber sécurité, ce que le GAC a été pour la communauté ICANN. Au début, ils ont commencé à se réunir dans des salles privées, et petit à petit, ils se sont intégrés à notre organisation.

C'est un processus qui peut prendre du temps. Et je vous encourage à tirer le plus grand profit possible de ce processus. Et maintenant, je dois partir.

[LATHA REDDY]: Je voulais juste vous dire que nous vous remercions. Et nos membres ont eu des interactions avec les membres d'ICANN, et je pense que nous savons ce que fait ICANN. Et nous avons la possibilité de tirer profit de cette coopération et de cette connaissance du processus d'ICANN.

Olaf vous voulez ajouter quelque chose ?

OLAF KOLKMAN: Oui, un de nos membres, de notre commission, est un leader à Interpol et donc nous avons bien compris cela au sein de notre commission.

Au niveau de l'approche multipartite, nous savons qu'il y a différentes approches. Il est clair qu'il s'agit d'une communauté qui a des responsabilités très spécifiques. Mais nous pensons que

l'activité publique sur internet nous oblige à nous occuper de cela.

Alors la Commission s'est rendu à différents endroits où les unités constitutives qui n'incluaient pas obligatoirement les forces de l'ordre, mais qui incluaient par exemple l'aspect plus militaire de la cyber-stabilité, ou l'aspect plus politique de la cyber-stabilité. S'il vous plait, faites un suivi de nos normes.

Dans ma propre communauté, nous essayons de travailler là-dessus. Le problème c'est que nous avons un mandat pour une année de plus, et pour nous participer davantage au processus de l'ICANN va être un défi.

OLIVIER CREPIN-LEBLOND: Je vous propose de prendre les dernières questions et ensuite on fera une réponse générale.

Jonathan Zuck, allez-y.

JONATHAN ZUCK: Vous parliez d'interagir avec les forces de l'ordre, et ça m'intéresse.

Mais je suis heureux que vous parliez aussi de certaines choses, parce que les normes pour moi me paraissent importantes. Et vous nous avez parlé de cela.

Et des fois on a l'impression que ces normes peuvent devenir des choses difficiles à appliquer. Je parlerais par exemple de moments dans l'histoire où on a des exemples où il y avait une pression publique dans ce sens… Mais en tout cas je pense qu'il faut essayer de faire appliquer ces normes par des organisations.

Et les organisations comme l'OMC, par exemple, c'est une organisation qui peut appliquer ce type de choses et les rendre obligatoires. Des organisations de ce type qui ont déjà des infrastructures pour l'application, le contrôle, des organisations qui sont responsables dans ce domaine pourraient être des acteurs importants.

OLIVIER CREPIN-LEBLOND: Merci Jonathan. La personne à côté de Nigel, allez-y.

[NANO DORWICH]: Bonjour, je viens de Serbie. Je voudrais poser ma question à Frédéric Douzet. Il me semble que ICANN a participé à au moins, et Microsoft à plusieurs opérations pour identifier un grand nombre de domaines qui étaient utilisés par des réseaux zombie ou par des systèmes de cyber-virus et d'extorsion à travers les cyber-virus. Leur inclusion dans ces opérations allait à l'encontre des normes que vous avez présentées il me semble.

OLIVIER CREPIN-LEBLOND: Merci. Nous allons donner à Frédéric la possibilité de réfléchir un petit peu avant de donner sa réponse. Holly Raiche, pendant ce temps, vous avez la parole.

HOLLY RAICHE: Holly Raiche, d'Australie. Je voudrais vous demander ce que vous faites en ce qui concerne la loi d'accès de 2019. Est-ce que vous avez fait des soumissions ou des déclarations ?

OLIVIER CREPIN-LEBLOND: Merci Holly, en Australie donc. Ok. Nous allons maintenant donner la parole à Frédéric Douzet.

FREDERICK DOUZET: Oui, merci. Donc pour répondre à la première question, je pense que je ne peux pas, au niveau des noms, nous ne voulons pas rentrer dans ce domaine parce que c'est très politique.

L'objectif du contrôle des normes et de la violation des normes vise plutôt à comprendre la façon dont on peut progresser au niveau de la cyber-stabilité et cela permet aussi d'avoir une analyse légale concernant les affaires précédentes de façon à construire un système qui nous permette de mieux comprendre notre système juridique au niveau international de façon à pouvoir répondre à ces problèmes.

Au niveau des réseaux zombie et ce qui a été dit, je dirais de nouveau que notre objectif est dépend de la façon dont les États demandent que cela soit fait par les fabricants, que les fabricants respectent cela ou le font de leur propre grès. Donc les gouvernements peuvent demander que ce soit fait parce qu'il y a un besoin. Ensuite, les agents de l'État et la loi internationale peut considérer cela comme des choses obligatoires aussi.

OLIVIER CREPIN-LEBLOND: Mickael Chertoff ?

MICKAEL CHERTOFF: Par rapport à la troisième question, à propos de l'Australie et des lois [concernant] le chiffrement, on n'est pas encore au point où l'on va faire une déclaration parce que nous n'avons pas encore fini de voter sur cette norme.

Mais je pense que nous pouvons donner un argument important, et c'est que cette norme sur la vulnérabilité comprend ce problème. Je pense que cela va durer un certain temps, cela va prendre un certain temps.

Nous aurons la possibilité de participer ici, et nous espérons pouvoir le faire une fois que notre rapport final sera terminé pour pouvoir travailler au niveau de la protection, d'une plaidoirie,

parce que la législation fait des choses que nous considérons comme incompatibles avec ces normes.

OLIVIER CREPIN-LEBLOND: Merci Mickael. Chris Painter.

CHRIS PAINTER: Merci. Je voulais ajouter quelque chose à ce que Frédéric a dit. Je dirais, par rapport à ce que Microsoft fait, il présente cela devant les tribunaux, il travaille avec les gouvernements, donc je ne pense pas que cela peut être interdit par nos normes ou que cela puisse aller à l'encontre de nos normes.

Il y a certaines choses, on doit considérer la violation et la commission peut faire cela, mais il vous faut voir aussi comment on peut mieux appliquer les normes et quelles sont les attentes dans ce sens. Parce que je pense que la tendance que l'on a, et on peut constater que les choses vont s'empirer, même si nous avons des bonnes normes, nous devons continuer quand même à être attentif dans ce domaine.

OLIVIER CREPIN-LEBLOND: Merci beaucoup Chris. Est-ce qu'il y a d'autres commentaires ?

MARIT JE SHAAKE: Je voudrais brièvement reprendre un petit peu ce que vous avez dit concernant les institutions qui existent au niveau de l'application des lois par les États lorsque cela existe. Nous n'avons pas encore travaillé complètement dans ce domaine, et la question qui a été posée sur les attributions, la responsabilité. De toute façon ce que vous dites c'est tout à fait la ligne dans laquelle nous travaillons.

On peut aussi voir ici, dans ma réponse, que nous n'avons pas fini notre travail. C'est quelque chose qui peut être approfondi. Et nous travaillons pour consulter les personnes qui pourraient nous donner et nous aider à approfondir ces normes et leur mise en œuvre.

OLIVIER CREPIN-LEBLOND: On me dit que la prochaine personne qui doit intervenir n'est pas arrivée, donc on a encore quelques minutes à notre disposition.

Mais vous devez partir peut-être. Vous avez un autre rendez-vous. Donc Wolgang vient de se lever. Donc nous avons une personne qui veut poser une question.

[DIEGO CANABARRO] : Je suis du Brésil. Moi, je me posais une question, un point d'information que je voulais obtenir. Vous avez parlé des

différentes couches logiques du cyber espace, et je voulais en savoir plus sur votre conception de cela.

Au niveau de l'espace public, qu'est-ce qui est privé, qu'est-ce qui est public au niveau de l'espace ? Et ça c'est une question de gouvernance de l'internet.

Il semble que tout ce que vous avez dit, ça fait partie de l'espace public, du cœur public de l'internet. Vous avez parlé également d'acteurs privés. Donc les câbles, l'infrastructure du routage, cette infrastructure qui dans 80 % des cas appartient au secteur privé, est-ce que c'est important ou pas, est-ce qu'il va y avoir un impact si on promeut cela.

OLIVIER CREPIN-LEBLOND: Merci de répondre à cette question. Latha ?

LATHA REDDY: Et bien oui, en effet, nous avons une explication en effet pour le cœur public. Ça c'est la technologie de l'internet mondial. Cette technologie est imparfaite. Pour nous, c'est une infrastructure essentielle, mais la technologie peut avoir des problèmes, a des vulnérabilités, il y a des acteurs malveillants, il y a parfois un aspect offensif, des attaques qui existent, qui créent de l'instabilité dans le cyber espace. Et cela est tout à fait néfaste.

Et nous avons essayé de souligner les éléments techniques qui, d'après nous, sont absolument essentiels pour le cœur même de l'internet et qui remettraient en cause le bon fonctionnement de l'internet.

Je crois que nous réfléchissons à tout ce qui ne permettrait plus à l'internet de fonctionner tel qu'il devrait fonctionner. Donc au niveau des attaques. Et ça, c'est pour des acteurs étatiques et non étatiques.

OLIVIER CREPIN-LEBLOND: Merci beaucoup de cette réponse. Oui, Anriette, je vois que vous voulez prendre la parole, vous faites partie de la commission.

ANRIETTE ESTERHUYSEN: Merci beaucoup Olivier, je voudrais rebondir sur ce qui a été dit, c'est une question fondamentale qui a été posée.

La norme sur le cœur même de l'internet est gérée – ce n'est pas un problème que ce soit une entité privée ou pas qui le gère – il faut que ce soit géré dans l'intérêt public, comme l'ICANN, l'intérêt du public dans le cadre de la résilience de l'internet et de la bonne opérabilité de l'internet.

Donc, il n'est pas nécessaire de le promouvoir, mais c'est déjà public. Vous voyez ? Et ça n'appartient à personne.

OLIVIER CREPIN-LEBLOND: Chris Painter ?

CHRIS PAINTER: On a beaucoup réfléchi à ces normes, parce que l'on comprend bien que ce dont on parle ici, ce ne sont pas des petits problèmes pour l'internet, c'est quelque chose qui pourrait faire s'effondrer l'internet si des acteurs gouvernementaux ou pas pourrait avoir un effet extrêmement néfaste sur l'internet.

C'est clair, les petits problèmes qui se posent au quotidien, ce n'est pas ça notre priorité. Nous ce serait quelqu'un ou quelque chose qui aurait un impact destructeur sur l'internet qui nous préoccupe.

OLIVIER CREPIN-LEBLOND: Merci beaucoup Chris. Et bien s'il y a d'autres questions sur ces thèmes, vous pouvez les envoyer au personnel de At-Large, à ICANN.ORG et on vous transmettra les questions. Merci beaucoup d'être venus nous rendre visite et d'avoir présenté. Ce fut un véritable plaisir de vous écouter.

LATHA REDDY: Et bien au nom de la Commission au global, j'aimerais vous remercier du temps que vous nous avez proposé. Ce fut un plaisir

de parler avec ICANN, avec l'At-Large aujourd'hui avec notre commission consultative. Merci beaucoup Olivier de nous avoir donné cette possibilité de nous exprimer.

OLIVIER CREPIN-LEBLOND: Nous aurons ensuite Keith Drazek qui viendra nous rejoindre dans la salle, et Cheryl Langdon-Orr également va venir nous parler. Donc ne quittez pas la salle, nous continuons notre travail.

NON IDENTIFIE: Mesdames et messieurs, nous allons commencer bientôt notre prochaine séance.

Les liaisons et membres régionaux, venez nous rejoindre autour de la table pour que nous puissions commencer notre travail.

CHERYL LANGDON-ORR: Mesdames et messieurs, s'il vous plait veuillez reprendre place pour que nous puissions recommencer notre travail.

Les leaders régionaux de l'At-Large, venez vous assoir autour de la table, nous aimons vous voir plutôt que vous soyez dans notre dos. N'hésitez pas à prendre place autour de la table si vous le désirez.

Donc peut-être qu'en parlant moins fort ça marchera mieux… Cheryl Langdon-Orr au micro…

J'ai l'honneur et le privilège, mon nom n'est pas devant moi, mais je suis liaison au conseil de la GNSO. Et Keith Drazek est président entrant du conseil de la GNSO.

Pourquoi est-ce que nous nous rencontrons aujourd'hui ? Donc peut-être pour ne pas lui permettre d'avoir une pause café, mais plus sérieusement, on doit parler de choses importantes. Parce qu'au niveau de la communauté At-Large, à la suite de notre révision, de la révision de l'organisation At-Large, nous devons être plus engagés dans les politiques nous a-t-on dit, et avons-nous décidé.

Et, au même moment, nous aimerions en savoir plus sur la GNSO, comment fonctionne la GNSO, qu'en est-il au niveau de la GNSO actuellement, quel est le rapport avec At-Large, comment vous envisagez cela, structure et fonction de l'organisation de la GNSO.

Et Keith, je sais que vous avez un document préliminaire au niveau du PDP, mais nous demandons aux personnes de se joindre au développement des politiques. Donc j'aimerais en savoir plus Keith sur tous ces points.

KEITH DRAZEK: Et bien merci beaucoup Cheryl, merci de m'avoir invité. Je suis donc le président entrant du conseil de la GNSO pour le PDP,

responsable du développement de politique pour les gTLD. Voilà ce que fait le conseil de la GNSO. Et je serais très heureux de vous parler un petit peu de la structure de la GNSO brièvement, de vous parler également de l'évolution du conseil, de l'engagement, du processus de développement des politiques, PDP.

Mais permettez-moi de vous dire que nous sommes très heureux d'avoir des membres de l'ALAC qui participent aux processus de la GNSO. Et, exemple récent, par exemple, la piste de travail numéro 5, vous êtes co-présidente de ce PDP – merci beaucoup de cet effort et de ce sacrifice – l'EPDP pour les spécifications temporaires qui remplaceront les spécifications temporaires, Alan et Hadia ont beaucoup travaillé à cela. C'est un sacrifice véritablement en temps. C'est si intense ce processus. C'est un travail herculéen véritablement, avec un calendrier très serré pour trouver ce qui suivra les spécifications temporaires.

Nous avons plusieurs phases, la GNSO en tant que responsable du processus, nous lançons la phase 2, avec une envergure qui va être définie. C'est urgent, c'est un travail urgent, nous devons avancer et divulguer tous ces points pour un nouveau modèle d'accès uniforme aux données.

Donc pour la GNSO, nous avons une charte. Une charte qui répond à nos objectifs. Nous voulons soutenir le groupe de travail

EPDP pour développer un plan de travail et établir des attentes. Le conseil de la GNSO va fournir au groupe de travail EPDP de plus en plus de conseils, mais la balle est dans la cour d'autres entités.

Kurt Pritz nous a indiqué que le travail de la phase 1 est pratiquement conclu. Nous avons décidé de demander une expression d'intérêt pour un autre président pour la phase 2, avec une date limite du 22 mars. J'espère qu'on va recevoir beaucoup de propositions, pour que l'on puisse remplacer Monsieur [inaudible] qui ne pourra pas gérer la phase numéro 2.

Mais j'aimerais prendre un peu de recul et parler de la structure du conseil de la GNSO, si vous n'êtes pas familier avec cela. Il y a deux chambres en fait, dans la GNSO. Il y a les parties contractantes, les registres et bureaux d'enregistrement. Et d'un autre côté, les parties non contractantes, nous avons les entités commerciales et non commerciales, donc tous les autres intérêts qui sont représentés à la GNSO. Donc propriété intellectuelle, entreprises, utilisateurs commerciaux, non-commerciaux, prestataires de services internet, etc.

Donc c'est assez complexe, avec différents points de vus, différents groupes qui travaillent dans ces chambres.

Il y a un seul président qui est sélectionné parmi les conseillers du groupe et deux vice-président pour chacune des chambres, parties contractantes et non contractantes.

Donc c'est comme cela que fonctionne le conseil de la GNSO et nous avons des conseillers de tous ces groupes qui travaillent. Vous avez un organigramme qui est disponible sur le site web de l'ICANN si cela vous intéresse.

Donc, en bref, nous avons d'excellentes interactions avec l'ALAC, avec le GAC, avec la communauté. Et on a parlé des procédures ultérieures, de la piste de travail numéro 5, de l'EPDP, et je crois nous aurons toujours plus d'opportunités qui se présenteront.

La GNSO, ces dernières 6 ou 7 années, a beaucoup évolué. Et lors de la dernière série de gTLD, en 2012 vous vous rappelez lorsqu'il y a eu ces documents qui ont été publiés, ce guide pour déposer les dossiers de demande de gTLD, le GAC a donné beaucoup de conseils au conseil d'administration de l'ICANN. Et on a reconnu à ce moment-là qu'on serait plus efficace dans notre développement de politique si nous avions des avis un peu différent et plus tôt.

Donc il y a de cela plusieurs années la GNSO, avec Jonathan Robinson, il y a trois ou quatre années, a travaillé avec le GAC, a tendu la main au GAC pour plus d'engagements dans notre processus de développement de politique. Je crois que c'est extrêmement important pour ne pas surprendre les personnes en fin de travail, mais que plus tôt on obtienne des points de vu un

petit peu différents et qu'on accueille ces points de vue d'une manière très délibérée, ce qui va nous aider dans notre travail.

Lorsque j'ai été président, je crois que c'est important d'être plus inclusif dans le développement de PDP en consultant, en s'engageant, un invitant la participation d'autres groupes, d'autres personnes.

Tout particulièrement sur la question du PDP 3.0, l'année dernière nous avions une présidente et on s'est rendu compte qu'il y avait des PDP qui duraient des années et des années, et des années encore. C'était vraiment un processus très, très long. Il y a des PDP qui ont pris 4 ans. Le RDS, par exemple, on a clôt le groupe, ils avaient travaillé pendant 3 ans parce que… Evidement maintenant nous avons le RGPD, nous avons des spécifications ultérieures, donc la situation est fort différente.

Mais je crois qu'on s'est rendu compte au niveau du conseil qu'on doit mieux travailler et mieux gérer notre processus de développement de politique, qu'il y ait des groupes qui soient bien mis en place.

On a remis l'accent sur l'efficacité, sur la gestion des PDP, et reconnaitre que les liaisons aux groupes de PDP doivent être plus engagées, plus actives, plus disponibles pour les membres du groupe de travail en cas de problème au niveau du processus, pour respecter les procédures qui existent.

Et je crois que nous avons eu un processus avec 16 recommandations pour améliorer notre capacité en tant que conseil d'être de meilleures gestionnaires du processus pour qu'on n'ait pas des PDP qui durent 4 ans, c'est trop long. Pour qu'on n'ait pas des PDP où il y ait des problèmes au dernier moment, où la dynamique du groupe n'est pas satisfaisante. Ça il faut le savoir très tôt, il faut réagir, il faut prendre des mesures, il faut rester sur la bonne voie.

Nous avons une large envergure au niveau des ressources en personnel, nous avons beaucoup de réunions, des réunions en face à face, des réunions à distance, ce qui revient très cher tout cela. Donc il faut établir des priorités.

Et si on a un EPDP, et bien il faut reconnaitre qu'il faut peut-être effectuer une pause pour un autre point parce que dans ce pipeline nous avons beaucoup d'éléments importants à gérer. Il y a différentes parties de la communauté qui participent. Donc il ya des ressources de la GNSO limitées en fin de compte.

Donc les recommandations l'année dernière étaient celle-là. Cette année on essaye de mettre en place tout cela.

On ne dit pas que tous les PDP vont ressembler à cela, mais on va évaluer, lorsque l'on avance dans nos PDP, lorsque l'on gère les PDP qui sont déjà démarrés, on va voir si on doit modifier un petit peu les chartes de ces groupes. Est-ce qu'on peut une nouvelle

fois mieux gérer ces PDP et être plus rapides, être plus efficaces, notamment lorsqu'on fait des recommandations au conseil d'administration.

Je pourrais répondre à vos questions après ces quelques mots.

Mais je vais vous donner un exemple. Il y a un débat actuellement sur le RPM, le PDP sur les mesures de protection des droits pour tous les gTLD. Il y a une phase 2 qui travaille à l'UDRP. Est-ce que l'on doit avoir une phase 2 et changer la charte de ce groupe à la fin de la phase 1 pour lancer la phase 2 ?

Donc c'est un petit peu un test si vous voulez, pour travailler un petit peu différemment dans les PDP.

CHERYL LANGDON-ORR: Merci beaucoup Keith. Désolé aux traducteurs, je vais aujourd'hui parler un petit peu plus lentement. Parce que nous sommes aujourd'hui interprété en trois langues.

Merci Keith.

J'aimerais donc vous donner la possibilité de poser des questions. Questions brèves. Et réponse brève.

JONATHAN ZUCK: En ce qui concerne les PDP plus courts, je crois qu'on a eu des succès avec le CCWG sur le PDP, sur le cadre de référence

responsabilité. Il y avait des dates limites. Est-ce que vous allez prioriser un petit peu les PDP ? Et est-ce que vous allez redéfinir l'envergure par rapport au calendrier à respecter pour les PDP ? Et comment vous allez avancer différemment.

KEITH DRAZEK: Vous voulez que je réponde lentement et aussi brièvement à cela… En effet, nous réfléchissons à ces points. Il y a des défis à relever au niveau des calendriers, mais je crois que ça pourrait être plus efficace de changer un petit peu la manière dont on travaille, pour une nouvelle manière de faire des PDP, des PDP 3.0.

CHERYL LANGDON-ORR: Vous avez été très clair, vous avez parlé très lentement et clairement. Merci beaucoup.

HOLLY RAICHE: Donc il y a eu une révision de la GNSO, il y a eu une recommandation qui n'a pas été prise en compte, c'est plus de collaboration entre la GNSO et l'ALAC. Par exemple pour des webinaires.

Dès le début, avoir la possibilité d'en savoir plus sur les PDP, de savoir qui participe, comment on participe, je crois que ce serait

très utile. Je crois qu'il y aurait deux fuseaux horaires peut-être à prendre en compte.

KEITH DRAZEK: Oui, c'est noté. Je l'ai entendu lors de la dernière réunion avec le GAC, pour l'EPDP, pour la charte de l'EPDP. Il y avait des attentes, des interprétations un petit peu différentes je crois. Et il n'y avait pas la possibilité à ce moment-là de s'engager totalement. Donc je suis d'accord avec votre recommandation, on doit prendre cela en ligne de compte. Deux fuseaux horaires.

CHERYL LANGDON-ORR: Il faut que ce soit les bons fuseaux horaires. Et je ne vais pas vous demander à chacun d'entre vous de remercier Keith de la même manière, parce que je vais moi aussi quitter la salle bientôt. Donc je crois que c'était intéressant de vous écouter. Et si je peux le dire au nom de tous, je crois que c'est toujours une bonne chose que nous nous retrouvions avec vous, avec votre équipe de direction pour véritablement mieux connaitre le conseil de la GNSO et plus partager.

Mesdames et messieurs dans 3 minutes nous aurons une nouvelle séance. Nous allons remercier Keith Drazek, président de la GNSO, de nous avoir parlé cet après-midi.

KEITH DRAZEK: Je serai très heureux de venir vous voir et répondre à vos questions un petit peu plus longuement la prochaine fois que je viendrai vous rendre visite. Merci beaucoup.

[FIN DE LA TRANSCRIPTION]