ICANN84 | Réunion générale annuelle – Discussion du GAC sur l'atténuation de l'utilisation malveillante du DNS
Mardi 28 octobre 2025 – 13h15 à 14h30 IST

JULIA CHARVOLEN

Bienvenue à la session du GAC sur l'utilisation malveillante du DNS et son atténuation. Le 28 octobre à 13 h 15 heure locale. Cette session est enregistrée et régie par les normes de conduite requises de l'ICANN, le code de conduite des participants de l'ICANN et la politique anti-harcèlement de l'ICANN.

Pendant cette session, les questions et les commentaires seront lus à voix haute s'ils sont soumis dans le bon format dans le chat de Zoom. Il y a de l'interprétation dans les six langues des Nations Unies et le portugais. Si vous souhaitez vous exprimer, levez la main dans le logiciel Zoom, dites votre nom et la langue que vous utiliserez si c'est une autre langue que l'anglais. Veuillez parler à un rythme raisonnable pour permettre une interprétation précise.

Je donne la parole à Nicholas Caballero, le président du GAC. À toi Nico.

NICOLAS CABALLERO

Merci Julia. Bienvenue à tous et à toutes. J'espère que vous avez bien profité de votre déjeuner à Dublin. J'ai le grand plaisir de présenter nos orateurs du jour. Nous avons Edmon Chung de DotAsia. Nous avons Jo-Fan Yu. J'espère que je prononce votre

nom de façon adéquate de TWNIC et je ne vois pas M. McDermott. J'imagine qu'il va rapidement arriver. Voilà, monsieur McDermott nous rejoint. Et, nos responsables thématiques GAC pour ce sujet si important qu'est l'atténuation de l'utilisation malveillante du DNS. Martina Barbero de la Commission européenne, Susan Chalmers des États-Unis et M. Tomo Miyamoto du Japon. Merci. Je donne d'ores et déjà la parole à Tomo qui va nous présenter le sujet, les objectifs, leur intégration dans le plan annuel du GAC. Tomo, à toi la parole!

TOMONORI MIYAMOTO Merci beaucoup, monsieur le président. Bienvenue à la session de l'atténuation de l'utilisation malveillante du DNS. Je suis Tomo Miyamoto du Japon.

Voici l'ordre du jour de notre session. Après une brève Intro, il y aura une présentation de Declan, puis l'on parlera des efforts de l'utilisation malveillante du DNS et de son atténuation en Irlande, puis l'on aura un point sur le PDP lié à cette question. Puis, l'on parlera également des programmes de notification de confiance, c'est Jo-Fan Yu et Edmon Chung qui vont nous en parler. Et, on parlera du communiqué.

Alors, gérer les utilisations malveillantes du DNS est une priorité du GAC. Et, je pense que c'est une priorité pour toutes les délégations représentées ici. C'est un véritable problème pour nos parties prenantes également. On le constate dans de nombreuses sessions de l'ICANN, tout le monde évoque cette question. Au vu des

contrats de l'ICANN, les accords de bureaux d'enregistrement et des opérateurs de registre prévoient des dispositions qui les poussent à répondre à ces rapports d'utilisation malveillante du DNS.

Mais, la définition du champ d'application est assez limitée. On parle d'hameçonnage dévoiement de réseaux zombies, de logiciels malveillants et de spam. Je sais que de nombreux pays ont des problèmes en matière d'utilisation malveillance du DNS. Ce peut-être de la fraude en crypto-monnaie ou des problèmes d'applications. Au Japon, par exemple, il y a un véritable problème de l'utilisation de logiciels malveillants et c'est un véritable problème.

Le GAC a une approche double en la matière, comme cela a été évoqué dans le plan annuel et évoqué cette semaine. Dans un premier temps, nous voulons faire évoluer la définition même de l'utilisation malveillante du DNS. Puis, il y a également le calendrier. On veut mettre en place une nouvelle politique avant la délégation des nouveaux gTLD. Puis, l'on veut également un atelier sur l'atténuation des utilisations malveillantes du DNS, notamment avec un partage des bonnes pratiques. Un atelier de renforcement des capacités dès lors, qui impliquera les différentes parties prenantes de la communauté. Donc, il y a différents types d'utilisation malveillante qui exige une diversité de mesures.

Certains d'entre vous auront ce graphique en mémoire. C'est un aperçu des communautés permanentes. Le vert, c'est le champ

d'application des contrats de l'ICANN. Assez limité, vous le constaterez, et avec la définition des abus du DNS que nous connaissons. Il y a les liens entre l'ICANN et les parties contractantes qui sont également évoqués. Ici, il y a un effet juridiquement contraignant, Donc, on veut mettre en place des mesures efficaces en temps opportun avant qu'il y ait une nouvelle délégation, de nouveaux gTLD.

Il faut également envisager des mesures dans les cadres bleus et rouges, notamment pour les opérateurs ccTLD, les bureaux d'enregistrement, les opérateurs de registre et les autres partenaires.

Alors, voici les progrès réalisés pour ce qui est de la discussion du nouveau PDP. Ce sont des prérogatives de l'ICANN pour mettre en place cette politique rapidement on a décidé de bien cibler le PDP. Donc, en novembre 2024, on a évoqué le rapport INFERMAL qui a évoqué quelques points, notamment les API libres ou les enregistrements groupés. Puis, il y a également une vérification additionnelle des données de contact qui est évoquée.

En mai de cette année, il y a eu l'Institut NetBeacon qui a publié un document, un livre blanc sur cinq PDP liés à l'utilisation malveillante du DNS, avec cinq éléments évoqués par ce livre blanc. En se fondant sur ces contributions, le GAC a évoqué un avis relatif au PDP sur l'utilisation malveillante du DNS et leur atténuation à Prague. C'est un avis de consensus qui met l'accent

sur les contrôles des noms de domaine associés. Et, nous pourrons éventuellement évoquer cela un peu plus tard.

Alors, pour cette présentation, nous vous souhaitons la bienvenue à Declan McDermott de .ie, l'opérateur ccTLD de l'Irlande, qui va nous parler de l'atténuation malveillante du DNS, notamment par le biais du suivi de ces utilisations illégales et techniques.

DECLAN MCDERMOTT Alors, je suis responsable réglementations et politiques Internet pour le ccTLD .ie. Je ne suis pas issu du monde technique, je viens du volet politique. Donc, si vous avez des questions techniques quant à l'atténuation de l'utilisation malveillante, je suggère que vous atténuez vos attentes de moi. Bon, si vous avez des questions, et bien vous pouvez vous tourner vers moi après la réunion et bon si je n'ai pas la réponse, je tenterai d'y répondre malgré tout. La prochaine planche, s'il vous plaît.

Alors, .ie gère le nom de domaine .ie depuis 2000 donc, c'est notre 25e anniversaire que nous avons célébré il y a quelques mois. Principales conclusions, donc il y a un faible volume et un faible taux d'utilisation malveillante. On a environ 300 000 noms de domaine enregistrés, et la plupart de ces titulaires de noms de domaine sont des personnes physiques. J'ai demandé à nos amis de NetBeacon d'avoir un aperçu des données pour ce qui est des utilisations malveillantes du point .ie. Ils nous ont donné des

informations sur le mois dernier, du mois d'août et il y a eu un cas détecté d'hameçonnage.

Donc, le taux d'utilisation malveillante est assez faible. Nous avons également demandé à la Fédération de recherche du DNS, qui nous a dit que notre taux d'abus était de 0,05 %, et c'est 365 derniers jours, il y a eu 100 instances détectées. Donc, je dirais que c'est un opérateur de registre de faible envergure comparé à d'autres, et il y a de très faibles taux d'utilisation malveillante, ce qui est assez commun en règle générale, pour les ccTLD, si j'ai bien compris la situation.

Alors, le point .ie dispose d'une exigence particulière, c'est à dire qu'il faut avoir un lien avec l'Irlande. Depuis sa création, le nom de domaine .ie été pensé pour être utilisé par des individus avec une connexion avec l'Irlande. Donc, il y a quatre catégories différentes. Il peut s'agir d'individus qui sont implantés en Irlande ou résidant en Irlande, ou il peut s'agir de citoyens de l'île d'Irlande qui vivent à l'étranger, ou il pourrait s'agir d'organisations implantées en Irlande avec un numéro d'entreprise, numéro d'organisme irlandais ou des organisations qui sont implantées hors de l'Irlande, mais qui fournissent des biens ou des services en Irlande. Voici les quatre catégories qui nous permettent d'avaliser cette connexion à l'Irlande, Je dirais que c'est une exigence unique pour un opérateur de registre. Il ne me semble pas que d'autres opérateurs de registre aient une telle exigence.

Pour ce qui est des utilisations malveillantes, le .ie a une définition un peu plus vaste que la définition de l'ICANN. Habituellement, nous ventilons cela en trois catégories, les utilisations malveillantes technique, donc les logiciels malveillants, l'hameçonnage et les réseaux zombies. Puis, nous avons également les utilisations malveillantes en matière de contenu. Ce peut être des pratiques illégales, des contenus illégaux tels que des contenus frauduleux ou des contenus de pédopornographie. Il peut y avoir également des enregistrements de mauvaise foi.

Les définitions importent oui, mais selon moi, ce qui importe d'autant plus c'est d'avoir un éventail de mesures qui nous permette de réagir à des situations particulières. Par exemple, un opérateur de registre ne doit pas être en mesure de déterminer ce qui est illicite, ce qui constitue de la mauvaise foi. Mais, s'il y a une instance judiciaire qui caractérise ce délit, et bien l'opérateur de registre doit pouvoir réagir de façon proportionnée à ce phénomène.

Moi, j'aime bien l'acronyme ATOM, mesures organisationnelles et techniques appropriées. C'est une liste non exhaustive des différentes mesures que sont les nôtres. Chez .ie, nous estimons qu'il faut des mesures organisationnelles et techniques. Je ne pense pas qu'il y ait de panacée. Je ne pense pas qu'il y ait une mesure qui va prévenir tout. Les suspensions de nom de domaine sont une chose, mais sur le plan réglementaire, ce sont des outils qui sont utiles. C'est nécessaire, mais ils ne sont pas très précis. Si

je tente de construire une maison de poupée, et bien, j'ai besoin de plus qu'un marteau.

Donc, il faut un éventail d'outils et d'instruments qui permettent de couvrir toutes les éventualités. Bon, ceux d'entre vous qui ont des antécédents en matière de cybersécurité, et bien, connaissent les techniques de détection et de prévention.

Alors, moi, je vais faire référence à un concept de la santé publique. Dans le monde de la santé publique, si l'on évoque la question de la prévention ou de l'atténuation, et bien l'on dit que la prévention, c'est le déploiement d'interventions appropriées pour prévenir la survenue d'un événement néfaste à la santé d'une communauté, d'un écosystème ou d'une population. Sur le plan fondamental, c'est ça, la prévention. Il s'agit d'avoir une intervention qui est soit nécessaire, soit ciblée, qui empêche la survenue d'un événement néfaste. Et tout cela est divisé en plusieurs couches.

Donc, ça, ça vient de l'écosystème de la santé publique, mais ce peut être appliqué à toute une série de champs politiques tels que la prévention du sans-abrisme ou l'évaluation de l'incidence environnementale. Moi, j'aime bien utiliser ce cadre lorsque je réfléchis aux différentes mesures d'atténuation. Alors, que sont ces différentes couches? Donc, il y a la prévention de plan Initial. Traiter un problème avant que cela prenne la forme d'un risque, c'est à dire d'éviter d'avoir une crise cardiaque à 60 ans en faisant du sport à 30 ans. Donc, on prévient une fuite de données aujourd'hui en protégeant ces données par le passé.

Donc, il s'agit d'avoir des bonnes mesures en place pour l'opérateur de registre. Au niveau gouvernemental, il faut un cadre réglementaire ou juridique qui vous permet d'atteindre vos objectifs. Si votre objectif c'est de renforcer la cybersécurité, il faut réfléchir. Si votre cadre juridique force vos opérateurs de registre, vos bureaux d'enregistrement à agir de façon non sûre. Si votre objectif est d'améliorer la protection des données, il faut se demander si votre cadre juridique force des organisations à mettre en place des mesures qui ne permettent pas la protection des données.

Cette prévention primaire vous pousse à vous pencher sur votre environnement réglementaire et à analyser l'adéquation de l'instrument.

La prévention secondaire, c'est à dire empêcher une menace imminente ou aux stades initiaux. Donc, on pourrait parler des premiers stades d'une maladie. Les symptômes sont apparus. Il s'agit d'avoir une réaction rapide pour empêcher la maladie d'empirer. Si votre site Web est compromis et qu'il est utilisé pour faire de l'hameçonnage, il faut réfléchir aux systèmes qui sont en place pour détecter cela, aux processus qui permettent de réagir à cela. S'il y a une attaque de déni de service comme anycast. Y a-t-il un outil qui permette de mettre un terme à l'attaque?

Prévention tertiaire. Lorsque quelque chose s'est déjà produit, par exemple, l'hôpital est attaqué par un rançongiciel, il y a quelque chose qui s'est produit et dans ce cas, il faut réfléchir aux outils qui

permettent d'empêcher un plus grand préjudice. Dans le cadre du nom de domaine, ce pourrait être une situation extrême, ce pourrait être une suspension ou une suppression du nom de domaine si cela est nécessaire et proportionné.

Et, le dernier point que beaucoup, souvent omettent est évidemment dans le secteur de la santé publique, c'est la prévention quaternaire. Il s'agit d'éviter des interventions disproportionnées et superflues. Alors, si la prévention secondaire c'est éviter les faux négatifs. La prévention quaternaire, c'est éviter les faux positifs, c'est à dire intervenir alors qu'il ne faut pas intervenir ou intervenir de façon disproportionnée ou alors lorsque votre action sape les droits fondamentaux ou manque la cible. Donc, on peut mettre en place des examens, de la politique, on peut réfléchir à des évaluations d'incidences réglementaires pour pallier cet éventuel problème de faux positifs.

Chez .ie, nous avons toute une série de mesures en place, donc nous avons toute une série de politiques, de pratiques. Et puis, il y a, lorsqu'on descend dans l'arborescence, des mesures plus ciblées. Bon, peut-être que chaque mesure individuellement cible un élément précis, mais en fin de compte, l'objectif Faîtier est la confiance et la sécurité de notre ccTLD .ie.

Un exemple. Nous avons d'excellentes relations avec notre ministère, notre régulateur. Nous avons un excellent protocole avec notre autorité de régulation. C'est l'exemple parfait de ces bonnes relations. Alors, ce protocole prévoit que lorsque des forces

de l'ordre ou lorsqu'une autorité de régulation a identifié un problème, imaginez que vous ayez un architecte qui dit qu'il est architecte alors qu'il ne l'est pas. C'est une atteinte à la loi, et donc la Chambre des architectes nous dit que, et bien, ce type, ce n'est pas un architecte et il faut agir.

Donc, nous aurons un contrôle, la vigilance. Nous nous pencherons sur la requête. Nous verrons ce qui est demandé. Nous verrons si la base juridique est fournie. Y a-t-il suffisamment d'informations pour que nous puissions prendre une décision? La demande est elle proportionnée? La demande est elle nécessaire? Ont-ils fourni les informations dont dispose la loi? Habituellement, le bureau d'enregistrement est le titulaire du nom de domaine doivent être notifiés.

Si la situation n'est pas urgente, on donne un certain nombre de jours au titulaire du nom de domaine pour qu'il réagisse. On donne les informations de contact du régulateur, car si elles ont des questions, elles peuvent se tourner directement en valeur avec le temps. Ce que l'on ne veut pas faire, c'est d'avoir le rôle d'arbitre ici, de dire voilà, c'est du contenu néfaste, il doit être retiré. Nous, nous voulons simplement agir en quelque sorte d'entremetteur. Le régulateur à un problème, on le met en lien avec le titulaire du nom de domaine pour qu'il puisse régler le problème eux même.

À la fin de cette période de temps, si le régulateur revient vers nous et nous dit qu'il n'y a pas de réponse satisfaisante, et bien en fonction de la situation de la situation, nous prenons des mesures

de correction qui peuvent être, par exemple, jusqu'à la suspension d'un nom de domaine. Mais en général, ce qu'il se passe, c'est que le bureau d'enregistrement nous dit je ne savais pas, il fait un changement très simple et on résout la situation de telle manière.

Si en revanche, nous avons un scénario catastrophe, nous avons insisté et le régulateur est au courant ainsi que les autorités de mise en œuvre de la loi. Ils savent qu'ils doivent avoir un fournisseur de service parce qu'ils savent que si nous avons des problèmes d'adresse IP, on ne peut pas retirer une adresse IP d'Internet. Donc, le régulateur et les organismes de mise en œuvre de la loi savent que s'ils veulent retirer un site d'Internet, il faut qu'ils se dirigent vers l'hôte directement.

Mais, si quelque chose doit être retiré très rapidement et cela ne fonctionne pas, et bien, ils peuvent rentrer en contact avec nous puisque nous travaillons avec ces noms de domaine pour le rendre plus difficile d'accès. Alors, moi, je touche du bois, ça n'a pas encore eu lieu, On n'a jamais eu ce problème. Prochaine diapositive.

Un dernier cadre que j'apprécie énormément de la part, encore une fois du domaine du secteur de la santé. C'est lorsque l'on faisait l'évaluation des outils et des interventions qui étaient disponibles et possibles. C'est l'échelle d'intervention. Encore une fois, c'est une autre manière de mettre en place des interventions et de les classer. Ces manières sont classées en termes d'invasion. Donc, plus l'invasion est importante, plus elle doit être justifiée.

Donc, si on commence au départ le premier échelon, c'est de ne rien faire. En Irlande, toutes les évaluations d'impact ne font rien. C'est le défaut. Donc, il faut expliquer pourquoi une intervention est nécessaire. Si on avance, le deuxième échelon, c'est donc d'expliquer pourquoi l'intervention est justifiée. Donc, pour se protéger de l'utilisation malveillante du DNS, par exemple contre l'hameçonnage. Le troisième échelon, c'est de permettre le choix.

Donc, en tant qu'opérateur de registre, nous offrons un choix, mais nous ne forçons pas nos clients à faire ce choix. Nous passons ensuite à un changement d'option préféré. Donc, par exemple, cette option de base, c'est de ne jamais diffuser des informations, sauf si elles sont requises. Et, dans ce cas-là, il faut un consentement explicite.

Puis, nous passons aux encouragements. Si le gouvernement, par exemple, a des organisations qui travaillent sur la sécurité, ce sont des financements, des bourses qui permettent cela. A la suite de cela, il y a donc le désencouragement. Si pour les organisations qui n'ont pas d'accréditation, par exemple, c'est une possibilité, puis nous nous enlevons la possibilité de faire des choix.

Par exemple, pour les opérateurs de registre de l'Union européenne, il faut vérifier les informations du registre via le NIS2 pour savoir de quel pays vous venez. Et, le dernier choix, c'est de retirer la possibilité de faire le choix. Dans ce cas là, si on voit un problème, il faut le signaler.

Par exemple, en Irlande, nous avons un ordre de de blocage de requêtes qui peut être demandé par un juge si c'est une situation de vie ou de mort, par exemple. Si cela ne viole pas les droits fondamentaux de l'utilisateur final et si le juge est convaincu que c'est absolument nécessaire et proportionné, il peut déterminer qu'il est nécessaire de bloquer l'accès à ce nom de domaine. Cela dure quelques jours, puis il faut redemander ce bloc.

C'est le choix le plus invasif qui doit donc être limité aux situations extrêmes. Et encore une fois, ces outils, s'ils sont utilisés d'une manière disproportionnée, les effets peuvent être néfaste.

Alors, les points à retenir, c'est que l'atténuation efficace requiert différentes mesures. Encore une fois, il n'y a pas de panacée. Donc, il faudra des mesures techniques et organisationnelles. Les interventions doivent être appropriées, nécessaires et proportionnées. Pour le cas du .ie, par exemple, nous nous sommes rendus compte qu'une collaboration pertinente entre les régulateurs et les opérateurs de registre et les bureaux d'enregistrement est fondamentale. Et enfin, il est important d'éviter des interventions surdimensionnées et non nécessaires.

TOMONORI MIYAMOTO Merci beaucoup pour votre présentation. Nous aimerions vous donner le temps de poser des questions si vous en avez. Nous n'avons pas beaucoup de temps, mais nous avons le temps pour

une ou deux questions. Pas de mains levées. Oui, une question de la part du Bangladesh.

DR. SHAMSUZZOHA Merci beaucoup. Merci pour cette très bonne présentation. Et, c'est très intéressant de savoir comment la collaboration est mise en œuvre en Irlande. J'ai deux questions très rapides. La première concerne les protocoles de régulation. De la manière dont vous l'avez expliqué, j'ai compris que c'est une action réactive. C'est lorsqu'il se passe quelque chose, c'est le régulateur qui intervient. Mais, qu'en est-il des mesures proactives? Qu'est-ce qui devrait être fait? Quel processus devrait être mis en place pour les prises de décisions proactives? Y a-t-il des possibilités pour le régulateur d'intervenir en amont?

Ma deuxième question est la suivante, pour vérifier la proportionnalité des mesures. Quel est le mécanisme qui est mis en place par le .ie? Est-ce qu'il y a un système obligatoire ou est-ce que c'est une évaluation de bonne foi ou d'initiative de bonne foi? Merci.

DECLAN MCDERMOTT Alors, je vais répondre à la deuxième question. Pour commencer, nous avons différentes révisions de politiques et de mécanismes politiques. Nous avons un comité externe multipartite qui est composé de différents bureaux d'enregistrement. Le gouvernement a également un siège à la table, et nous avons

différentes organisations qui sont impliquées dans la communauté Internet de l'Irlande. C'est à ce moment-là que les mécanismes révisent les changements de politique et tous les changements de politique qui sont pertinents. Et il faut que ce comité ait son mot à dire dans tout changement politique, pour que ces changements politiques soient justes et soient alignés avec les valeurs du .ie.

Il y a également une autre option. S'il y a un changement politique important, dans ce cas là, il peut passer par une consultation publique. Nous l'avons déjà fait dans le passé, en particulier lors de modifications politiques importantes. Pour la première question. En réalité, cela dépend toujours du contexte spécifique. De la part du .ie, nous sommes un opérateur de registre assez petit. Cela n'a pas beaucoup de sens pour nous d'avoir des mesures proactives, une modération de contenu. Je ne suis même pas sûr que nous aurions même l'autorisation de le faire en fonction de la législation locale.

Mais en réalité, tout cela dépend du contexte du régulateur, de trouver un équilibre entre l'exposition et les risques qui existent. Parce que si on regarde les statistiques, par exemple, d'utilisation malveillante du .ie. Nous sommes à une exposition très faibles en réalité.

TOMONORI MIYAMOTO Merci beaucoup pour la question. Nous passons donc à la suite. La mise à jour sur les PDP. Martina, vous avez la parole.

MARTINA BARBERO

Merci beaucoup Tomo. Je vais essayer de passer le plus vite possible sur ce sujet très important parce que nous sommes déjà en retard. Donc, prochaine diapositive s'il vous plaît.

Tomo l'a déjà mentionné lors de la réunion de Prague, le communiqué conseillait à la GNSO, demander à la GNSO de prendre toutes les préparations nécessaires en amont de l'ICANN 84 pour un PDP à champ d'application restreint, puisque cela revenait du rapport préliminaire sur l'utilisation malveillante du DNS qui a été publié en septembre, et lors des commentaires publics qui ont été publiés. À la suite de cela, Le GAC a envoyé une réponse et je vous donnerai quelques indications sur la manière, sur ce que nous avons souligné de cette réponse.

Ce que vous devez savoir par rapport à ce rapport d'incident, c'est qu'il suggère la priorisation des sujets, des travaux sur l'utilisation malveillante du DNS, suggérés des API non restreints et des vérifications de noms de domaine associées, ainsi que des DGA, des algorithmes de génération des domaines. Donc, sur cette question des API non restreints, de vérifier qu'il soit possible qu'il soit aligné avec un groupe, avec un travail politique et d'indiquer que les DGA soient appropriés pour un travail politique également.

Le GAC a donc offert son soutien pour les deux sujets liés au travail politique les API non restreints et les algorithmes de génération de domaine. Le GAC est toujours très pragmatique. Nous cherchons à prioriser l'approche qui amènera une résolution la plus efficace et

la plus rapide possible. En tant que GAC, nous avons également souligné dans ce rapport, qu'il y a d'autres lacunes que nous avons identifiées qui doivent trouver réponse, puisque les deux PDP que nous allons lancer apporteront énormément d'avancées dans la lutte contre l'utilisation malveillante du DNS. Cela reste un sujet très vaste, et deux PDP ne seront pas suffisants pour lutter de manière efficace.

Les lacunes qui ont été identifiées dans ce rapport doivent trouver réponse. Le GAC a souligné certains points importants qui sont donc listés dans cette réponse. Nous avons également souligné que le GAC souhaiteraient participer au processus d'élaboration des politiques, mais pour cela, nous avons besoin de précisions sur la méthode de travail et la possibilité d'alterner entre la participation active et d'observateurs, puisque c'est une situation dans laquelle nous nous sommes déjà retrouvés dans le passé et qui fonctionne très bien pour nous. Prochaine diapositive.

Hier, nous avons tenu une session communautaire menée par la GNSO sur les PDP et sur les PDP attendus, et je voulais souligner quelques discussions qui ont déjà eu lieu. En ce qui concerne la structure des PDP, il semblerait que nous sommes assez d'accord sur le fait d'avoir deux PDP au lieu d'un seul, même si certains détails en termes de charte et de fonctionnement n'étaient pas encore précisés dans la discussion d'hier. Certaines communautés étaient également d'accord sur le fait de réfléchir à deux fois avant de lancer certains sujets via un troisième PDP.

Et, sur certains sujets, donc les API et les noms de domaine non restreints. Nous avons discuté des problèmes de définition, en particulier pour les API, parce que dans un commentaire précédent du GAC, nous avons déjà parlé de l'enregistrement en masse, d'enregistrements groupés par rapport aux API. Et, désormais, on nous dit que les API sont une manière d'enregistrer plusieurs noms de domaine de manière groupée. Mais, si nous nous concentrons seulement sur les API, nous ne résoudrons pas le problème des enregistrements groupés.

Pour les domaines associés. C'est un sujet qui paraîtrait assez simple, même s'il est important de trouver l'équilibre entre la clarification, entre les moments où nous faisons des vérifications, où les caractéristiques des identités des titulaires de noms de domaine, des méthodes de paiement. Donc, maintenir la transparence tout en permettant aux titulaires de noms de domaine d'avoir une approche qui ne donne pas toutes les informations aux personnes malveillantes sur Internet. Donc, c'est très important si nous passons à la prochaine diapositive.

Vous voyez ici une suggestion. Donc, si les PDP sont lancés, ce qui est probable désormais, vu la charte, le GAC voudrait y prendre part en utilisant l'expérience. Pardon. Il faut que je ralentisse. J'essaye de me dépêcher, mais je vais trop vite. Pardon. C'est quelque chose qui a fonctionné dans le passé, dans les processus d'élaboration des politiques. Nous avions une petite équipe parce que, comme vous le savez, dans les processus d'élaboration des politiques, nous avons un ou deux représentants du GAC plus des suppléants

si nécessaire, si la charte est modifiée selon la requête du GAC. Mais, tout le GAC ne peut pas y participer. Nous savons que l'utilisation malveillante du DNS est un sujet qui est fondamental pour la plupart des personnes dans cette salle.

Donc, la meilleure manière pour assurer la participation efficace de tous les membres du GAC, c'est d'avoir des petits groupes, une petite équipe comme nous l'appelons, qui préparerait le travail du PDP et qui permettrait à toutes les personnes intéressées de participer et d'envoyer un représentant du GAC qui aurait toutes ces informations. Cela a fonctionné dans le passé. Cela pourrait être une approche que nous pourrions mener encore une fois pour ce PDP. Prochaine diapositive.

Voici donc ma dernière diapositive, et j'espère que nous pourrons avoir une discussion ici sur ce sujet. Nous avons trois questions à vous poser. La première est la plus importante peut-être pour aujourd'hui, c'est de savoir si basé sur ces discussions que nous avons tenues dans cette salle, mais également hier avec la communauté y a-t-il des commentaires supplémentaires qui doivent être soulignés à la GNSO ou la communauté plus large en ce qui concerne le PDP, en ce qui concerne sa structure ou son sujet, ou les deux? Et, si vous pouvez nous faire savoir si vous seriez intéressés par ces efforts du PDP ou si vous souhaitez intégrer ce petit groupe qui travaillerait sur ce PDP. Donc, si quelqu'un est motivé, veuillez-nous le faire savoir.

La deuxième question concerne le travail supplémentaire qui doit être fait sur l'utilisation malveillante du DNS, donc d'aller au-delà des PDP. Nous avons une liste de sujets potentiels qui doit être évaluée, et s'il y a un message qui doit être passé à la communauté qui va au delà des commentaires publics du GAC. C'est également quelque chose que nous souhaitons savoir.

Et enfin, évidemment, une question plus large, y a-t-il des considérations à prendre en compte sur l'utilisation malveillante du DNS basé sur ce rapport préliminaire d'incidence. Donc, si vous avez des sujets que vous souhaiteriez ajouter. Nico, je vous rends la parole et je vous laisse modérer la discussion.

NICOLAS CABALLERO Merci beaucoup pour ces cette présentation détaillée et nuancée Martina. La Commission européenne veut prendre la parole, et c'est une très bonne opportunité pour que nos collègues du GAC puissent intervenir sur ces questions, sur… Y a-t-il des prises de paroles là-dessus? l'Allemagne, vous avez la parole.

RUDY NOLDE Tout d'abord, merci beaucoup aux personnes en charge de ce sujet pour cette très bonne présentation et pour tout votre travail ces derniers mois. Pour l'Allemagne, l'utilisation du DNS est l'une des priorités principales au sein de l'ICANN. Nous serions ravis de pouvoir vous aider et nous souhaiterions participer à cette petite

équipe. Et, nous sommes prêts à travailler où vous avez besoin de nous.

Sur la deuxième question, par rapport aux lacunes restantes, d'une manière peut-être plus générale, j'aimerais que ce PDP à venir ou ces PDP à venir puissent servir comme modèle de travail. Donc, nous avons restreint ce sujet, nous nous sommes concentrés sur un sujet très précis et désormais nous pourrons peut-être travailler de manière plus large. Donc, d'avoir une compréhension au sein de la GNSO qu'une fois que nous avons fait face à ce sujet, nous pourrions travailler sur d'autres sujets plutôt que d'attendre deux ans un nouveau PDP ou d'attendre de voir la situation, l'évolution de la situation.

Voilà, mes deux commentaires sur ce sujet. Merci beaucoup.

NICOLAS CABALLERO Merci beaucoup à l'Allemagne et j'imagine que vous vous portez volontaire pour la partie 1A de la question, c'est ça? Non, pardon, c'était une blague, évidemment. Merci. Merci à l'Allemagne. J'ai l'Inde, puis les États-Unis. L'Inde, vous avez la parole.

SANTHOSH THOTTINGAL Merci, monsieur le président. Nous sommes également intéressés par ce travail du PDP. Nous soutenons le lancement de ces PDP à champ d'application restreint. C'est également une priorité principale pour l'Inde et elle a été identifiée dans ce rapport, en

particulier pour l'accès aux API et aux enregistrements en groupe et le manque de vérification.

Ces deux sujets entraînent une utilisation malveillante du DNS à grande échelle. Et nous sommes tout à fait d'accord avec le GAC et avec le consensus de l'ICANN 83 de lancer une action de PDP sur ces sujets. Voilà. Merci beaucoup.

NICOLAS CABALLERO Merci à l'Inde. J'ai les États-Unis.

SUSAN CHALMERS Alors, je suis ravi de prendre la parole. Pour ce qui est de la deuxième question. Je me rappelle notre débat avec l'ALAC à propos de la transparence et de la rédaction des rapports et du signalement. Et, il apparaît que les exigences en matière de signalement des parties contractantes ne sont en réalité pas dans les contrats. Il y a une exigence de conservation des dossiers, des rapports d'utilisation malveillante reçus par le bureau d'enregistrement, mais il n'y a pas d'obligation de signalement public relatif au nombre de rapports d'utilisation malveillante reçus et traités.

Je sais cela car pendant nos discussions avec l'ensemble de la communauté. Par ailleurs, cela a été une session formidable. Pendant cette session, il y a eu une question relative à la conformité pour les contrôles de nom de domaine associé et le PDP afférent, et la façon dont la conformité pouvait être efficace. Si

jamais il y a une exigence en matière de transparence, de signalement, cela pourrait renforcer le volet conformité. Désolé, c'est très technique comme intervention, mais je pense que cela a du sens pour le volet conformité. Et nous avons par ailleurs soumis cela dans nos commentaires relatifs au GAC. Nous avons décidé d'être impliqués sur ce point d'emblée. Nico, à toi la parole!

NICOLAS CABALLERO J'ai le Danemark.

FINN PETERSEN Merci. Finn Petersen du Danemark au micro. Merci beaucoup de cette présentation. À propos de la question un. On a parlé des API, cela me paraît un peu trop restrictif. On parle d'enregistrement en groupe au GAC même si le champ d'application de ce PDP est assez restreint, et bien l'on pourrait tenter de bien cibler ce PDP afin que l'on ne tente pas de résoudre le mauvais problème et que l'on ait un PDP avec un résultat qui puisse être mis en œuvre efficacement.

Pour ce qui est de l'enregistrement des noms de domaine ou des contrôles de noms de domaine associés, évidemment, les contrôles qui seront menés ne seront pas aussi efficaces s'ils sont divulgués au préalable. Mais, s'il n'y a pas de ligne directrice, comment est-ce que le département responsable de la conformité peut s'assurer qu'il fait bien respecter le résultat du PDP? Voilà. Il faut se pencher sur ces questions. D'une part, il ne faut pas être transparent pour les acteurs malveillants, mais d'autre part, il faut

donner les outils nécessaires aux départements de conformité de l'ICANN pour qu'ils puissent bien mettre en œuvre la politique issue du PDP à l'avenir.

Le Danemark sera tout à fait disposé à contribuer. À cet axe de travail en tant que membre associé.

NICOLAS CABALLERO Oui, c'est bien noté. Merci. Cela a trait au 1A j'imagine. N'est ce pas? J'ai la Commission européenne.

GEMMA CAROLILLO Merci Nico. Gemma Carolillo au micro pour la Commission européenne. Bon, nous avons bien avancé ces dernières années. On parle toujours d'utilisation malveillante du DNS, mais il faut garder à l'esprit que ce n'est pas le GAC seul qui peut faire quelque chose. Je pense que la communauté fait du bon progrès. Donc je voulais vraiment exprimer une certaine satisfaction.

Pour ce qui est de la question numéro deux. Bon, la question un on ne pourra pas y échapper. La Commission est déjà un des responsables thématiques, mais je voulais me faire l'écho d'un commentaire de Susan. Bon, au moment de l'amendement des contrats, le GAC avait déjà soumis la question de la transparence. Et c'est vraiment un sujet crucial selon le GAC. Et, selon nous, cela aurait pu être traité lorsqu'on a modifié les contrats. Bon, nous avons mis la priorité sur ce point en tant que lacune politique restante, et cela fait partie du rapport qui a été publié.

Il y a deux autres éléments qui sont mis en exergue dans le rapport, notamment la mise en place de mesures proactives préventives. Nico, tu seras ravie que l'on fait référence aux algorithmes de détection. Voilà, un autre axe de travail qui est recommandé. Puis il y a dans ce rapport, une référence qui est faite à l'exactitude des données d'enregistrement, notamment le volet validation. Bon, si j'ai bien compris, il y a des bonnes nouvelles au vu de ce qu'a dit la petite équipe de la GNSO sur l'exactitude. Donc, qu'il y ai cet axe de travail qui va être donné à la petite équipe de la GNSO qui traite de l'utilisation malveillante du DNS. Et donc il faudrait. On va constater qu'il y aura de l'activité sur ce point.

NICOLAS CABALLERO Je suis ravi de la question de l'algorithme mais aussi un peu préoccupée. Souvenez-vous que les méchants, ils connaissent l'existence de ces outils. Et, je ne parle pas de ChatGPT ou de grands modèles de langage, Je parle d'algorithmes très sophistiqués qui utilisent du clustering ou un mécanisme qui s'appelle Random Forest. Je ne vais pas rentrer dans les détails mais bon voilà.

La parole est toujours à ceux qui la veulent pour l'instant. Si personne ne souhaite la prendre, nous pouvons passer au prochain sujet à l'ordre du jour. Je vais donner la parole à Susan qui va nous parler du programme des mécanismes de notification de confiance. Susan, à toi la parole!

SUSAN CHALMERS

Nous allons désormais évoquer un autre sujet. Mon collègue Tomo l'a dit un peu plus tôt, il y a des objectifs stratégiques du GAC quant à l'utilisation malveillante du DNS. Et ces objectifs se ventile en deux catégories. Il y a d'une part les efforts politiques relatifs à l'ICANN sur les utilisations malveillantes du DNS. À cet égard, nous souhaitons que les PDP avancent. D'autre part, il y a un atelier de renforcement des capacités qui perdure et les responsables thématiques vont continuer à diffuser des ressources auprès des responsables du GAC afin de renforcer les capacités des délégations sur le DNS.

Dans la section utilisation malveillante du DNS, dans la section 4.7, l'une des idées, c'est de fournir des informations quant aux programmes de mécanisme de notification de confiance. Alors, passons à la planche suivante qui vous est familière.

Donc, les programmes de mécanisme de notification de confiance peuvent être utilisés pour traiter les utilisations malveillantes du DNS, qui sont hors des attributions des contrats ICANN. Aujourd'hui, nous avons la chance d'être rejoints par des représentants de TWNIC et de DotAsia qui vont nous présenter leur programme de mécanismes de notification de confiance. Donc, je me tourne vers eux.

EDMON CHUNG

J'ai déjà échangé avec Jo-Fan et c'est moi qui vais débuter, puis je donnerai la parole à ma collègue. Merci. C'est un sujet qui me tient à cœur. C'est un volet absolument crucial.

Voici ma propre mouture de la planche de Tomo et de Susan. En effet, il y a des utilisations malveillantes du DNS qui surviennent hors du champ d'application de l'ICANN et cela se produit à différents endroits du réseau. Se concentrer simplement sur l'ICANN, cela ne suffit pas. Planche suivante.

Vous avez ici une perspective différente qui ne fait qu'appuyer ce qui a été évoqué par Declan précédemment, à propos d'avoir une perspective un peu plus vaste sur ce que sont les utilisations malveillantes du DNS. Voici les perspectives de .asia. Il y a les utilisations malveillantes du cyberespace et à l'intérieur de cela, il y a les utilisations malveillantes du DNS. Et ensuite encore en sous-catégories, il y a les utilisations malveillantes qui doivent être atténuées par les TLD. Et, il y a une partie de ces utilisations malveillantes qui vont au delà du volet de l'ICANN. Et ça, outre les contenus pédopornographiques et d'autres problèmes, je pense que cela apporte réellement. On ne peut pas forcément avoir un processus d'élaboration des politiques de l'ICANN pour cela.

Moi, je veux vous parler de notre collaboration avec .kids. Nous avons commencé cela lors de la précédente série de nouveaux gTLD. Donc, les politiques pour le .sexe ne sont évidemment pas les mêmes pour le .kids. Il est intéressant de voir comment les… l'orateur se reprend. Les opérateurs de registre doivent se fonder

sur le champ d'application de l'ICANN pour gérer une affaire. Mais, on ne doit pas s'arrêter là. Il y a dans certains cas un besoin d'aller plus loin. Le .kids est un exemple essentiel de cela.

Alors, nous avons lancé le .kids il y a deux ans. Les plateformes d'utilisation malveillante du DNS et de l'atténuation de ces utilisations malveillantes, celles qui ont été mises en place il y a deux ans ont été très utiles pour lutter contre ces utilisations. Nous a permis également de constituer une liste d'éléments à surveiller.

Voilà, notre périple a commencé en 2011. Il y avait à l'époque un forum sur l'utilisation malveillante du DNS, un des premiers auxquels le .asia a participé. Nous avons bien progressé ces quinze dernières années.

Voici la dernière planche. J'aimerais vous parler des mécanismes de notification de confiance. À ce stade, nous cherchons à aller au-delà des exigences contractuelles. Nous commençons par une approche inter-opérateur de registre. Donc, il y a des accords qui sont bien formalisés. On a des échanges avec d'autres opérateurs de registre ccTLD et peut-être avec d'autres gTLD, mais je veux vous dire pourquoi les ccTLD sont en première ligne.

Alors, pourquoi est-ce qu'on a des relations inter-opérateur de registre? On veut le même niveau de sensibilité, car la suspension d'un nom de domaine, c'est un outil un peu brut. Les opérateurs de registre peuvent agir en la matière. Et, nous, on veut que les différents opérateurs de registre puissent avoir la même sensibilité, si tant est que le cas exige que l'on suspende le nom de

domaine de façon accélérée. Alors, nous avons une collaboration avec .tw et .uk, TWNIC et Nominet. Nous avons des accords bilatéraux.

Nous avons une adresse électronique qui se consacre uniquement à cela. Et, nous avons un mécanisme qui nous permet de confirmer l'expéditeur. Il y a tout un mécanisme qui nous permet d'agir rapidement en cas de signalement, et nous appliquons vraiment cette collaboration et nous invitons d'autres ccTLD à nous rejoindre. Par ailleurs, cela fait un an que nous avons déployé ce sujet et ces derniers mois, nous avons commencé à agir et nous recevons des notifications pour certains domaines.

On constate parfois que dans la vraie vie, que ceux qui font de l'hameçonnage ciblent certaines régions. S'ils entendent hameçonner des utilisateurs à Taipei, certains de nos systèmes de supervision n'appréhendent pas cela, mais nos collègues à Taïwan peuvent appréhender cela et eux peuvent nous transmettre la notification et ensuite nous pouvons agir. C'est la raison pour laquelle collaborer avec d'autres ccTLD nous enthousiasme. Il y a beaucoup de choses que nous pouvons faire avec une empreinte internationale. Si l'on n'a pas cette empreinte, on va manquer des attaques d'hameçonnage ou des utilisations malveillantes qui ciblent une région géographique en particulier.

Nous nous penchons également sur d'autres volets qui vont au delà du champ de l'ICANN. On se base sur la définition de l'ICANN de l'utilisation malveillante du DNS, mais nous voulons étendre ce

réseau de mécanismes de notification de confiance pour couvrir d'autres types d'utilisation malveillante. Et, c'est la raison pour laquelle nous invitons d'autres ccTLD à collaborer avec nous. Et, par le biais de ces ccTLD, nous pourrons même échanger avec les [Inaudible] nationaux et les équipes de réaction. Donc, on peut garder cette sensibilité de niveau opérateur de registre tout en traitant des utilisations malveillantes qui vont au-delà du champ même de l'ICANN. Voici pour ma présentation. Je vais donner la parole à Jo-Fan. Susan peut-être?

SUSAN CHALMERS Merci, Edmon. Alors, je veux faire un pas en arrière. J'aurais dû le faire un peu plus tôt. Alors, nous avons un représentant d'un opérateur de registre qui opère un gTLD, et nous avons également le PDG de TWNIC, qui opère un ccTLD. Voilà, c'est important.

Et, Jo-Fan, je ne veux pas anticiper ta présentation, mais je voulais savoir si vous pouviez nous dire ce que représentait un mécanisme de notification de confiance.

JO-FAN YU Merci. Je suis Jo-Fan Yu. Merci de m'avoir invité. Je suis ravi de partager la perspective d'un opérateur de ccTLD et de ce que nous pensons, du cadre de mécanisme de notification de confiance.

Alors. Pourquoi avons-nous besoin de ce cadre? Nous savons que les utilisations malveillantes du DNS ont une empreinte internationale, mais nous avons simultanément une demande

croissante en matière de responsabilité. Alors, la réponse habituelle déployée ces jours-ci n'est pas suffisamment rapide et il y a également des entraves judiciaires. Dès lors, nous avons besoin de ce cadre, de mécanismes de notification de confiance.

Je veux soumettre un point important à la perspective d'un ccTLD. Vous le voyez, au vu de ces données, en tant que société ccTLD, nous recevons régulièrement des notifications de notre gouvernement à propos de sites web illicites. Ce sont des données qui couvrent la période de janvier à septembre 2025. Moins de 1 % de sites web illégaux sont des .tw. Donc, dans notre juridiction, plus de 99 % des sites web illégaux sont dans un champ qui ne nous permet pas d'agir. Donc, selon un ccTLD, c'est vraiment très important d'avoir cela.

Alors, qu'est-ce qu'un cadre de mécanisme de notification de confiance. C'est un mécanisme qui permet des actions rapides et qui permettent de créer des règles préétablies. Bien sûr, nous gérons également l'utilisation malveillante du DNS dans certains cas, de manière plus efficace et plus efficiente. Et il est très important également d'avoir ici la confiance et la transparence dans ces processus. Actuellement, ce cadre nous permet de collaborer avec des opérateurs de registre et des bureaux d'enregistrement.

Comme le .asia, le .uk et certains gTLD également, ainsi que des bureaux d'enregistrement. En plus de cela, en plus de l'utilisation malveillante du contenu, nous travaillons principalement sur

l'utilisation malveillante du DNS et nous utilisons donc des SOP. Nous utilisons des accords qui nous permettent de négocier avec nos partenaires en mettant en compte des principes de diligence raisonnable et de transparence.

Vous voyez ici, donc, sur cette diapositive, la manière dont nous fonctionnons. Donc, sans les notifications de confiance, nous avons des informations de la part du gouvernement, des organes de mise en œuvre d'application de la loi. Nous faisons des recherches puis nous faisons un rapport. Puis. À la suite de ce rapport, un autre organe effectue un deuxième rapport.

Alors, que lorsque nous avons ce mécanisme de confiance, de notification de confiance, vous voyez que le .twnic fait ses recherches lui-même et peut directement utiliser un SOP qui avaient été établis préalablement et peut agir directement. Nous n'avons donc pas besoin de répéter ses efforts d'investigation.

Donc, les avantages de ce type de cadre sont les suivants. Tout d'abord, nous avons un cadre qui permet d'accélérer l'intelligence liée aux menaces et à la gestion de l'utilisation malveillante du DNS. Le deuxième avantage, c'est la réduction de la difficulté des investigations pour les bureaux d'enregistrement et les opérateurs de registre. Nous sommes également bien plus proactifs puisque nous sommes plus efficaces. Désormais, cela ne prend que quelques instants, que quelques jours pour pouvoir faire face à ces menaces. Cela nous permet d'être plus proactif et de réagir avant une escalade de la menace.

En 2025, je voulais vous présenter les données de 2025. Cette année, nous avons géré 51 domaine. Nous nous attendions à gérer bien plus de domaines que cela en réalité, mais la plupart de nos chiffres venaient de la deuxième partie de cette année. Donc, ce chiffre sera peut-être plus élevé l'année prochaine. 78 % ont été confirmés comme des sites frauduleux ou d'hameçonnage.

Le temps de réponse est inférieur à deux jours. En général, cela prend un ou deux jours et nous nous sommes dit que nous pourrions tout de même améliorer ce temps de réponse en utilisant l'automatisation. Un avantage, c'est que jusqu'à présent, nous n'avons reçu aucun appel, aucune demande d'appel. Ce qui veut dire que cette procédure fonctionne. Prochaine diapositive. Merci.

Alors, quels sont les défis auxquels nous devrons faire face? Et, bien, puisque les opérateurs de registres et les bureaux d'enregistrement ont différents critères, nous dépendons des accords passés avec ceux-ci. Cela entraîne donc un problème d'échelle, en particulier pour ce cadre. Mais, je pense que pour les prochaines étapes, nous allons continuer d'augmenter la confiance dans ces partenariats, tout en développant et en montrant des modèles non réglementaires qui ont fonctionné pour une coopération de l'industrie. Et, nous sommes également alignés avec l'ICANN et les bonnes pratiques liées à l'atténuation de l'utilisation malveillante du DNS, du GAC.

Nous pensons donc que cette étape de mécanisme de notification de confiance est absolument cruciale et nous permettra de rassembler la communauté de l'Internet. Et, nous encourageons donc les représentants du GAC. Nous leur demandons de demander à leurs ccTLD de comprendre ce qu'il en revient. Et, si vous avez des questions, si vous êtes intéressés, vous pouvez rentrer en contact avec nous. Merci beaucoup.

SUSAN CHALMERS Merci beaucoup Jo-Fan et merci Edmon. Merci pour votre présentation. Nous aimerions désormais vous donner la parole pour donner la parole au représentant du GAC, pour voir si vous avez des questions à poser à Edmon ou à Jo-Fan.

Brian Beckham Merci beaucoup Susan. Merci Jo-Fan. J'avais une question sur votre premier point, de votre dernière diapositive, sur les questions des différents critères entre les opérateurs de registre et les bureaux d'enregistrement et la mise à l'échelle. Je me demandais s'il serait intéressant de réfléchir à un cadre uniformisé pour pouvoir faire face à cette question, en particulier pour les mécanismes de confiance, pour que nous puissions utiliser les vérifications qui sont faites dans un contexte, et dans ce contexte de l'écosystème de manière plus large.

Jo-Fan Yu

Merci beaucoup pour votre réponse. Pardon. Est-ce que je peux répondre directement? Merci. C'est une très bonne question, effectivement. Oui, effectivement, ce serait très utile d'avoir une plateforme technique qui nous permettrait d'avoir une harmonisation des négociations et des échanges d'échange d'informations. Mais, je pense que la vraie difficulté ici, ce sont les niveaux de connaissance au sein de la communauté sur ces sujets. Nous savons qu'il y a de plus en plus de connaissances, mais nous ne sommes pas encore une connaissance parfaite. Donc la question, c'est de savoir comment nous formulons ces critères, ce partage d'informations et comment nous prenons action. Mais, c'est un vrai problème. Vous avez raison.

NICOLAS CABALLERO

Merci beaucoup. Edmon, vous vouliez répondre? Vous avez la parole.

EDMON CHUNG

Merci beaucoup. Juste pour ajouter très rapidement, la réponse la plus courte, c'est de dire oui, évidemment, le .asia travaille avec le TW pour les formats, pour améliorer ce ces documents qui sont envoyés pour pouvoir accélérer ces retraits de DNS. Nous travaillons également avec CleanDNS et avec NetBeacon. Ces organisations pour essayer de trouver des normes d'industrie qui nous permettraient d'harmoniser ces processus.

NICOLAS CABALLERO

Merci beaucoup. J'ai le Japon qui a levé la main.

TOMONORI MIYAMOTO Merci beaucoup pour vos présentations. J'aimerais vous demander ce que vous attendez de notre part? Comment est-ce que nous, en tant que membres du GAC, nous pouvons vous aider pour vous aider dans vos projets?

EDMON CHUNG Et, bien, en encourageant vos ccTLD à nous rejoindre parce que, comme je l'ai dit, nous priorisons le travail avec les opérateurs de registre pour le moment, puisque ce sont… c'est un sujet assez sensible pour le moment, en particulier les retraits des noms de domaine pour les gTLD, mais j'aimerais me tourner vers les membres du GAC aujourd'hui pour vous encourager et demander à vos ccTLD de nous rejoindre dans notre réseau.

JO-FAN YU Oui, je pense effectivement que les ccTLD ont un grand rôle à jouer et si les membres du GAC pouvaient sensibiliser sur cette question et encourager les encourager à nous rejoindre, cela nous aiderait grandement.

NICOLAS CABALLERO Merci le Japon pour votre question. Est-ce qu'il y a d'autres commentaires, d'autres questions pour ces cinq dernières minutes avant de rendre la parole aux Etats-Unis, pour des questions liées au communiqué?

THIAGO DAL-TOE Merci beaucoup. Merci pour votre présentation. Ma question est la suivante nous n'avons pas de possibilité au niveau de notre pays de créer un mécanisme de notification de confiance, nous pouvons rejoindre d'autres mécanismes. Cependant, et dans ce cas là, quel est le processus et comment acceptez-vous de telles candidatures?

EDMON CHUNG Et, bien, pour le moment, nous le faisons de manière bilatérale puisque chaque ccTLD aura sans doute des exigences différentes en ce qui concerne les notifications mutuelles. À côté de cela, nous partageons également des données. Donc, pour le moment, nous partageons toutes les notifications de retrait de nom de domaine avec TW et vice versa, mais certains accords peuvent ne pas inclure ceci.

Donc, pour le moment, ce sont des accords bilatéraux, des protocoles d'entente qui sont établis entre nous et le ccTLD pour savoir si nous avons besoin de systèmes ou d'autres Type d'accord, et bien, cela pourrait prendre la forme seulement d'emails protégés où nous échangeons les clés, mais nous avons également un système que nous pouvons développer avec le ccTLD directement.

NICOLAS CABALLERO J'ai une question justement là-dessus. Comment est-ce que vous partagez les données? Est-ce que vous les partagez en CSV? Est-ce que c'est un .odf?

EDMON CHUNG

Oui, ce sont des CSV et nous partageons donc les domaines retirés et code simple pour des raisons de suspension.

SUSAN CHALMERS

Merci beaucoup, monsieur le président. Il nous reste quelques minutes. Est-ce que nous pouvons passer donc désormais au point final de l'ordre du jour? Les membres du GAC auront donc vu que nous avons déjà envoyé certains points à prendre en compte pour l'élaboration du communiqué. Et, je voulais attirer votre attention sur ces points pour commencer à y réfléchir. Pour le moment, les codirigeants de ce sujet n'ont pas de recommandation. Ils sont ravis de l'avis qui avait été produits à Prague, et les progrès qui ont été faits sur ce sujet par le communiqué depuis lors.

Voici donc les points d'importance. Je vais les lire, mais vous les voyez également à l'écran. Si quelqu'un voulait en rajouter un point pour la section des points d'importance, ce serait formidable. Nous sommes en train de travailler déjà sur le projet de texte, donc vous avez la parole.

NICOLAS CABALLERO

Merci beaucoup aux Etats-Unis pour cela. Comme Susan l'a dit, vous avez encore la possibilité de prendre la parole si vous avez d'autres idées. Comme d'habitude, toute bonne idée est la bienvenue. Avant de conclure, est-ce que quelqu'un souhaiterait ajouter quelque chose? Je ne vois pas de main levée en ligne. Il y

en a-t-il dans la salle? Non plus. Ce qui veut dire que nous sommes d'accord. Et, bien, très bien, merci beaucoup. Nous n'avons pas besoin de rester plus longtemps. Il nous reste deux minutes, mais pas besoin de les utiliser apparemment. Nous avons donc une pause café tout de suite. Une pause café de 30 minutes. Donc, soyez de retour s'il vous plaît à 3 h, heure locale. Merci beaucoup. La séance est levée.

[FIN DE LA TRANSCRIPTION]