FR

ICANN85 Mumbai | Forum de la communauté – GAC : discussion sur l’atténuation de l’utilisation malveillante du DNS
Lundi 9 mars 2026 – 16h30 à 17h30 IST

NICOLAS CABALLERO	Bonjour à tous et à toutes. Je vous demande de vous asseoir. Nous allons bientôt commencer. Nous allons commencer dans une ou deux minutes.
JULIA CHARVOLEN	Bienvenue à cette session du GAC sur l'atténuation de l'utilisation malveillante du DNS, lundi 9 mars 16 h 30, heure locale. Veuillez noter que cette session est enregistrée et régie par les normes de conduite requises par l'ICANN, par le code de conduite des participants de la communauté de l'ICANN et la politique anti-harcèlement de la communauté de l’ICANN. Veuillez bien donner votre nom pour le compte rendu et la langue dans laquelle vous vous exprimez s'il s'agit d'une autre langue que l'anglais. Et pour le bien de nos interprètes, veuillez parler à un rythme raisonnable et éteindre tous vos dispositifs quand vous parlez. Sans plus attendre, je passe la parole à notre président du GAC, Nicolas Caballero.
NICOLAS CABALLERO	Merci beaucoup, Julia. Bienvenue à cette séance sur l'atténuation de l'utilisation malveillante du DNS. Nous avons un excellent panel

avec nos responsables du GAC pour ce thème : Martina Barbero de la Commission européenne qui nous rejoindra en ligne, Tomo Miyamoto à ma droite, Gabe Andrews du gouvernement des États-Unis, qui est également coprésident du groupe de travail sur la sécurité publique, Susan Chalmers des États-Unis. Et notre invité Devesh Tyagi - j'espère ne pas avoir écorché votre nom, toutes mes excuses par avance – gestionnaire du ccTLD .IN et Manju Chen du réseau de mécanismes de notification de confiance. C'est une séance d'une heure et j'espère très franchement que nous aurons tout le temps dont nous aurons besoin pour une petite séance de questions-réponses à la fin de notre session. L'idée, c'est d'avoir un échange interactif avec vous tous et vous toutes. Et sans plus attendre, je passe la parole à Susan.

SUSAN CHALMERS

Merci, président. Bon après-midi, chers collègues du GAC. Je m'appelle Susan Chalmers. Je représente les États-Unis. Je suis également coresponsable pour le thème de l'atténuation de l'utilisation malveillante du DNS avec mon collègue du Japon et de la Commission européenne. Cette séance du GAC sur l'atténuation de l'utilisation malveillante du DNS est une priorité, porte sur un thème prioritaire pour le GAC. Alors c'est vrai que nous avons en fait toute une série d'attaques par réseaux zombies notamment.

Alors nous avons un plan annuel. Voilà, ma présentation s'affiche Alors, le plan annuel du GAC 2025-2026 propose deux pistes de travail. Une première piste, alors c'est en fait un développement de

politiques justement, un processus d'élaboration de politiques sur justement les utilisations malveillantes du DNS. Et puis, nous avons en fait la piste de travail de renforcement des capacités. Il s'agit en fait de renforcer les connaissances et les capacités des membres du GAC concernant ces thématiques.

Alors, quand on parle d'utilisation malveillante du DNS, on parle de cyber-activités que la plupart des gouvernements considèrent comme étant des cyberdélits, des cybercrimes (p. ex. hameçonnage, dévoiement, etc.). Il y a une définition spécifique. Ça veut dire en fait l'hameçonnage, le dévoiement notamment, ou encore les spams ou les pourriels lorsque les pourriels sont utilisés justement pour envoyer des logiciels malveillants ou encore des réseaux zombies. Hameçonnage et dévoiement. Alors vous savez qu'il y a des acteurs qui exécutent ces menaces par le biais des services de fournisseurs d'Internet, d'hébergement. Alors, nous avons un axe de travail notamment qui se centre sur les identifiants, et nous nous centrons sur les politiques pour les registres et pour les bureaux d'enregistrement qui ont des contrats avec l'ICANN pour que ces parties contractantes puissent activement prendre des mesures pour empêcher que l'on utilise et que l'on exploite les noms de domaine par ces facteurs de risque.

De manière plus générale, les registres et les bureaux d'enregistrement sont tenus par contrat justement de veiller à atténuer les risques d'utilisation malveillante. Et puis, le département de conformité de l'ICANN procède à des audits justement pour voir si ces exigences contractuelles sont bien

respectées. Ce sont les deux faces d'une même monnaie. Nous avons en fait une série d'amendements qui ont été proposés au contrat entre les registres et les bureaux d'enregistrement et l'ICANN. Ces amendements sont entrés environ en 2024. Sur ce transparent, nous voyons un tout petit peu l'historique. Ce n'est pas en fait un transparent ou une diapositive exhaustive. Alors, je crois que nous sommes 19 représentations, 19 nouveaux représentants du GAC ici depuis Dublin. Est-ce qu'il y a des nouveaux venus? Est-ce qu'on peut leur demander de lever la main?

NICOLAS CABALLERO Alors les nouveaux représentants au GAC, est-ce que vous pouvez lever la main?

SUSAN CHALMERS Merci. Bienvenue. Alors, petite astuce de professionnel. Alors, l'équipe de soutien du GAC, en fait, élabore des fiches d'information pour les membres du GAC et cette équipe a réussi justement à faire une fiche avec tout l'historique de l'utilisation malveillante du DNS et les interactions avec les membres du GAC. En fait, c'est un document d'une quinzaine de pages qui vous donne un excellent aperçu de tout l'historique de cette thématique, de ce sujet.

Alors voilà quelques jalons, outre les amendements au contrat. Alors, par exemple, un autre jalon, c'est notre avis de l'ICANN 83.

C'était donc la réunion de Prague. Je ne vais pas vous lire ce qui apparaît à l'écran, mais voilà ce que le GAC a proposé dans son communiqué l'année dernière et puis, plus récemment. Voilà quelque chose qui nous a fait très plaisir. La GNSO a adopté en fait une nouvelle charte de PDP – de processus d'élaboration de politiques – pour les vérifications de domaines associés. D'ailleurs, durant notre programme à mi-parcours, mon collègue va parler des activités annuelles actuelles concernant ce processus d'élaboration de politiques concernant les ADC, comme on les appelle, les vérifications de domaines associés.

Alors si nous pouvions passer à l'ordre du jour, voilà notre programme pour cette session. Outre ce qui se fait au niveau de l'ICANN, nous allons d'abord écouter deux présentations qui nous permettront de mieux comprendre les différentes politiques et arrangements opérationnels, en fait, qui sont mis en place en dehors de l'ICANN, face aux utilisations malveillantes du DNS. NIXI, notre hôte, est l'administrateur en fait du TLD géographique .IN nous montrera la politique adoptée ici pour empêcher les utilisations malveillantes du DNS. Et puis, sur la base de notre dernière séance à Dublin durant l'ICANN 84, en faisant fond sur cette séance, nous allons maintenant entendre une présentation du réseau de mécanismes de notification de confiance, le TNN, et nous allons en fait parler du lien qui existe avec notre plan annuel de renforcement des capacités. Alors, de manière générale, le TNN, c'est plus qu'un programme, c'est un réseau de mécanismes externes à l'ICANN. Mais Manju Chen, directrice de politiques du

réseau de notification de confiance, nous fera une petite présentation. Mais sans plus attendre, je vous propose de bien écouter Devesh Tyagi de NIXI qui est en fait le gestionnaire du domaine .IN.

DEVESH TYAGI

Merci. Merci beaucoup. Bonsoir. Alors nous sommes un registre en fonctionnement depuis 2012 et au cours des deux dernières années, disons, nous avons pris plusieurs initiatives que nous aimerions vous présenter. Ces initiatives se basent sur notre expérience de terrain, sur la base de ce que nous avons constaté sur le terrain. Alors, voilà quelques-unes de ces mesures que nous avons mises en place. Vérification par mots clés du nom de domaine. Vérification WHOIS. Incorporation de nos efforts avec la coopération avec les forces de l'ordre indiennes. C'est vrai que pour l'instant, nous entretenons des discussions avec ces forces de l'ordre et nous avons reçu pas mal de suggestions de leur part que nous avons incorporées dans nos politiques pour atténuer les utilisations malveillantes du DNS que nous avons constaté.

Alors tout d'abord, nous avons commencé en fait un processus d'identification pour les ressortissants étrangers qui demandent, en fait, d'être intégrés au registre. Alors, maintenant, nous avons une vérification. Nous utilisons des documents comme les passeports, cartes d'identité et autres types de documents d'identification. Autre chose que nous avons fait, nous avons pris les contrats d'accréditation des bureaux d'enregistrement et nous

avons introduit une nouvelle clause, la clause 4.4.15, et les candidats étrangers qui demandent en fait un domaine .IN doivent montrer patte blanche et dire que vraiment ils ont un objectif ou un lien commercial légitime en Inde. Nous avons réussi ainsi à atténuer certains problèmes, certaines menaces que nous avions constatés avec les domaines .IN. Transparent suivant, s'il vous plaît.

Alors, concernant ces autres initiatives d'atténuation que nous avons mises en place depuis octobre 2023, nous avons une initiative en particulier qui nous permet de surveiller l'enregistrement de domaine. Nous avons mis en place, en fait, des mesures comme par exemple, le placement de mots clés sensibles et bien connus comme .gov, .nic, .bharat, etc., sur une liste réservée pour empêcher les utilisations malveillantes. Nous nous sommes rendu compte en fait que très souvent, il y avait par exemple des utilisations malveillantes cachées derrière des initiatives soi-disant gouvernementales. Et donc nous avons vraiment placé tous ces noms – .gov, .nic, .bharat – dans notre liste de surveillance. Lorsque ces domaines sont enregistrés, nous procédons en fait à une enquête.

Autre initiative que nous avons lancée depuis mai 2024, c'est que nous avons un mécanisme en temps réel pour signaler et bloquer les enregistrements de domaine lorsqu'ils sont présentés par des récidivistes qui utilisent en fait des identifiants courriels malveillants ou encore des numéros de téléphone malveillants à des fins malveillantes. Voilà, donc nous avons une liste de

contrevenants au cours des dernières année. Si nous enregistrons une demande d'enregistrement de la part d'un courriel ou d'un numéro de téléphone portable qui est dans cette liste, il y a signalement, et nous prenons une mesure pour bloquer ces demandes.

Nous procédons à une vérification manuelle également des détails WHOIS des noms de domaine. Parfois, certains champs doivent être, bien sûr, remplis pour l'annuaire WHOIS. Nous nous rendons compte que parfois, il y a vraiment des informations erronées qui sont indiquées à des fins malveillantes. Si nous ne pouvons confirmer, ou en tout cas, une fois que nous vérifions de manière manuelle, nous pouvons constater s'il y a des fins malveillantes ou pas. Et nous examinons et nous agissons. Lorsque nous recevons la liste de noms de domaines reçus d'agences telles que, par exemple, l'équipe d'intervention informatique d'urgence notamment ou le Centre de coordination de la cybercriminalité indienne et d'autres forces de l'ordre, toutes ces instances ont des listes de noms réservés, de noms qui font l'objet d'utilisation malveillante. Là, encore une fois, nous utilisons ces listes pour pouvoir signaler les cas d'utilisation malveillante et ce qui nous permet d'agir directement. Alors nous avons un suivi régulier des enregistrements de domaine depuis octobre 2023. Nous avons en fait ce mécanisme régulier de suivi que nous avons mis en place. Nous surveillons en fait les enregistrements ou les domaines enregistrés quotidiennement. Alors, c'est là que nous surveillons s'il y a effectivement des activités de cybercriminalité,

d'hameçonnage, de problèmes potentiels à la réputation. Nous avons une liste de mots clés qui a été mise en place sur la base des contributions des forces de l'ordre, notamment de MeitY et de NIXI. Alors, nous avons également des termes sensibles comme PMO, Reserve Bank of India par exemple. Je vous le disais, nous avions pris une mesure similaire concernant notamment les noms de domaine où figure par exemple le mot gov. Alors, nous avons pu en fait identifier et atténuer les menaces en faisant rapport notamment au Centre de coordination de la cybercriminalité indien et ainsi qu'aux institutions concernées. Et puis en fait, nous nous sommes rendu compte que, très souvent, on utilisait par exemple le nom de la banque indienne ou encore du Centre de lutte contre la cybercriminalité à des fins malveillantes.

Alors voici quelques statistiques ou voici plutôt quelques listes de noms interdits. Là, évidemment, ce sont des cas d'utilisation malveillante qui nous ont été signalés, tout simplement parce que nous avions déjà mis sur notre liste de surveillance un numéro de téléphone portable notamment, ou encore des courriels suspects. À travers toutes ces initiatives, nous avons réussi à atténuer les utilisations malveillantes. Et je vais vous présenter, en fait, les mesures que nous avons mises en place, les rapports de menace. Alors ces rapports émanent des forces de l'ordre, du Centre de coordination de la cybercriminalité, de l'équipe d'intervention informatique d'urgence informatique notamment et de MeitY. Vous voyez en fait que depuis le lancement de cette initiative, en 2024 notamment, nous avons reçu 78 rapports de menaces, puis on est

passé à 23 en 2025. Cette année, nous n'avons reçu qu'un seul rapport de la part des forces de l'ordre.

Voilà, ces initiatives que nous avons prises sont couronnées de succès. Pour le Centre de coordination de la cybercriminalité indienne, c'est donc la grande agence de cybercriminalité ici en Inde. Donc, vous voyez les chiffres pour 2023, 2024, 2025. En 2025, nous en avions 17; en 2024, 211. Donc on est passé à 17 puis à zéro pour cette année. Et puis, pour l'équipe d'intervention informatique d'urgence, nous avons reçu 506 rapports en 2024. Nous sommes passés à 177 en 2025 et pour cette année, nous n'en comptons que sept. Donc voilà, vous voyez vous même que le nombre d'incidents a vraiment diminué de manière importante.

Et ça, c'est une initiative de grande ampleur que nous avons mis en œuvre au niveau de KYC. Et nous mettons en œuvre maintenant eKYC. Ici, vous voyez que plus de 3 000 domaines sont enregistrés par jour sur .IN. Grâce à ce processus de vérification qu'on a mis en œuvre, 4 % environ représentent des domaines que nous pouvons identifier comme étant potentiellement une menace. Une fois qu'ils sont mis en attente, les gens peuvent déjà procéder à une vérification uniquement sur ces 4 % de demandes qui sont en attente. Donc, vous voyez que sur ces 4 % de domaines en attente qui font l'objet d'une vérification en raison d'une utilisation malveillante potentielle, etc., vous voyez ici les chiffres et il est inutile que je les commente, puisque vous voyez par vous-même. Grâce à cette initiative, vous voyez ici qu'on a très bien progressé à ce niveau-là aussi. Nous en sommes maintenant au numéro de

série 58 avec 4 millions de noms de domaine, et nous avons dénombré 2 276 noms de domaine enregistrés à des fins malveillantes. Vous voyez que des progrès énormes ont été accomplis.

J'aimerais vous dire que nous travaillons au niveau de l'accord d'authentification des bureaux d'enregistrement et, à ce niveau-là, lorsqu'on reçoit des menaces ou lors de grands événements comme le G20 et autres, alors nous voulons être fin prêt au niveau de la sécurité. C'est la raison pour laquelle le registre .IN et d'autres types d'initiatives de ce genre ont eu d'excellents résultats. Merci. Diapo suivante. Alors, ce nouvel accord d'accréditation des bureaux d'enregistrement ont fait que les noms de domaine sont plus sûrs. Donc, quelques nouvelles clauses principales qui ont été mises en œuvre dans ce cadre : les KYC sont obligatoires pour tous les titulaires de nom de domaine, le maintien des transactions IP et financière pour les bureaux d'enregistrement, la désignation d'un responsable des plaintes pour chaque bureau d'enregistrement afin d'atténuer l'enregistrement potentiel de noms de domaine à des fins malveillantes. Diapo suivante.

J'aimerais partager les résultats avec vous également de cette mesure. Vous voyez ici le Tribunal suprême de Delhi, qui a salué les résultats en reconnaissant l'efficacité de ce processus, en disant que ce processus a renforcé la conformité et sauvegardé les intérêts des titulaires de noms de domaine dans un écosystème qui est le nôtre. Et ça me semble être un pas en avant considérable pour nous tous. Même les forces de l'ordre ont salué le soutien de

NIXI dans la lutte contre la cybercriminalité au niveau du pays. Voilà ce que je voulais partager avec vous. Je vous remercie de l'occasion qui m'a été donnée de vous faire cette présentation.

NICOLAS CABALLERO Merci beaucoup, Devesh. Nous avons 3 à 5 minutes pour des questions. Comme nous n'avons pas beaucoup de temps, nous allons donner la priorité au gouvernement. S'il n'y a pas de questions de la part de nos représentants gouvernementaux, on donnera la possibilité aux autres participants de poser des questions. Cela étant dit, voyons s'il y a des demandes d'intervention en ligne. Voyons s'il y a des demandes de parole en salle, des questions à l'intention de M. Devesh. Oui. Allez-y, je vous en prie.

PERSONNE NON IDENTIFIÉE Bonjour, représentant des bureaux d'enregistrement. Je voulais savoir ce que vous entendez exactement par rapport de menaces.

DEVESH TYAGI Rapport de menace, ça veut dire que les forces de l'ordre, sur la base de leur propre outil d'analyse, voient quels sont les domaines qui sont menacés parce que, chaque jour, les opérateurs de registre partagent toutes les informations au niveau des noms de domaine, avec toutes les forces de l'ordre du pays. Grâce à ces outils, ils peuvent analyser ces domaines et élaborer le rapport de menace sur la base de ces informations.

NICOLAS CABALLERO Merci beaucoup. D'autres demandes d'intervention? Le Taipei chinois.

PEI YING Bonjour. Je suis la représentante du Taipei chinois et je travaille également avec TWNIC. J'avais une question. Est-ce que vous pourriez partager votre expérience, notamment par rapport à ce que vous venez de décrire à l'instant? Parce que d'après ce que j'ai compris, c'est une assistance volontaire qui est prêtée de la part de votre organisation.

DEVESH TYAGI Oui, nous pouvons tout à fait partager de plus amples informations par rapport à notre expérience. Oui, il s'agit d'une initiative proactive parce que, avant tout et par le passé, on répondait après coup aux menaces. Maintenant, on essaie de prévenir, d'avoir une attitude proactive face aux menaces et d'anticiper ces menaces. Donc, je vous le disais, sur tous ces milliers de domaines enregistrés, on a pu identifier 4 % de domaines susceptibles de représenter une menace. Et donc, sur ces milliers de noms de domaines enregistrés, seuls 4 % représentaient potentiellement une menace.

NICOLAS CABALLERO Merci beaucoup, le Taipei chinois, pour votre question. Si vous souhaitez intervenir, faites-le savoir. Souvenez-vous que nous

accordons la priorité aux représentants gouvernementaux du GAC. Je vous prie de m'en excuser, mais parce que nous n'avons pas beaucoup de temps. C'est ainsi qu'on doit procéder. Je vous en prie.

BANGLADESH Merci. Représentant du Bangladesh au GAC. Je voulais vous féliciter de cette excellente initiative prise par le gouvernement de l'Inde. J'aimerais savoir, en Inde, vous obtenez des informations au niveau de l'utilisation malveillante du DNS et vous appliquez des mesures à ce niveau-là. Qu'en est-il de l'utilisation malveillante du DNS pour ce qui se passe au-delà du .IN, est-ce que vous recevez ce même type d'information de manière régulière? Et à ce moment-là que faites-vous? Et quelles mesures appliquez-vous?

DEVESH TYAGI Oui aujourd'hui, nous parlons à haut niveau et c'est un travail en cours. Mais on travaille essentiellement pour obtenir ce résultat.

NICOLAS CABALLERO Merci le Bangladesh pour cette question. Je vois une main levée sur ma droite. Allez-y!

MELANIE ALDONCE Merci. Je m'appelle Melanie Aldonce du Chili. Merci Docteur de votre présentation. J'aimerais savoir si vous avez trouvé des domaines qui sont enregistrés mais qui ne sont pas activés

immédiatement, c'est-à-dire qu'ils ne sont pas alloués à un fournisseur d'hébergement, parce qu'on sait qu'il y a beaucoup de noms de domaine qui font l'objet d'abus, qui sont enregistrés et qui restent inactifs pendant très longtemps.

DEVESH TYAGI Oui. Une question tout à fait pertinente que vous posez là. Nous en sommes parfaitement conscients et j'aimerais vous dire que le processus que je vous ai présenté aujourd'hui va maintenant devenir automatique. Par conséquent, tous les cinq mois, grâce à un outil IA que nous avons créé, nous allons pouvoir voir et analyser tous les noms de domaine dont dispose un opérateur de registre. Et ça, c'est un outil qui a été créé parce qu'on sait qu'il y a certains noms de domaine qui sont dormants et sont réactivés après une certaine période de temps. Donc on analyse, grâce à cet outil, chaque domaine en utilisant cet outil automatique généré par l'intelligence artificielle afin de pouvoir détecter ce genre de nom de domaine.

NICOLAS CABALLERO Merci beaucoup. Julia?

JULIA CHARVOLEN Non, je n'ai pas de question, mais je vais lire une question qui est posée sur le tchat par Tiago. Combien de bureaux d'enregistrement commercialisent un ccTLD .IN? Et voyez-vous des demandes

d'enregistrement malveillantes liées à une grande fourchette de bureaux d'enregistrement ou seulement quelques-uns?

Oui, excusez-moi, je vais répéter. Combien de bureaux d'enregistrement commercialisent des ccTLD. IN? Et voyez-vous des demandes d'enregistrement malveillantes liées à un grand nombre de bureaux d'enregistrement ou quelques-uns seulement?

DEVESH TYAGI Nous voyons que chaque bureau d'enregistrement a des activités commerciales par l'intermédiaire de leur domaine qui est enregistré auprès d'eux. Donc, pour les bureaux d'enregistrement étrangers, nous vérifions quelle est leur affiliation par rapport aux domaines .IN, et chaque fois qu'un bureau d'enregistrement a un titulaire de nom de domaine étranger ou indien, on voit s'il est conforme aux KYC. Ça, c'est la condition sine qua non.

NICOLAS CABALLERO On va avancer, et je vais céder la parole à Martina Barbero, de la Commission européenne, puis à Gabriel Andrews. Merci. À vous, Martina.

MARTINA BARBERO Bonjour. J'espère qu'on m'entend bien. Toutes mes salutations depuis Bruxelles. Je suis désolée de ne pas être là. Donc je vais faire un point sur les progrès au niveau des discussions sur le PDP. Diapo suivante, s'il vous plaît.

Depuis le lancement de ce PDP, et comme ça a été indiqué dans l'introduction de cette séance, nous avons décidé de formaliser la manière dont travaille le GAC en constituant un petit groupe ou une petite équipe spécifique du GAC. C'est la manière de se préparer aux discussions relatives à ce PDP. L'idée avec la création de ce groupe, c'était de suivre l'exemple d'autres groupes existants. L'idée, c'est de se réunir régulièrement, de collaborer. Gabriel et moi-même transmettons la position des membres du groupe de travail au PDP. Et comme il y a eu beaucoup d'échanges au niveau du PDP, nous avons considéré que la création de ce groupe était une bonne idée pour que les membres du GAC puissent pleinement participer aux discussions relatives à l'utilisation malveillante du DNS, sans pour autant utiliser toute la liste de diffusion du GAC. Pour ce faire, donc, à l'heure actuelle, nous avons 17 membres du GAC qui participent à ce groupe. Sachez que ce groupe est toujours ouvert à accueillir de nouveaux membres. Si vous voulez rejoindre ce groupe, faites-nous connaître votre intérêt et sachez que, très prochainement, nous allons nous retrouver avec une fréquence accrue. Diapo suivante, s'il vous plaît.

Comme Susan l'a déjà dit, le lancement du PDP a été décidé par le Conseil de la GNSO en décembre, et la première réunion du groupe sur le PDP s'est tenue il y a deux jours. Hier donc, on s'est réuni pour la première fois lors de l'ICANN 85. Le premier PDP se concentre sur la vérification des domaines associés, l'un des principaux éléments prioritaires identifiés dans le rapport publié en été dernier. Ensuite, PDP-2, sauvegardes pour un API pour les nouveaux clients. On ne

sait pas quand est-ce que cela va être lancé, et il y a l'obligation du GAC d'être constituée par quatre membres pleins, moi-même et Gabriel qui est le président également du CPWG et du FBI. Également, un participant des forces de police de l'Allemagne, Wolfgang, mais il n'a pas le droit de vote. Et on a Naum, de la police grecque qui participe également au PDP, mais en tant que suppléant, si jamais Gabriel ou moi-même ne pouvons pas participer. Donc il a un rôle de suppléant et il n'a pas droit d'intervention. Donc nous sommes un groupe assez fort, une petite équipe assez forte et nous avons une longue liste d'observateurs du GAC, ce qui est très, très utile.

Évidemment, la première réunion s'est tenue ici hier et puis, transparent suivant, nous allons voir tout ce que nous avons déjà abordé. Alors, l'idée de cette réunion de lancement à l'ICANN 85, c'était d'avoir des informations sur le calendrier des travaux. Alors, vous voyez que nous avons ici mis en exergue, en fait, les grands jalons de notre plan de travail, avec un rapport initial qui peut être entendu en février 2027, rapport final pour septembre 2027, et puis examen par la GNSO de ce rapport final en octobre ou novembre 2027. Et aujourd'hui, durant la troisième réunion, en fait, nous avons entendu quelques présentations d'experts sur le sujet, sur la manière dont les vérifications de domaine associées sont menées, avec un échange de meilleures pratiques et expression des problèmes plus préoccupants. Les informations les plus importantes à retenir de ce transparent ou de cette diapositive, c'est qu'il nous faudra vraiment apporter une contribution

précoce, justement, à la Charte d'ici le 20 mars 2026. Alors, c'est vraiment maintenant puisque l'ICANN 85 dure jusqu'à jeudi. Alors nous allons préparer la contribution précoce au sein de la petite équipe ou du petit groupe. Nous avons fait un Google Doc évolutif où les différents membres apportent leur contribution, et nous continuerons à travailler sur ce document au sein du petit groupe du GAC pour bien couvrir toutes les thématiques mises en exergue. Je vais peut-être passer la parole à Gab qui va rentrer dans le détail des prochaines étapes.

GABRIEL ANDREWS

Bonjour. Gabriel Andrews au micro. Est-ce qu'on peut passer à la diapo suivante? Eh bien, c'était la bonne. Donc voilà certaines des questions en fait, qui figurent dans la charte du PDP, et ce sont les questions auxquelles nous devons apporter des réponses. Comme Martina vient de le dire, notre date limite, notre échéance, c'est vendredi dans une semaine, c'est-à-dire le 20 mars. Donc nous avançons très, très rapidement dans le cadre de ce processus d'élaboration des politiques. Le président Paul McGrady, qui est là, vraiment nous mène à la baguette pour que justement nous soyons dans les temps. Mais c'est ce que nous avons demandé. Ce PDP doit être rapide et nous essayons de répondre rapidement à toutes ces questions. Et je voulais simplement vous signaler que nous anticipons de pouvoir, en fait, soumettre un projet de réponse dans le courant de la semaine prochaine. Vous n'aurez peut-être pas tout le temps dont vous bénéficiez d'habitude pour passer en revue ces réponses. Donc ce sont des thèmes qui vous intéressent.

Comme le disait Martina, participez au petit groupe, collaborez à l'élaboration et à la rédaction des réponses aux questions posées dans la charte. Diapo suivante.

Alors pour l'avenir, Martina avait bien dit que le prochain PDP a trait à l'accès aux API. Vous vous souviendrez que lorsque le rapport INFERMAL a été publié par le GAC, on parlait de différents attributs liés à l'enregistrement des domaines et les utilisations malveillantes constatées. Et on s'était dit, en fait, que l'utilisation d'API était le point de corrélation par rapport aux utilisations malveillantes le plus fort. C'est la raison pour laquelle nous voulons vraiment discuter de cette thématique, et nous anticipons un tout petit peu le travail qui va suivre sur les vérifications des domaines associés. Par ailleurs, le GAC, par le passé, a vraiment mis l'accent sur le fait qu'il nous fallait peut-être mettre l'accent sur des PDP plus ciblés, notamment pour couvrir les mesures de suivi et de prévention, en parlant aussi d'exactitude des données d'enregistrement, une transparence accrue dans les obligations de notification, politiques de consensus sur les utilisations malveillantes des sous-domaines. Nous savons que les sous-domaines sont utilisés très souvent en matière d'hameçonnage, et ça veut dire que, vous savez, des domaines peuvent avoir plusieurs sous-domaines. Il y a aussi le mécanisme de coordination centralisé pour les domaines qui sont créés à travers l'utilisation d'algorithmes de génération de domaine, ce qu'on appelle les DGA. Et il y a attaque par réseau zombie. Alors, voilà tous les éléments

qui ont été mis en avant par les membres du GAC et qui feront peut-être l'objet d'un travail d'analyse à l'avenir.

NICOLAS CABALLERO Eh bien, avant de passer la parole à Tomo, je vais peut-être demander à la salle s'il y a des questions. Je vois qu'il y a une demande d'intervention de la part de la Commission européenne en ligne. Gemma, vous avez la parole.

GEMMA CAROLILLO Merci beaucoup, Nico. Je ne prendrai pas beaucoup de temps. Je voulais simplement vous féliciter et féliciter tous les collègues du GAC qui apportent une contribution très importante à ce processus, un processus qui commence très, très bien. Et je voulais également dire, pour information, pour les membres du GAC et puis pour le président du PDP, nous encourageons en fait le groupe PDP à revoir la charte afin encore de raccourcir le calendrier. Pourquoi? La fin de ce processus, c'est dans un an et demi. Mais même pour le rapport initial, il faudra attendre l'année prochaine. Alors ça veut dire quoi? Ça veut dire qu'il faudra qu'on se réunisse une fois par semaine. Cela va mobiliser beaucoup de ressources. Nous avons d'autres thématiques de travail. Alors c'est vrai que le travail en fait ou, en tout cas, le mandat est très, très ciblé et il a fait l'objet d'un consensus. Donc, le calendrier est très serré et il est très encourageant également de voir que, en fait, les autres thèmes signalés par la GNSO vont être discutés au niveau de la méthodologie. Les thèmes qui ont été présentés par Gab sont déjà

une priorité pour nous d'ailleurs, en particulier les problèmes rencontrés en matière d'exactitude de données d'enregistrement ou encore la question de la transparence accrue pour les obligations en matière de notification. C'est très, très important pour nous.

NICOLAS CABALLERO Merci beaucoup, la Commission européenne. J'ai l'Inde qui demande la parole.

SUSHIL PAL Représentant de l'Inde au GAC. Félicitations à l'équipe dirigeante du GAC d'avoir vraiment engagé ces travaux. Je voulais simplement souligner à quel point il est important de travailler sur les autres domaines qui figurent sur la liste des priorités du GAC. Le suivi actif dans le cadre des mesures de prévention. Oui, nous devons nous centrer sur les mesures de prévention. Ce sont des mesures très, très importantes effectivement, surtout pour la validation concurrente des données d'enregistrement et des données des titulaires de noms de domaine. Alors, il ne faudrait pas surcharger la GNSO de travail. On essaie maintenant d'accélérer le processus, d'anticiper les événements. Alors, je sais que nous avons un calendrier à l'horizon 2027, mais nous voyons en fait que les cybercriminels exploitent l'anonymat, l'anonymisation. Nous avons vu en fait les résultats partagés par Devesh Tyagi en matière de méthodologie suivie en Inde. Pour répondre à la question du Sri Lanka, j'aimerais y répondre d'ailleurs : Que pouvons-nous faire

face aux titulaires de noms de domaine qui sont en dehors de notre domaine .IN? Par exemple, le fait est bien de réduire par exemple la période de validation. C'est également un problème. C'est une période de 15 jours. Alors tout avis du GAC à l'intention du conseil d'administration pour accélérer ce processus – je ne parle pas du PDP – serait le bienvenu. Cela nous permettrait de mieux contrôler également les titulaires de nom de domaine.

NICOLAS CABALLERO Merci beaucoup. Nous prenons bien note de cette proposition. À ce stade, je crois que je n'ai plus qu'à donner la parole à Tomo, qui va nous parler du réseau de mécanisme de notification de confiance avec Manju Chen. Tomo.

TOMORI MIYAMOTO Merci beaucoup. Est ce qu'on peut passer au transparent suivant, s'il vous plaît? Alors tout d'abord, revenons encore une fois à notre plan annuel et notre communiqué du GAC de Dublin, à l'ICANN 84. Nous avons arrêté une approche qui nous permettra de faire avancer les PDP, comme l'a dit Martina et comme l'a dit Gab. Et puis un autre axe de travail, c'est le renforcement des capacités, notamment un tutoriel pour les nouveaux membres du GAC. Nous accueillons 19 ou 20 nouveaux membres du GAC; donc il faut les former. Et puis, il est important de partager les meilleures pratiques qui peuvent contribuer à atténuer les utilisations malveillantes du DNS. Et comme on le voit au 4.4.7, il est important,

évidemment, de vraiment parler d'exemples de meilleures pratiques.

Alors, vous le reconnaissez peut-être à ce transparent. Voici en fait le cadre de l'autorité contractuelle de l'ICANN. C'est en fait une portée limitée. C'est donc l'encadré vert. La définition de l'utilisation malveillante du DNS est également limitée. On parle ici bien sûr de logiciels malveillants, de dévoiement, d'hameçonnage et encore de réseau zombi. Mais le processus est beaucoup plus large. On le voit par exemple par rapport à ce qu'on fait au Japon. Donc, on a besoin d'une certaine flexibilité. Que peut-on faire au-delà du champ de compétence de l'ICANN? Eh bien, ce que nous pouvons faire par exemple, c'est de créer un réseau de mécanismes de notification de confiance. Et sans plus attendre, je vais passer la parole à Manju Chen qui va nous présenter le réseau de mécanismes de notification de confiance – TNN pour l'acronyme en anglais.

MANHU CHEN Bonjour, je m'appelle Manju Chen, directrice de politiques du réseau de mécanismes de notification de confiance (TNN). Merci beaucoup. Voilà, c'est une petite introduction. Donc tout le monde nous a déjà fait un état des lieux. Alors sans plus attendre, parce que j'aimerais répondre surtout à vos questions, passons au transparent suivant. Vous avez déjà entendu notre présentation lors de l'ICANN 84 à Dublin, dot Asia et TWNIC ont présenté leur réseau. Ça a été un tout petit peu notre point de départ, car il s'agit

là de deux mécanismes de notifications. Donc nous avons pris le même concept, mais nous avons passé des... Nous pensons que les accords bilatéraux sont trop lents, donc nous voulons vraiment construire un réseau. Et si vous faites partie du réseau, vous êtes un mécanisme de notification de confiance. Alors, cela veut dire que tous les intermédiaires peuvent avoir confiance en vous parce que vous faites partie de ce réseau. Si vous êtes un intermédiaire, vous savez que tous les avis que vous recevez sont du TNN, et donc qu'ils sont validés et de confiance. Alors nous nous limitons pour l'instant aux ccTLD et la région APAC. Alors c'est vrai que beaucoup de ccTLD ont déjà manifesté leur intérêt au sein de la région APAC et nous ont signalé qu'ils voulaient rejoindre le réseau, mais nous parlons également à beaucoup de registres de gTLD au niveau international. Bon nombre sont très, très intéressés par ce réseau, et c'est la grande différence entre nous, dirais-je, et d'autres initiatives, dot Asia et TWNIC. Alors, ce que les registres et les bureaux d'enregistrement ont déjà dit lorsqu'ils ont manifesté leur intérêt, en fait, nous voulons en fait couvrir plus de 200 TLD. Ça veut dire 60 noms de domaine. Si l'on s'en tient aux manifestations d'intérêt que nous avons reçues, nous recevons beaucoup d'attention aussi de la part de ces acteurs qui veulent devenir des mécanismes de notification de confiance. Mais pour le moment, nous nous centrons sur les intermédiaires, les opérateurs de registres et les bureaux d'enregistrement également. Car si nous n'avons pas d'intermédiaire, à qui allons-nous envoyer les avis? Et

c'est la raison pour laquelle les intermédiaires sont un petit peu notre priorité.

Donc, quel était le problème que nous avons identifié : s'acquitter de transfert de coûts injuste en cas d'attaque d'hameçonnage? Ils n'ont pas le temps ni l'expérience pour y faire face. Donc, ils sous-traitent cela à des prestataires sur le service qui font ce service sans avoir autorité pour retirer aucun domaine, parce qu'ils ne sont pas opérateur de registre ni bureau d'enregistrement. Ce qu'ils font, c'est simplement envoyer des notifications aux intermédiaires à titre gratuit. Et parce que c'est gratuit, ils en envoient énormément et ils sont envoyés pour envoyer des notifications. Ils ne sont pas payés pour s'assurer de la qualité. Et l'intermédiaire de l'autre côté a à voir avec cette responsabilité sociale et avec ce genre de choses. Donc ils ne sont pas tenus pour responsable en cas de problème. Donc, c'était simplement un coût et aucun encouragement. Donc, pour réduire les coûts, on essaie de faire en sorte que l'on réduise ces coûts. Donc, on était les uns et les autres tout aussi mécontents face à cette situation.

Et outre cela, je pense que la plupart d'entre vous connaissent bien cette situation où vous êtes submergés d'attaques et de plaintes, d'attaques de la part de vos concitoyens, et vous sentez que l'ICANN n'agit pas suffisamment à ce niveau-là, que les choses devraient aller plus vite. Mais c'est simplement pour vous montrer que nous comprenons que les gouvernements sont sous pression, que leurs besoins restent sans réponse et qu'il faut trouver le moyen de faire face à cette situation. Donc, tout le monde accuse

les uns les autres d'être à l'origine de ce problème. Donc, quelle est notre mission? Nous voulons réduire les coûts et les risques pour les intermédiaires, pour qu'ils se sentent plus à l'aise pour envoyer des pré-demandes. Et comment est-ce qu'on procède? En améliorant la détection et le retrait. Et pour cela, on améliore la qualité et l'exactitude de la requête pour que ces intermédiaires et la confiance nécessaire pour procéder au retrait. Et on implique également les gouvernements parce que vous êtes important. C'est la raison pour laquelle je suis ici. Je veux vous inviter à nous rejoindre, à rejoindre notre réseau pour qu'on puisse ensemble travailler.

Et d'ailleurs, j'ajouterai que notre réseau vise à être un processus multipartite. On veut inviter tout un chacun à y participer. Et si vous êtes intéressés, je partagerai avec vous le document politique pour que tous les membres du GAC en aient connaissance et je serai ravie d'entendre votre opinion. Et enfin, nous savons que cela n'a pas lieu uniquement au niveau du DNS. À l'ICANN, nous avons un champ d'application très limité au niveau du DNS. Mais pour lutter réellement contre les abus dont tout le monde de l'Internet, nous avons besoin d'une coopération entre tous les secteurs. Donc, voilà les objectifs que nous voulons atteindre.

Les personnes à l'origine de la notification devront vérifier et également vérifier que ce mécanisme de notification est réellement authentifié. Et une fois qu'ils sont authentifiés et qu'ils sont considérés comme faisant autorité, alors on considère qu'ils sont dignes de confiance. Et je ne vais pas vous donner plus de

détails à ce niveau-là. Enfin, on veut réduire les risques juridiques, en particulier pour les intermédiaires, pour qu'ils puissent se sentir plus à l'aise au moment de prendre des actions. Donc, nous voulons créer une chaîne de contrats qui permettra aux intermédiaires de se sentir plus sûrs lorsqu'ils entreprennent quelque action que ce soit et lorsqu'il retire ou procède au retrait des noms de domaine.

Cette personne qui envoie des notifications dignes de confiance devra répondre à toute une série de conditions d'exigences. Également. La requête devra faire l'objet d'une vérification, on en a parlé, ne devra pas être automatique et devra être précise. Précise, ce n'est peut-être pas le bon terme. Ce qu'on veut dire, c'est qu'il faut se conformer à une diligence raisonnable pour s'assurer qu'il y a une vérification et une authentification. C'est comme ça qu'on s'assure que le mécanisme est digne de confiance.

Ensuite, les intermédiaires jouent un rôle à ce niveau-là, aussi au niveau des forces de l'ordre, et je vais vous expliquer leur rôle dans un instant. Toutes les notifications sont codifiées et standardisées pour éviter tout problème. Et en raison de cette chaîne de contrat et chaîne de confiance au niveau des intermédiaires, les intermédiaires pourront effectuer des priorités au niveau des demandes qui leur parviennent. Donc voilà comment nous comptons nous y prendre pour inverser le transfert de coûts. Et je vais vous expliquer maintenant comment cela va fonctionner pour les forces de l'ordre. Diapo suivante, s'il vous plaît.

Donc les forces de l'ordre. Nous abordons la chose un peu différemment parce qu'une exigence en termes de mécanisme de notification digne de confiance pourrait s'avérer très difficile pour les forces de l'ordre. Et si on donne la priorité à certains pays par rapport à d'autres, ce ne serait pas juste au niveau des forces de l'ordre. Alors je n'ai pas suffisamment de temps pour rentrer dans plus de détails. Mais il faut répondre à deux conditions. D'abord, si vous voulez rejoindre TNN, il faut reconnaître toutes les notifications qu'il va falloir traiter. Et en raison également du problème dont je vous ai parlé et en raison de cette volonté d'inverser le transfert de coûts, il faut prévoir une indemnisation pour TNN et les intermédiaires. Donc ça, Tomo en a déjà parlé. On veut impliquer tout le monde dans ce processus. Ça commence déjà à décoller à l'ICANN, mais à l'avenir, on veut faire participer tous les acteurs du secteur, du secteur des télécommunications et autres.

NICOLAS CABALLERO Merci beaucoup. Et malheureusement, nous n'avons plus le temps pour une séance de questions-réponses. Je suis désolé. Vous pouvez contacter Manju et son équipe par la suite. Directement et sans plus attendre, je vais céder la parole à Tomo pour quelques considérations ultimes et suggestions ultimes de la part du GAC.

TOMORI MIYAMOTO Merci beaucoup. Diapo suivante. Je vais vous présenter quelques aspects à prendre en considération. Nous avons trois piliers.

D'abord, le développement des ADC, de la politique ADC, vérification des domaines associés. Ensuite, l'avenir du développement de politiques relatives à l'utilisation malveillante du DNS, possibilité d'efforts futurs et collaboration pour le PDP-2 et d'autres lacunes identifiées dans le rapport final. Et troisième, possibilité d'efforts futurs et collaborations futures pour renforcer tout effort visant à atténuer l'utilisation malveillante du DNS. Voilà, donc je vous laisse intervenir si nous en avons le temps et je me tiens à votre disposition si vous avez des suggestions.

SUSHIL PAL

Représentant de l'Inde au GAC. Oui, un commentaire par rapport à ce communiqué de Mumbai. Je vous exhorte à insister sur le mécanisme de prévention pour réduire les abus au niveau des enregistrements des noms de domaine.

SUSAN CHALMERS

Je pense que par rapport à cette suggestion, on a le PDP actuel et les PDP futurs. Peut-être, que dans cette section, ça pourrait bien s'inclure. Je crois qu'il y a un élément qui a été inclus dans le rapport thématique. Et à la GNSO, nous avons entendu qu'il y a une méthodologie qui est développée pour établir des priorités au niveau de différents domaines de travail futur. Donc, ça pourrait être une section dans laquelle on pourrait inclure ce texte.

SUSHIL PAL

Oui, je crois que c'est effectivement mentionné, mais je pense que c'est apparu comme une question d'importance dans le dernier communiqué également. Et c'est quelque chose qui est tangible, il me semble. Si on essaie d'accélérer le processus PDP pour les noms de domaine associés – et nous en attendons les résultats d'ici un an, alors c'est un excellent moyen de montrer que cette mesure de prévention peut accomplir beaucoup plus que ce qu'on peut s'attendre à avoir de la part d'un processus quelconque PDP ou un processus lié à des domaines associés. Donc si on peut attendre, très bien, Mais je pense que cette mesure de prévention, ça peut être un avis au conseil d'administration pour opérer un amendement contractuel dont on a grandement besoin.

NICOLAS CABALLERO

Merci l'Inde. Merci les États-Unis. On aura le temps d'en parler lors de la séance de rédaction du communiqué. Ne vous inquiétez pas. Merci beaucoup. Nous n'avons plus de temps. Le mot de la fin peut-être pour Susan. Susan, allez-y.

SUSAN CHALMERS

Merci. Donc, depuis plusieurs réunions maintenant, les responsables thématiques du GAC ont invité les pays et les représentants ccTLD de venir nous faire une présentation, et je pense qu'on devrait avoir des archives de toutes ces présentations si intéressantes. Mais pour ceux d'entre vous qui êtes nouveau dans ce processus et sur cette thématique, il y a un processus de politique ccTLD. Ensuite, il y a l'espace gTLD. Deux espaces très

différents l'un de l'autre et uniques en soi aussi. Dans ce processus multipartite, il y a des pratiques nationales et, là encore, c'est un processus à part qui évolue et qui est informé par le point de vue de la communauté. Donc, pour ceux d'entre vous qui êtes nouveaux dans cet espace, je voulais m'assurer que vous voyez bien la différence entre ces deux espaces. Voilà tout ce que je voulais dire. Il ne me reste plus qu'à vous remercier tous de votre participation.

NICOLAS CABALLERO Merci beaucoup. L'Inde, c'est une ancienne main? Très bien, donc nous allons lever la séance. Merci beaucoup, Devesh. Merci Manju, Tomo, Susan, bien sûr, et Gabriel. Nous nous retrouvons demain à 9 h pour la réunion avec l'ALAC. Merci beaucoup! Profitez bien de votre café et soirée. Merci.

[FIN DE LA TRANSCRIPTION]