ICANN68 | Forum de politiques virtuel – GAC : atténuation de l'utilisation malveillante du DNS (avec le PSWG) (2/2)
Mardi 23 juin 2020 – 16h30 à 17h30 MYT

GULTEN TEPE : Nous allons commencer les enregistrements.

Bonjour, bon après-midi et bonne soirée à tous. Je suis Gulten Tepe de l'équipe de soutien au GAC de l'ICANN et je suis la gestionnaire de la participation à distance de cette séance. Bienvenue à la séance du GAC sur l'atténuation des risques liés à l'abus du DNS mardi 23 juin à 16h30 fuseau horaire de Kuala Lumpur.

En raison des bombardements Zoom qu'on a subis, toutes les séances seront tenues en mode webinaire. Dans les séminaires webinaire, pour pouvoir parler, il faut être identifié en tant que paneliste. Pour qu'on puisse le faire de manière automatique, les membres du GAC doivent entrer dans la salle Zoom avec leur adresse courriel du GAC ou bien avec un lien individuel qui leur aura été distribué par la liste de diffusion du GAC. C'est pourquoi il est important de vérifier vos courriels et de chercher un courriel disant « liste de participants » et « courriel pour pouvoir entrer dans la séance ». Ma collègue Julia Charvolen vous montre le courriel sur l'écran.

Si un membre du GAC ne peut pas lever la main ou voir le nom des autres panelistes, lui ou elle devra rejoindre la séance à l'aide du lien qui lui aura été envoyé. Une fois que vous êtes reconnu comme

paneliste dans la salle Zoom, vous allez avoir droit aux différentes fonctionnalités que vous avez habituellement dans une salle Zoom. Nous vous prions de mettre le mot « GAC » à côté de votre nom. Si vous utilisez une adresse courriel différente, vous n'aurez pas la possibilité d'être paneliste et vous n'allez pas avoir accès à toutes les fonctionnalités.

Si vous souhaitez poser des questions, veuillez les taper dans le chat en ajoutant au début et à la fin de votre phrase le mot « question » ou « commentaire ». Merci d'être bref.

Le service d'interprétation simultanée sera disponible pour le GAC dans les six langues des Nations Unies plus portugais à travers à la fois Zoom et la plateforme d'interprétation simultanée à distance de Congress Rental Network. Les participants sont encouragés à télécharger l'application et suivre les indications qui sont données sur le chat de Zoom ou dans la page du programme de l'ICANN68. Votre micro sera en muet pendant toute la séance à moins que vous souhaitiez prendre la parole.

Si vous souhaitez prendre la parole, veuillez lever la main. On vous donnera permission pour activer votre micro. Merci d'activer votre micro à ce moment-là et lorsque vous parlez, assurez-vous d'avoir mis en muet tous les autres dispositifs, y compris l'application de Congress Rental Network. Dites votre nom clairement et la langue dans laquelle vous allez parler. Parlez clairement et à un débit raisonnable pour que vos propos puissent être interprétés correctement. Nous avons un service de transcription en temps réel.

Pour y avoir accès, vous devez cliquer sur le lien fourni dans le chat du Zoom.

Finalement, cette séance, comme toutes les autres activités de l'ICANN, est régie par les normes de conduite requises par l'ICANN. Pour référence, vous trouverez le lien vers cette politique sur le chat.

Maintenant, je vais donner la parole à la présidente du GAC, Manal Ismail. Manal, vous avez la parole.

PRÉSIDENTE MANAL ISMAIL : Merci beaucoup Gulten.

Bonjour à tous. Bienvenue à cette nouvelle séance. J'espère que vous avez profité de la pause. C'est notre deuxième séance consacrée à l'utilisation malveillante du DNS. Nous en avons eu une hier. C'est notre deuxième et dernière séance à ce sujet.

Cette séance va durer une heure et elle sera dirigée par les coprésidents du groupe de travail PSWG, qui feront également une synthèse de ce qui a été abordé lors de la séance plénière d'hier. Je vais donc donner la parole à Laureen Kapin. Cathrin, est-ce que vous allez commencer ? Cathrin, vous avez la parole.

CATHRIN BAUER-BULST : Merci à tous. Merci à toutes les personnes présentes. On a déjà 199 personnes ; c'est vraiment un sujet qui motive les gens.

Je m'appelle Cathrin Bauer-Bulst. Je travaille à la Commission Européenne et je suis l'une des coprésidentes du groupe de travail du GAC sur la sécurité publique. Comme Manal l'a annoncé, Chris et Laureen seront avec moi pour diriger cette séance, et je vais commencer par passer en revue l'agenda.

Tout d'abord, comme on l'a déjà dit, nous voulons faire une synthèse sur la séance plénière que nous avons eue hier et parler des moments forts de cette séance et de ces discussions. Ensuite, nous allons continuer avec la discussion qu'on a commencée lundi pour partager un petit peu d'information sur l'expérience de la pandémie de la covid-19. Nous voulons aborder la question de la réponse à la covid-19, mais la question de la fraude de manière plus générale.

Nous voulons partager des informations sur les contributions des gouvernements pour éduquer les consommateurs pour s'assurer que les autorités sont en mesure de jouer leur rôle dans l'écosystème pour prévenir les arnaques et les abus du DNS.

Ensuite, nous avons le temps, nous voudrions engager une discussion. Il y a eu quelques questions hier et nous sommes bien entendu ouverts à continuer cette discussion car il y a un certain nombre de points par rapport auxquels le GAC doit encore débattre, notamment en ce qui concerne les nouvelles étapes.

Finalement, nous voudrions passer en revue quelles sont les séances consacrées à l'utilisation malveillante du DNS dans cette réunion de l'ICANN89.

Hier, nous avons eu une séance plénière intercommunautaire consacrée à l'utilisation malveillante du DNS qui a été divisée en deux parties différentes. La première partie a été consacrée au développement depuis l'ICANN66 à Montréal – c'était la dernière réunion présentielle que nous avons eue ; après, il y a eu l'expérience avec la covid-19. Et la deuxième partie a été consacrée aux prochaines étapes possibles pour la communauté de l'ICANN. Je vais donc vous parler des moments forts des discussions. Et je vais donner la parole à Chris Lewis-Evan qui va nous parler un petit peu de la séance d'hier.

Tout d'abord, nous avons entendu des informations très intéressantes de la part des parties contractantes qui nous ont raconté quel a été leur travail, notamment en ce qui concerne la définition de l'utilisation malveillante du DNS. Nous avons connu quels sont leurs efforts. Nous avons pu voir que la définition tient compte d'un certain nombre d'arnaques, hameçonnages, logiciels espion. Il y a une définition de base sur laquelle nous avons commencé à débattre. Il y a d'autres définitions de l'utilisation malveillante du DNS sachant que les parties contractantes ne se sont pas mises d'accord par rapport à une définition, mais il s'agit déjà d'un bon point de départ.

Les opérateurs de registre et bureaux d'enregistrement nous ont raconté quels étaient leurs efforts pour atténuer ces risques, notamment à travers de meilleures pratiques. Et il y a eu des orientations, des directives par rapport à des efforts spécifiques qui ont été entrepris pour atténuer certains types d'abus. Cela a été fait

par les opérateurs de registre de Google pour combattre les abus du DNS.

Les meilleures pratiques ont été également abordées sous forme des actions des forces de l'ordre. Et nous avons également entendu de la part du groupe de travail des utilisateurs commerciaux quelle était leur expérience par rapport à la fraude. Leur expérience a été très intéressante. Entre autres, il y a eu des statistiques par rapport aux noms de domaine liés à la covid-19 qui était 15 % plus susceptibles de faire l'objet d'arnaque ou de fraude. Donc ils nous ont raconté un petit peu ce qu'ils font pour pouvoir lutter contre ce type de risque. Il y a un phénomène important également au niveau des bouleversements qui ont lieu dans le monde, et cela également augmente les risques pour les citoyens.

Ensuite, Laureen nous a partagé l'expérience de la Commission fédérale américaine du commerce. Elle en reparlera ici. Puis, on a parlé également des prochaines étapes pour la communauté de l'ICANN.

Un point important de cette séance qui a été partagé, c'est la nécessité d'avoir des données plus précises. Les registres ont dit qu'il n'y avait pas de définition exacte et qu'il fallait également collecter des informations. On a parlé des normes, des standards et du fait qu'il n'y a pas suffisamment de données pour pouvoir documenter de manière précise ces actions pour les parties contractantes.

Il y a également la nécessité de construire des partenariats entre les bureaux d'enregistrement et les opérateurs de registre. Ils ont également partagé leurs expériences avec les forces de l'ordre et cela a été une expérience positive. Et il y a eu également des témoignages par rapport à des actions conjointes avec les gouvernements et les forces de l'ordre. Tout le monde a partagé des meilleures pratiques et des informations et il a été question de voir comment ces meilleures pratiques et ces expériences pourraient être partagées de manière plus large pour pouvoir mieux les diffuser.

Beaucoup de personnes ont signalé le fait qu'on ne repart pas de zéro. Il y a un bon travail de base qui a déjà été fait, cela comprend le cadre. Un représentant d'un centre a mis l'accent sur la mise en place de vérifications par les ccTLD qui ont permis de vérifier l'exactitude de certaines données et cela s'est révélé très important pour pouvoir lutter contre les abus.

Le SSAC a également partagé son expérience avec un nouveau cadre pour pouvoir également fournir davantage de directives et d'orientations.

Il y a eu des difficultés qui ont été signalées également pour ce qui est de l'application de certaines règles. Notamment, ici, il faut noter le fait que certains engagements ont été difficiles à faire appliquer de la part de la conformité contractuelle.

Il y a également une discussion assez vive et des commentaires. Disons que cela ne valait même pas la peine d'investir dans des règles

puisque ces règles n'allaient pas être appliquées dans l'écosystème. Donc il est très difficile de pouvoir faire en sorte que ces règles puissent être appliquées.

On a parlé également des revendeurs. C'est une autre question qui intéresse le GAC car il peut être très facile de pouvoir bouger d'une conséquence à l'autre dans l'écosystème de l'ICANN. Et c'est vraiment un sujet sur lequel il vaut la peine de s'y pencher.

Il y a eu également des initiatives qui ont été commentées, comme le nouveau système d'encouragement au PIR pour les bureaux d'enregistrement, pour qu'ils mettent en place des mesures anti-abus et pour qu'ils mettent en place également une vérification de performance et cela, pour les opérateurs de registre et les bureaux d'enregistrement.

Ensuite, il y a un nouveau projet de la part de l'ICANN qui cible les renseignements en matière de menaces. Apparemment, j'ai parlé trop vite pour les interprètes. L'ICANN a créé un système de veille qui identifie des menaces. Ce système pourrait être utilisé de manière plus large dans l'avenir. Ici, je reviens à la question de savoir comment collecter et diffuser une nouvelle pratique, comme c'est le cas par exemple des bonnes pratiques de l'OCTO. L'idée, comme l'a dit David Conrad, c'était que ces efforts d'atténuation soient mieux compris et servent à faire appliquer les règles.

Pour ce qui est des réflexions par rapport à cela, c'était très bien de voir ces nouveaux efforts qui sont très prometteurs et ce mouvement

qui se met en place pour atténuer ce type de risques. En même temps, il ne faut pas oublier tout ce qu'on a déjà identifié comme solutions, comme par exemple la vérification de données, les données d'enregistrement.

En 2017, une étude qui a été menée a montré qu'il y a énormément de cas d'abus. Et d'autres études postérieures ont parlé également du RDS, du SSAC.

Je voulais également revenir à ce que Gabriel a déjà dit : 65 % des enregistrements ont été faits par des services d'anonymisation et d'enregistrements fiduciaires. Et il est très difficile de ne pas utiliser ces services, qui sont très promus. Ici, nous n'avons pas encore une politique en place, malgré le fait qu'on sait que le EPDP ne va pas se pencher sur cette question. Cela constitue une difficulté importante car les procédures peuvent prendre des semaines pour voir qui est derrière un service d'anonymisation et d'enregistrements fiduciaires et cela rend les enquêtes plus compliquées.

Nous saluons les nouvelles idées. Il y a beaucoup de travail qui a déjà été fait. Donc on ne repart pas à zéro et on doit se baser sur ce qui a déjà été fait. On aura l'occasion de discuter de cela dans une minute. Mais pour cela, je vais demander à Chris de partager ses impressions vis-à-vis de cette séance intercommunautaire avant d'entrer dans les détails concernant nos expériences sur la gestion de la crise.

PRÉSIDENTE MANAL ISMAIL : Excusez-moi de vous interrompre Cathrin, Laureen et Chris, mais je voudrais savoir si vous comptez répondre aux questions à la fin de la séance, parce que je vois déjà qu'on a une question dans la section des questions et réponses, mais je ne suis pas sûre de la procédure que vous voudriez suivre.

CATHRIN BAUER-BULST : Peut-être qu'on pourrait attendre jusqu'à la fin de la présentation et répondre aux questions pendant la discussion à la fin.

PRÉSIDENTE MANAL ISMAIL : Très bien, merci.

CHRISTOPHER LEWIS-EVANS : Merci. Je vais demander à ce que l'on passe à la diapositive suivante.

Je suis Chris Lewis-Evans de l'Agence de criminalité nationale du Royaume-Uni (*Nation crime agency*). Je vais vous présenter quelques points saillants de la séance intercommunautaire. Et je signalerai tout de suite l'impact sur le public, sur les consommateurs et sur les utilisateurs finaux du système du DNS et spécifiquement l'échelle de ce que l'on a vu depuis notre service public de protection.

Lors de la séance intercommunautaire, Laureen a partagé des diapositives qui était très bien faites. Je vous conseille de voir l'enregistrement si vous n'avez pas suivi sa présentation hier. Mais il me semble qu'il est fondamental de dire avant tout qu'il y a beaucoup

de pays au monde desquels la cybercriminalité est l'un des délits les moins signalés en termes généraux. Dans le cadre de la covid-19, nous avons bien sûr vu énormément de statistiques. Il est difficile d'analyser les statistiques et de faire des comparaisons parce qu'il y avait tellement peu de signalements avant la pandémie.

Dans cette première diapositive que je voulais partager avec vous la période entre janvier et la date actuelle, à peu près. On y voit la quantité de plaintes reçues par la FTC, la *Federal Trade Commission* des États-Unis et vous voyez à droite en bas, c'est à la mi-mars que la quantité de plaintes a commencé à augmenter et ce, considérablement. Et il y a eu une augmentation incroyable tout au cours de cette période.

La plupart de ces signalements portaient sur les achats en ligne. C'était la première catégorie. Et la deuxième portait sur les voyages et nécessitait des besoins de programmation de vacances ou autre type de fraudes. Pour moi, ici le bilan, la leçon est la quantité de signalements. Et on ne sait pas si c'est en raison du fait que les gens ont commencé à informer de ces cas de cyberdélit et d'en informer les entités gouvernementales ou si c'est parce qu'il y a eu beaucoup plus de cas.

Dans l'espace du DNS, peut-être, c'est le cas parce que les gens ont commencé à se pencher sur la manière d'informer de tous ces abus. Lors de la séance intercommunautaire, il a été dit – comme d'ailleurs cela a été déjà dit lors des séminaires en ligne préparatoires à l'ICANN68 – que l'espace des noms de domaine et les noms de

domaine qui ont été enregistrés au cours de cette période étaient nombreux, mais qu'il n'y avait qu'une très petite proportion qui enregistrait ses noms de domaine à des fins malveillantes.

Or, comme vous le voyez sur la diapositive que vous avez à l'écran en ce moment, cela représente énormément de dommages pour les personnes, c'est très nuisible aux utilisateurs et l'impact est énorme pour les utilisateurs. Comme la communauté l'a identifié lors de l'ICANN66 et de l'ICANN67, l'abus du DNS est un véritable problème et il nous faut des solutions pour pouvoir arrêter ces préjudices.

Ce que vous voyez marqué avec un cercle rouge en haut de la diapositive montre les méthodes utilisées pour le recueille des données.

Donc le troisième point est lié à la quantité de méthodes de contact. Pour les deux cas, c'est lié au DNS, que ce soit pour un site web ou pour un DNS associé à une adresse courriel, et on voit dans les deux cas qu'on a à peu près les mêmes quantités, elles sont presqu'exactement les mêmes. Et les autres formes de contact en fait représentent toutefois une perte monétaire, économique.

Depuis le 23 mars, nous avons eu un total de plus de 16 millions £ en fraude. Il est intéressant de savoir que ces statistiques représentent des victimes qui dans un quart des cas, donc 25 %, étaient des gens étaient entre 18 et 26 ans. Lorsqu'on parle des achats en ligne par exemple, en général, on assume que ce sont des personnes qui ne sont pas habituées à la technologie ou qui sont plus âgées. On ne

s'attendrait pas à avoir des victimes entre 18 et 26 ans. Donc on continue d'apprendre à chaque fois quelles sont les méthodes utilisées et voit de plus en plus que tout le monde peut faire l'objet d'une telle menace. Donc 16 millions £ était le montant qui venait de ces fraudes. On a eu 2 378 victimes qui ont perdu 7 millions £ en raison d'attaques liées au coronavirus. Dans le cas du Royaume-Uni, on a des données jusqu'au 12 juin et c'est jusqu'à cette date qu'on a vu ces 7 millions £.

Les cas d'abus dans le contexte de la covid-19 ne se sont peut-être pas concentrés sur les noms associés à la covid-19 ou au vaccin ou autres. Or, il existe toutefois des cas d'abus et l'impact que cela a sur le public est très élevé. Et pendant une pandémie, vous savez, on sent beaucoup plus ce type d'attaques. On voit donc qu'il est vraiment nécessaire que l'on se penche sur ce type d'abus et que l'on trouve des solutions.

Avec ce, je vais recéder la parole à Laureen, je pense, puis on discutera ensemble de la manière de générer des changements possibles.

LAUREEN KAPIN : Merci Chris.

On avance à la diapositive suivante.

Je voulais souligner que pour aborder les cas d'abus du DNS, nous avons certaines mesures que nous pouvons prendre dans l'univers de l'ICANN et en particulier, pour nous assurer qu'il y ait des obligations

suffisamment fortes pour empêcher que ce type d'activités exploitent le DNS.

Nous avons donc la possibilité de coopérer en tant que gouvernement. Nous travaillons en collaboration avec les parties privées tels que les opérateurs de registre et les bureaux d'enregistrement pour remédier à ce type de comportement lorsqu'il est identifié.

Mais il y a un autre outil très viable qui est celui de l'éducation des consommateurs. Dans notre rôle en tant que gouvernements, nous avons énormément de travail à faire dans la sensibilisation du public, les utilisateurs finaux eux-mêmes et les gens qui utilisent l'internet pour leurs transactions, pour leurs affaires, pour communiquer. Et surtout pendant la pandémie, c'était un outil essentiel pour la communication de nos populations. Nous en tant que gouvernements pouvons essayer de réduire les abus de DNS à travers cette possibilité de leur communiquer comment ils peuvent eux-mêmes se protéger de ce type d'attaques.

Je voulais donc vous donner un petit aperçu de ce que fait le gouvernement des États-Unis au niveau de nos utilisateurs finaux et de leur éducation et spécifiquement ce qu'a fait mon agence, la FTC, qui est la principale agence de protection des consommateurs aux États-Unis, la Commission fédérale du commerce.

Il y a des documents sur le coronavirus puisque c'est le sujet du moment qui génère le plus d'intérêt public et le plus de préoccupations. La FTC a donc dédié une partie de son site web à des

questions liées au coronavirus. Vous pourrez le consulter vous-mêmes à travers ftc.com/coronavirus. Vous verrez qu'il y a différents onglets informatifs à consulter dans cette page qui pourraient vous intéresser. Dans le premier onglet, on a des informations pour le consommateur.

Lorsqu'on pense à la FTC, on pense aux consommateurs. Mais on a également un deuxième onglet qui est consacré aux sociétés, aux entreprises. On les oriente vis-à-vis de la manière de se protéger contre ces arnaques et de maintenir l'intégrité de leurs transactions avec le public.

Pour les forces de l'ordre, on a un troisième onglet.

La FTC a été très active dans l'envoi de lettres de mise en garde aux compagnies, surtout aux entreprises qui font de la publicité sur internet et surtout pour celles qui offrent des produits ou des services qui n'ont pas de fondement, qui sont censés par exemple guérir le coronavirus ou vous protéger du virus. Il y a des ressources et j'en parlerai dans un moment.

Mais il est important de remarquer sur cette diapositive – puisque Chris parlait des plaintes – que la FTC reçoit des plaintes des consommateurs de partout dans le monde. Et dans notre site web, si vous accédez à ftc.com, dès la page d'accueil, vous verrez très clairement comment signaler un cas d'escroquerie ou d'arnaque. Diapositive suivante.

Voici des ressources qui sont disponibles sur notre microsite dédié au coronavirus : comment éviter les arnaques. Ces informations sont

disponibles à travers des documents visuels mais il y a également une vidéo. Il y a l'impact financier du coronavirus – on sait qu'il y a énormément de gens qui ne peuvent plus faire leur travail, qui ne reçoivent plus de salaire – et les données de plaintes. Ce sont des informations publiques qui sont non seulement disponibles aux fins informatives mais si vous êtes un gouvernement ou une agence gouvernementale ou une organisation qu'elle qu'en soit le type qui souhaite utiliser ces informations, il est facile de pouvoir saisir ces documents et d'y ajouter votre logo. On n'a pas de documents qui soient propriétaires mais plutôt, on vise à ce que tout le monde puisse utiliser ces matériaux et les transmettre. Diapositive suivante.

Ici, vous voyez un document d'information que nous avons pour les consommateurs : rester calme et éviter les fraudes liées au coronavirus. Nous essayons de faire en sorte que les messages soient faciles à comprendre. Par exemple, faites attention, ignorez toutes les offres de vaccin ou de test de dépistage parce qu'il n'y en a pas encore, parce que c'est une méthode qu'ils utilisent pour vous contacter par exemple, les appels automatisés fait par des machines. Faites attention à des courriels de hameçonnage ou à des textos. Et essayez d'éviter et recherchez bien avant de faire un don.

Pour ceux qui préfèrent les vidéos, nous avons également des vidéos préparées pour les consommateurs qui abordent des points de base. Nous essayons donc de communiquer les informations les plus importantes aux consommateurs.

Nous encourageons les gens intéressés à ces questions à visiter notre site web. Nous serons ravis de partager ces informations avec tous ceux qui pourraient en bénéficier, et je pense que c'est tout le monde.

CATHRIN BAUER-BULST : Merci Laureen. Je voulais signaler que des efforts similaires ont eu lieu dans d'autres pays. Par exemple, je voulais partager l'exemple de Europol où des efforts sont faits pour aider les consommateurs à se protéger. Comme vous le voyez sur l'écran, vous voyez la page vers le site d'Europol qui collecte énormément d'informations, aussi bien pour les consommateurs que pour les forces de l'ordre et les agences d'application de la loi.

Pendant la crise de la covid-19, Europol a abordé deux pistes de travail pour conseiller non seulement les consommateurs mais aussi les décideurs politiques et les forces de l'ordre. Dans cette première piste, Europol a sorti une série de rapports par rapport à la pandémie qui ne se limitaient pas uniquement à l'abus du DNS mais qui étaient un peu plus larges. Vous voyez qu'il y a eu des développement par rapport à d'autres domaines : violence domestique, abus sexuels. Toutes ces questions ont été abordées du point de vue de rapports qui étaient adressés aux consommateurs et au public, mais aussi aux forces de l'ordre avec des perspectives stratégiques pour les forces de l'ordre et leurs partenaires. Ensuite, on a également ciblé les décideurs politiques pour leur fournir des considérations stratégiques dont ils devraient tenir compte avant de prendre des décisions.

Dans une deuxième piste de travail, Europol prépare du matériel éducatif pour les entreprises. L'approche est celle d'essayer de garder une réputation de source d'informations fiables. Donc pendant cette crise, l'idée, c'était de faire en sorte que les autorités puissent rester des sources d'informations fiables, ce qui s'avérait difficile parce que c'était difficile pour les utilisateurs de trouver des sources d'informations fiables auxquelles ils puissent faire confiance pour trouver des informations qui soient vraies. Donc Europol a mis à disposition ce matériel. On passe à la diapositive suivante.

Je ne vais pas rentrer dans le détail. Le site ressemble un petit peu à celui de la FTC, mais vous voyez un petit peu quels sont les sujets les plus importants sur lesquels nous nous sommes concentrés pour donner des informations fiables à travers des schémas faciles à comprendre dans plusieurs langues parce que comme vous le savez, dans l'Union européenne, on a 22 langues officielles, donc ces informations ont été distribuées dans plusieurs langues. Diapositive suivante.

Je voulais mentionner une autre piste de travail d'Europol. J'ai dit avant que les bureaux d'enregistrement avaient rendu disponible un document avec des meilleures pratiques où il y avait des informations très ciblées par rapport à des mesures à prendre en termes de la pandémie de la covid-19. Europol a transformé cette information en un formulaire que les forces de l'ordre pouvaient utiliser pour s'assurer que les rapports ou les signalements aux bureaux

d'enregistrement contenaient des informations dont ces bureaux d'enregistrement avaient besoin pour pouvoir lutter contre les abus.

Nous avons donc vu comment cette coopération pouvait être facilitée, non seulement maintenant mais dans l'avenir parce que comme on l'a dit lors de la séance plénière, nous essayons de bâtir des partenariats, travailler en coordination avec les forces de l'ordre et les agences d'application de la loi à travers la création d'un point de contact unique, d'un guichet unique où l'on peut centraliser des expertises, des expériences, partager des informations non seulement par rapport à l'industrie du DNS mais aussi par rapport à d'autres domaines qui peuvent être intéressants pour les parties contractantes, donc créer ce point de contact unique.

Voilà notre effort pour expliquer quelle est l'approche que nous avons adoptée dans l'écosystème. Je vous assure que nous ne comptons pas uniquement sur la communauté de l'ICANN pour résoudre les problèmes d'abus. Il faut que les organisations, les gouvernements, les autres acteurs soient aussi présents, que l'on puisse voir le trafic également. Et nous devons nous assurer que des règles de trafic appropriées soient en place, non seulement au niveau de l'écosystème de l'ICANN. Diapositive suivante s'il vous plaît.

Nous pouvons maintenant ouvrir la séance à des questions et aux prochaines étapes pour les GAC. Je voudrais signaler les efforts déjà en cours qui sont ici sur la liste. Nous les avons abordés pendant la séance intercommunautaire. Il y a un outil qui est très important pour le signalement des cas d'utilisation malveillante des noms de

domaine, le DAAR car il donne des informations qui pourraient à l'avenir devenir plus détaillées. Je veux également attirer l'attention sur un élément qui apparu dans une séance de l'ALAC, une lettre par rapport à l'application des engagements d'intérêt public de manière plus générale, car ces engagements sont difficiles à faire appliquer par le département de la conformité contractuelle de l'ICANN. Ensuite, le plan de travail du PSWG avec des pistes de travail spécifiques consacrées à l'abus du DNS auquel travaille Gabriel Andrews qui continue à travailler sur cette question.

De manière plus spécifique, pour aujourd'hui, nous invitons les membres du GAC à saisir cette occasion pour réfléchir aux prochaines étapes de ces efforts et peut-être aborder ces questions avec le Conseil d'Administration. Il y a la question des services d'anonymisation et d'enregistrement fiduciaires et de la divulgation des informations de ces services, la recommandation de l'équipe de révision CCT sur les mesures proactives anti-abus. Ces mesures devraient être mises en place avant la nouvelle série – c'est l'avis du GAC. Et ensuite, le système de signalement de l'exactitude du WHOIS.

Et maintenant, si vous me permettez, je vais donner la parole à Laureen et à Chris pour voir s'ils ont des commentaires finaux avant d'ouvrir la séance à des questions ou à des commentaires.

LAUREEN KAPIN : Je voudrais ajouter un élément, vous dire que c'est un sujet par rapport auquel la meilleure façon de réussir, c'est de travailler en

coopération. Les bureaux d'enregistrement, les registres, l'ICANN, le remarquable personnel de l'ICANN qui travaille dans la partie technique, dans la partie sécurité et qui travaille avec le PSWG, cette coopération doit inclure également nos collègues du GAC et les gouvernements du monde entier. Il faut créer des partenariats avec les forces de l'ordre, les agences d'application de la loi et de protection des consommateurs. C'est un effort qui doit se faire en coopération pour pouvoir lutter contre les différentes formes d'abus du DNS, notamment dans des moments difficiles comme cela a été le cas lors de la pandémie de la covid-19.

CHRISTOPHER LEWIS-EVANS : Je vais aborder brièvement le plan de travail du PSWG qui a été publié. Et dans ce plan, nous mettons l'accent sur le travail pour lutter contre l'abus du DNS avec un certain nombre de points qui sont importants et dont nous avons parlé dans le chat, différents aspects par rapport au DNS et comment nous pouvons éviter les cas d'abus. J'invite les participants du GAC à regarder ce plan de travail pour voir comment nous nous y prenons pour travailler dans ce domaine.

Merci.

CATHRIN BAUER-BULST : Merci Laureen et Chris.

Je vais maintenant ouvrir la séance à des questions si vous souhaitez faire des commentaires. Manal, est-ce que vous souhaitez faire un commentaire avant de passer à la partie questions et réponses ?

PRÉSIDENTE MANAL ISMAIL : Je pense qu'il nous reste une quinzaine de minutes encore. Nous avons Kavouss qui a levé sa main et qui a posé plusieurs questions sur le chat. Kavouss, s'il vous plaît.

IRAN : Est-ce que vous m'entendez ?

PRÉSIDENTE MANAL ISMAIL : Si vous pouvez parler plus près du micro.

IRAN : Merci Cathrin qui nous a donné beaucoup d'informations en quelques minutes. Et merci à tous les autres.

Il y a énormément d'informations. Si l'objectif, ce sont ces trois points, il n'y a aucun problème, c'est-à-dire la protection anti-abus, le service d'anonymisation et d'enregistrements fiduciaires et le plan de travail et la relation avec la covid-19.

Autrement, je vais demander à Chris et aux autres de fournir la même information pour les années précédentes pour voir comment cela a changé ou évolué. Si l'objectif, ce sont ces trois points, nous n'avons

pas de problème pour les considérer. Comment nous pourrions agir en ce sens ?

PRÉSIDENTE MANAL ISMAIL : Merci Kavouss.

Y a-t-il des réponses ou des réactions à cette remarque de Kavouss ?

Avant de passer aux questions qui sont dans la section de questions et réponses, il y a également un commentaire du représentant de l'Inde auprès du GAC et je m'excuse, je sais qu'il y en a qui s'attendent à ce que leur question soit répondue. En général, on donne la priorité aux questions du GAC. Donc permettez-moi de donner d'abord la parole à l'Inde puis on passera aux questions qui ont été posées dans la section questions et réponses.

L'Inde dit : « Le PSWG devrait également travailler avec le directeur des sauvegardes des consommateurs de l'ICANN pour être plus efficace dans sa considération des cas d'abus de DNS et autres. » Merci l'Inde.

Nous allons maintenant passer aux questions qui ont été posées par écrit. On a 10 questions ou commentaires. Je ne suis pas experte, j'espère les lire dans le bon ordre, je ne suis pas sûre. Il me semble que la première était une question que vous avez déjà abordée, Cathrin, sur le chat. Je vais quand même la lire.

La question dit : « Madame Bauer-Bulst a dit qu'il était difficile de s'exempter des service d'anonymisation ou d'enregistrements

fiduciaires. Dans la plupart des cas, la confidentialité du WHOIS est un service payant mais le RGPD cache les données WHOIS et ce n'est pas payant. Est-ce qu'elle a entendu que ce voile du RGPD était difficile à éliminer ? Ou veut-elle entendre que toutes ces questions sont comprises dans l'anonymisation ? » Cathrin, vous avez déjà répondu ?

CATHRIN BAUER-BULST : Oui, mais si j'ai bien compris, Cristina voulait aborder la question également.

PRÉSIDENTE MANAL ISMAIL : Merci de me le signaler également. Cristina ?

CRISTINA : Désolée, je pense qu'il y a eu un problème parce que je n'ai pas de réponse à la question.

PRÉSIDENTE MANAL ISMAIL : Ne vous inquiétez pas, on est tous en train d'apprendre.

CATHRIN BAUER-BULST : Pour ceux qui ne l'ont pas vu sur le chat, ce n'est pas que je mélange ce masque des données personnelles et des services d'anonymisation et d'enregistrements fiduciaires. Je ne mélange pas les exigences d'un service et de l'autre. Mais on m'a offert au moins trois fois ces services pendant le processus d'enregistrement d'un nom de domaine.

Et pour ce qui est dit sur le chat par rapport aux échanges avec le directeur des sauvegardes de l'ICANN, on a échangé avec Brian lorsqu'il était toujours là et que la position existait toujours, mais comme cela a été dit par Michaela sur le chat, il est parti, il n'y a pas eu de remplacement, on ne sait pas quels seront les plans. Mais lorsque cela était possible, oui, on a échangé avec lui et on le referait si c'était possible.

Merci.

PRÉSIDENTE MANAL ISMAIL : Très bien, merci Cathrin.

Nous avons une autre question. Je ne suis pas sûre pourquoi elle est envoyée par un participant anonyme, je ne sais pas si on devrait y répondre ou pas. En tout cas, la question dit : « L'ICANN aborde l'abus du DNS dans le cadre de sa mission avec une vision un peu plus élargie, mais cela ne suffit pas. Pour l'utilisateurs final, l'utilisateur commercial ou l'utilisateur individuel, la forme d'abus qui fait le plus de mal est ce que l'on pourrait définir comme l'abus de l'espace web du domaine pour que des contenus malveillants ou frauduleux ou trompeurs soient publiés pour l'exploitation ou pour dans gains économiques ou faire d'autres types de dégâts en utilisant un nom de domaine pour créer un espace web dans le but de divulguer du contenu qui pourrait tromper les gens malheureux pour qu'ils postulent pour un emploi qui pourrait être en fait une forme d'esclavage moderne. Il y a d'autres moyens et d'autres dommages

liés au contenu qui sont plus évidents et moins compliqués que l'ICANN ne vise pas à résoudre. Y a-t-il des initiatives externes, séparées ou privées en dehors du processus formel de l'ICANN qui entre dans cette classification de ce qu'est l'abus du DNS et que l'ICANN puisse résoudre ? »

CATHRIN BAUER-BULST : Je pourrais essayer de répondre à ce commentaire. C'est une question excellente.

Hier, lors de la séance intercommunautaire, on a vu d'ailleurs des graphiques montrant que quelqu'un avait créé un écosystème de noms de domaine qui est comparé à l'écosystème de gestion des contenus. Donc on comparait les deux avec les données des titulaires de nom de domaine. On pouvait voir le contenu des sites web tels qu'ils étaient approuvés par le prioritaire ou le titulaire du nom de domaine. Et d'autre part, du côté du DNS, on avait les bureaux d'enregistrement, l'opérateurs de registre et le service de nom si je ne me trompe. Et ce qui m'a frappé est que pour l'acteur en dehors de cet écosystème, pour celui qui veut tromper et qui veut faire de l'argent, on a toujours trois entités qui apparaissent lorsqu'on voit les données associées à l'enregistrement. Mais on n'a pas de mesures concrètes que l'on puisse prendre lorsqu'on a des entités criminelles. Mais une mesure que l'on essaie de prendre contre un cas d'abus, on se demande toujours : « Que pourrait-on faire en attendant à ce qu'il y ait une définition des parties contractantes ? » C'est pourquoi on apprécie

les commentaires des parties contractantes qui sont vus comme des définitions ou qui essaient de donner une réponse à cette lacune.

Peut-être que dans le contexte de la covid-19, ce qui serait encourageant serait de voir que les gens faisaient attention à cet espace, qu'on a énormément de données et qu'on pourrait peut-être mieux identifier les types d'abus qui sont entrepris et pouvoir essayer d'y répondre. On pourrait essayer de trouver une réponse dans l'écosystème de l'ICANN et au-delà.

Puis il y a une autre question un peu plus philosophique qui apparaît dans ce contexte, c'est : Qu'est-ce qui est au-delà de l'écosystème de l'ICANN ? Est-ce que cela appartient aux gouvernements que de légiférer dans ce sens, de générer des interactions dans ces cadres nécessairement nationaux et dans le rapport avec l'écosystème international qui est géré par l'ICANN ? Voilà mon essaie de réponse.

Peut-être que Laureen ou Chris ou d'autres souhaiteraient intervenir.

PRÉSIDENTE MANAL ISMAIL : Merci Cathrin. S'il n'y a pas d'ajout de la part de Laureen ou de Chris, peut-être qu'on pourrait donner la parole au représentant de la Russie qui lève la main.

RUSSIE : Bonjour. Vous m'entendez ?

On a beaucoup discuté de la question de la covid-19 mais il faut garder à l'esprit les autres questions, les autres contextes et les autres problèmes qui existent. Par exemple le DNS sur HTTPS et le DNS sur [inaudible]. Donc la question de [inaudible] par exemple qui essaie d'améliorer la sécurité pour le DNS, on a parlé du DNS et de l'IOT lors de la séance précédente. Cependant, le DoH comporte des risques pour l'intérêt public, la protection en ligne des enfants par exemple. Je voudrais savoir si notre groupe du PSWG a fait les recherches sur ces sujets, s'il y a des analyses de risques qui aient été effectuées, etc. Quelle est la position de l'ICANN en tant qu'opérateur mondial du DNS ?

Merci.

PRÉSIDENTE MANAL ISMAIL : Merci la Russie.

Y a-t-il des commentaires des présentateurs ? Je vois Chris qui lève la main. Allez-y.

CHRISTOPHER LEWIS-EVANS : Merci et merci pour cette question.

Nous avons signalé que le DoH et le DoT sont des questions qui pourraient poser des risques à la sécurité publique. Nous y travaillons en ce moment. Malheureusement, certains des événements récents ont entravés nos efforts. Mais la question de DoT et DoH fait l'objet d'énormément d'évaluations, d'analyses de risque en dehors de notre

mission. Donc on prévoit évaluer tout cela, oui et nous nous concentrerons sur cette question au cours de la prochaine année. Et comme Fabien l'a très bien exprimé sur le chat, il y a également une évaluation d'impact des risques sur le DoH et le DoT qui est effectuée par l'ICANN. Donc il y a énormément de travail que nous pourrions utiliser pour soutenir le travail du PSWG.

Merci.

PRÉSIDENTE MANAL ISMAIL : Merci Chris.

J'ai une question de James Bladel qui reprend cela. Il dit : « Merci. Il serait utile de présenter ces questions séparément pour que l'on puisse comprendre quelles parties de ces incidents ont lieu sur facebook.com ou twitter.com ou sur des noms de domaine similaires qu'un bureau d'enregistrement ne mettra jamais en suspension en raison d'incidents individuels d'abus de DNS. »

S'il n'y a pas de réponse immédiate à ce commentaire, on a ici une autre intervention écrite qui dit : « Ce n'est pas une question. Je pense que c'est lié aux questions techniques. Donc j'invite les responsables à lire cette intervention. »

Autre question, encore une fois, d'un participant anonyme : « Comment l'éducation vis-à-vis de l'abus est-elle et dans quelle mesure ? Dans notre monde, il y a énormément de types d'abus, certains sont plus compliqués, d'autres plus technologiques, mais ils

sont tous au-delà des capacités de 80 % de la population mondiale qui n'arrivent pas à les comprendre. Même si les ressources déployées et les fonds disponibles pour l'éducation étaient illimités, l'abus requière des formes de consultation et des mesures ascendantes bien délibérées et considérées et des mesures de backhand techniques de la part du DNSSEC et du SSAC et autrement dit, une forme de codage anti-abus dans le DNS. La prévention des abus pourrait devoir être intégrée dans le DNS avec ou sans obligation. Pourquoi souligne-t-on l'éducation des consommateurs sur l'abus ? Est-ce que cela protègerait tous les consommateurs tout le temps contre toutes les formes d'abus ? »

LAUREEN KAPIN : Je peux répondre à cette question.

Nous considérons l'éducation des consommateurs comme un outil important mais pas le seul. Il me semble que l'on pourrait travailler davantage sur les études visant à mesurer l'impact. Il est difficile de faire des recherches dans ce domaine. Il faudrait des groupes de contrôle qui étaient éduqués, des groupes qui ne le sont pas, puis pour une certaine période de temps comparer les résultats entre les deux. Mais nous savons que les connaissances représentent du pouvoir dans ce domaine. Donc si on donne aux jeunes des informations utiles, surtout dans ce domaine qui dépend de la science – comme dans le cas de la covid-19 –, l'éducation peut être une ressource utile pour aider le public à interpréter ce qui est valide, ce qui est utile, ce qui ne l'est pas. C'est pourquoi je pense qu'il est un

outil important et qu'il faudrait que ce soit ajouté à notre boîte à outils ensemble avec son application, avec les obligations contractuelles, avec les exigences et avec la coopération volontaire des gens qui utilisent ce système à des fins commerciales. La coopération, d'ailleurs, j'ajouterais, était très bonne dans cet effort de lutter contre les menaces qui sont apparues dans le contexte de la crise.

PRÉSIDENTE MANAL ISMAIL : Merci Laureen.

Je m'excuse, je sais qu'il nous reste des questions. John, Nigel, Fabricio, j'espère ne pas avoir oublié d'intervention mais malheureusement, nous sommes déjà en retard d'une minute et nous allons devoir conclure la séance.

Y a-t-il des remarques finales de nos présentateurs avant de clore cette séance ? Autrement, nous allons conclure la réunion d'aujourd'hui. Je vous remercie tous.

L'équipe de direction du GAC, comme vous le saurez, sera disponible entre 16h00 UTC et 16h30 et se mettra à la disposition des collègues du GAC qui ont eu des difficultés pour participer aux séances en raison du décalage horaire.

Demain, nous allons commencer à 10h00 heure de Kuala Lumpur, 2h00 UTC, avec une séance de rédaction du communiqué.

Merci tout le monde, ayez une bonne journée ou bonne fin de journée. Merci à nos présentateurs. La réunion est désormais ajournée. Merci.

[FIN DE LA TRANSCRIPTION]