ICANN73 | Forum virtuel de la communauté – Séance du GAC sur l'utilisation malveillante du DNS et mise à jour du PSWG
Mardi 8 mars 2022 – 14h30 à 15h15 AST

GULTEN TEPE : La séance va commencer. Merci de lancer l'enregistrement.

Bienvenue à l'ICANN73, rapport mis à jour du PSWG du GAC, suivi par la séance de l'utilisation malveillante du DNS le 8 mars à 18 h 30 UTC. Pour des contraintes de temps, nous n'allons pas faire l'appel aujourd'hui, mais la feuille de présence des membres du GAC sera disponible en annexe du communiqué du GAC.

Pour que la participation au modèle multipartite soit transparente, nous vous demandons de vous connecter aux sessions en utilisant votre nom complet. Autrement, vous pouvez être retiré de la séance.

Si vous souhaitez poser une question ou faire un commentaire, veuillez le taper dans le chat en ajoutant au début à la fin de votre phrase le mot « Question » ou « Comment » pour que tous les participants puissent le voir.

Le service d'interprétation simultanée pour les séances du GAC est disponible dans les six langues des Nations Unies plus le portugais. Les participants peuvent sélectionner la langue dans laquelle ils souhaitent écouter ou parler en cliquant sur l'icône d'interprétation situé dans la barre d'outils de Zoom.

Enfin, 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. À vous Manal.

PRÉSIDENTE MANAL ISMAIL : Merci beaucoup Gulten. Merci de revenir aussi vite de la pause.

Nous allons aborder la question de l'utilisation malveillante du DNS pendant 45 minutes, puis des nouveaux gTLD dans les dernières 45 minutes. Ici, vous voyez les responsables de chacune des questions à aborder, les orateurs invités sur l'atténuation de l'utilisation malveillante du DNS, il y aura des gens du groupe de travail de la sécurité publique, Laureen Kapin de la Commission fédérale du commerce des États-Unis, Chris Lewis Evans de l'Agence nationale de délits du Royaume-Université, vice-président aussi, Gabriel Andrews du FBI des États-Unis. Notre orateur de la partie du GAC, c'est Sumitaka Shirakabe du Japon, du ministère des Affaires internes et des communications. Et nous avons un orateur invité en plus du représentant du Japon, à savoir Ivett Paulovics, coauteure d'une étude sur l'utilisation malveillante du DNS de la Commission européenne.

Nous avons beaucoup de questions à aborder, alors je vais passer la parole à nos orateurs.

LAUREEN KAPIN : Je vais vous parler cette fois-ci comme coprésidente du groupe de travail sur la sécurité publique du GAC.

Ici, vous voyez une feuille de route de ce que nous allons faire pendant cette séance très brève et très condensée. Pourquoi l'atténuation de l'utilisation malveillante DNS est importante ? Nous allons entendre parler d'une étude récente de la Commission européenne sur l'utilisation malveillante du DNS. On va présenter des informations supplémentaires, on va parler des faits récents qui ont trait à la nouvelle initiative de l'étude du groupe d'études techniques sur la sécurité du DNS, le travail du SSAC qui a trait aussi à ce nouvel outil d'information centralisé de l'utilisation malveillante du DNS qui a trait à l'Institut centralisé de l'utilisation malveillante. Il y a aussi des représentants de la GNSO qui font partie de la petite équipe sur l'utilisation malveillante du DNS.

Nous allons parler aussi de la séance plénière sur l'utilisation malveillante du DNS qui aura lieu et on abordera les différences entre les domaines enregistrés malicieusement et les domaines compromis, ce que cela signifie. On va aborder notre travail futur. On va écouter notre collègue du Japon qui va aussi nous montrer comment il peut y avoir des dispositions améliorées dans les contrats et aussi les meilleures pratiques, les évaluations et les études. Passons à l'image suivante.

On essaie de donner des antécédents. Pourquoi ces questions sont importantes pour le GAC ? Nous allons en entendre parler, il y aura des discussions et des débats sur les définitions. Mais nous voulons vous

donner des informations sur les différentes définitions. Quand on parle de l'utilisation malveillante du DNS, ce sont des menaces à la sécurité : hameçonnage, botnet, logiciels malveillants. Et tout cela apparaît dans l'avis sur les sauvegardes aux mesures de protection du GAC de Pékin et ce texte figure dans les contrats, à savoir des menaces à la sécurité qui doivent être prises en compte par les registres.

Mais aussi il y a d'autres définitions. Par exemple, l'équipe de révision de la confiance du consommateur a fait référence à une définition qui faisait partie d'une étude précédente de l'ICANN, un document précédent de l'ICANN. On a parlé d'activités non sollicitées, trompeuses qui font un usage actif dans le DNS et de procédures utilisées pour enregistrer les noms de domaines. Et aussi, je vais vous parler d'une déclaration du GAC sur l'utilisation malveillante du DNS qui inclut plus de détails, des activités qui peuvent avoir un impact sur les consommateurs.

Et il y a aussi quelque chose d'assez familier qui a très aux statuts de l'ICANN qui parle d'une menace à l'infrastructure de DNS. Quand on parle du DNS, on parle du système des noms de domaine et ceci peut affecter la structure, la sécurité et la stabilité. On va se concentrer aussi sur l'utilisation malveillante du DNS, sur les questions de sécurité publique, parce que nous savons que ce groupe est un canal qui, avec ceux en charge de la sécurité des consommateurs, a donné son avis au comité consultatif gouvernemental parce qu'ils sont des experts en la matière.

En 2015, on a formé le groupe, on a eu un plan de travail. On fait référence aux formalités ayant trait au fait d'être un groupe de travail au sein du GAC. Il ne s'agit pas seulement du GAC et du groupe de travail sur la sécurité publique, mais il y a un grand nombre de parties prenantes au sein de l'ICANN qui font de l'utilisation malveillante du DNS une de ses priorités, parce que nous reconnaissons que les données actuelles de l'ICANN ne fournissent pas des obligations contraignantes pour atténuer l'utilisation malveillante du DNS. Tout ceci, vous le trouverez dans des déclarations de l'ICANN, dans des discussions de la communauté, dans la correspondance du Conseil d'Administration où il y a eu une lettre spécifique du 12 février 2020 qui fait référence à des dispositions contractuelles qui n'étaient pas suffisamment claires pour que les obligations soient opposables. Et le GAC aussi a contribué dans différents sites, à savoir des équipes de révision, des commentaires publics sur le travail de ces équipes de révision et a aussi participé aux travaux d'élaboration de politiques.

Voici donc les antécédents. Vous avez ici plusieurs liens qui sont très utiles. Plus tard, vous pourrez les visiter et vous obtiendrez des informations. Diapositive suivante s'il vous plaît.

Nous allons parler de certains faits récents. Parmi eux, il y en a qui sont très détaillés et l'un d'eux est l'étude très détaillée de la Commission européenne sur l'utilisation malveillante du DNS. Je vais faire une petite introduction avant de passer la parole à mon collègue. Il s'agit d'une nouvelle étude demandée par la Commission européenne présentée vers la fin de janvier et qui a été communiquée

au GAC au début de février. Au groupe de travail sur la sécurité publique, nous avons pu avoir une présentation en février.

Certaines observations générales. Elle est très pratique, elle se concentre sur les rôles et responsabilités de tout l'écosystème, ce qui est vraiment utile. Elle ne se concentre pas seulement sur les parties techniques de l'utilisation malveillante, les attaquants et ceux qui font l'utilisation malveillante, mais aussi sur les intermédiaires, non seulement les parties contractantes de l'ICANN pour ainsi dire, mais aussi des entités qui font partie du système également. Ce que je veux dire, c'est que nous ne parlons pas seulement des opérateurs de registre et des bureaux d'enregistrement, mais aussi de ceux qui fournissent l'hébergement et les revendeurs comme d'autres intermédiaires. Les organismes de sécurité, d'éducation aux consommateurs peuvent contribuer à cet égard. Il y a un grand nombre d'observations dans cette étude qui sont apparues dans d'autres travaux de la communauté, par exemple au SSAC et dans d'autres équipes de révision qui incluent la sécurité, la flexibilité et la stabilité que j'ai mentionnées auparavant.

Une des choses intéressante et nécessaire, c'est l'observation qu'il est difficile de faire ou d'établir une différence entre l'utilisation malveillante technique et la sécurité botnet, le hameçonnage, les logiciels malveillants et ce qui a trait à l'utilisation malveillante liée au contenu. Bien des fois, la frontière n'est pas très claire entre ces types d'utilisation malveillante. Il y a plus d'un exemple dans l'étude, mais on parle du hameçonnage qui peut inclure aussi un domaine enregistré malicieusement et on peut recevoir un courrier

électronique qui dit de cliquer dans ce lien et alors là, on accède à des sites web avec des contenus malveillants. Il ne s'agit pas seulement de sécurité technique de l'utilisation malveillante du DNS, mais on parle aussi de l'utilisation malveillante liée au contenu. On parle aussi d'un logiciel malveillant par exemple qui peut nous amener à un site web avec du contenu malveillant.

Il y aura une séance plénière sur les domaines enregistrés malicieusement et les domaines compromis. Et là, il y a deux questions en parallèle. Je veux que vous compreniez la complexité de tout l'écosystème. Il est très important aussi de comprendre comment ceci est lié aux statuts constitutifs de l'ICANN et ce que l'ICANN peut faire à cet égard. Image suivante s'il vous plaît.

Ici, voici ma dernière observation avant d'écouter l'un des auteurs de l'étude. Voilà certains résultats et il y en a qui sont spécifiquement importants. Les nouveaux gTLD se trouvent dans l'un des groupes où il y a davantage d'utilisation malveillante au sein des TLD. Il y a une flèche qui pointe à un peu plus de 6 % : c'est le pourcentage des nouveaux gTLD. Mais lorsqu'on regarde l'utilisation malveillante dans les domaines, vous voyez que ce pourcentage des gTLD augmente bien plus que le 6 % ; on parle ici de plus de 20 %. Ceci est très important, surtout lorsque l'on parle des nouvelles séries de gTLD que l'on va aborder prochainement.

Il y a 41 % d'utilisation malveillante et ceci n'est pas concentré dans tous les nouveaux gTLD, mais il y a certains nouveaux gTLD qui souffrent de la concentration de l'utilisation malveillante, ceci au

niveau des bureaux d'enregistrements. Ici, on voit aussi les cinq bureaux d'enregistrement qui ont le plus d'utilisations malveillantes et qui représentent 48 % de tous les noms de domaine enregistrés malicieusement. Vous pouvez observer également que les bureaux d'enregistrement et les fournisseurs de services internet peuvent aussi répondre au rapport de l'utilisation malveillante et peuvent décider des actions rapides et décisives pour avoir un impact sur le préjudice de l'utilisation malveillante. Les gouvernements doivent informer de cette question parce que bien des fois, les bureaux d'enregistrement et les fournisseurs de services internet prennent cela très au sérieux.

Cela dit, je vais passer directement la parole à l'auteure de l'étude de la Commission européenne et je tiens à la remercie et spécifiquement de nous accompagner aujourd'hui et de partager une partie de ce qui a été dit ici.

IVETTE PAULOVICS : Merci beaucoup Laureen. Merci beaucoup de m'avoir accueillie. Étant donné le temps dont nous disposons, je vais passer directement à la présentation que je vais faire. Voilà, donc je vous demande s'il vous plaît de la mettre à l'écran. Merci beaucoup.

Je parlerai donc des objectifs de l'étude que la Commission européenne nous avait demandé de faire, la méthodologie utilisée et les délais, la définition que nous proposons pour l'utilisation malveillante du DNS, l'ampleur des mesures, les bonnes pratiques que nous avons identifiées et nos recommandations. Prochaine diapositive s'il vous plaît.

Les objectifs de cette étude étaient assez larges. L'étude avait été commandée pour identifier une définition de l'utilisation malveillante du DNS, en voir les typologies, les catégories, le rôle des acteurs impliqués et pour évaluer aussi l'ampleur de ce phénomène de l'utilisation malveillante du DNS. Nous devons tenir compte aussi des politiques, des lois, des pratiques internationales et des pratiques de l'industrie. Dans la mesure du possible, l'objectif était de voir ou d'identifier de bonnes pratiques qui pourraient être appliquées à d'autres acteurs, à des intermédiaires et au niveau de l'ICANN et de l'Union européenne. Et l'objectif concernait l'identification de mesures nécessaires pour aborder l'utilisation malveillante du DNS.

Pour ce qui est de la méthodologie appliquée, nous avons d'une part fait une recherche directe avec des mesures en temps réel, avec des enquêtes, des entretiens et des ateliers, des séminaires. Nous avons eu la participation d'un grand nombre d'experts. Pendant les mesures en temps réel, nous avons analysé plus de 2 700 000 incidents et environ 1,7 millions de noms de domaines qui ont fait l'objet d'une utilisation malveillante et qui étaient inclus dans des listes d'URL ayant une mauvaise réputation. Nous avons aussi fait une révision très large des rapports présentés par des tiers par rapport à l'utilisation secondaire. Cette étude a pris un an. Nous avons fait nos mesures au cours de deuxième trimestre de 2021. Prochaine diapositive s'il vous plaît.

Quant à la définition de l'utilisation malveillante, Laureen a déjà mentionné la limitation d'une certaine terminologie utilisée jusqu'à présent. Nous voyons qu'il est assez difficile de différencier les

menaces concernant des questions techniques et des contenus, car ces menaces sont juxtaposées souvent. Donc nous proposons l'utilisation d'une définition large, plus ample. L'utilisation malveillante du DNS est toute activité qui se sert des noms de domaine ou du protocole du DNS pour effectuer des activités illégales ou qui peuvent résulter en dommages.

Notre approche concerne les bases et nous analysons chaque incident, chaque problème. Ce qu'il faut signaler par rapport à notre approche, c'est qu'elle fait la différence entre les noms de domaine enregistrés avec une intention malveillante et les noms de domaines qui sont compromis, c'est-à-dire ceux qui sont enregistrés par leur titulaire de nom de domaine mais qui sont plus tard compromis par différentes sortes d'acteurs malveillants.

Comment faisons-nous pour catégoriser l'utilisation malveillante du DNS ? Il y a trois catégories. En premier lieu, il y a les noms de domaines qui ont été enregistrés de manière malveillante. Deuxièmement, il y a l'utilisation malveillante concernant l'opération du DNS et d'autres infrastructures. Et troisièmement, il y a l'utilisation malveillante concernant des domaines utilisés pour distribuer un contenu malveillant. Par rapport à cette troisième catégorie, nous avons inclus les noms de domaine compromis ou enregistrés à des fins malveillantes.

Cette approche est importante parce qu'elle permet d'établir la différence entre des noms de domaines qui ont été enregistrés à des

fins malicieuses, malveillantes et cela nous permet de voir qui doit répondre et agir par rapport à cette utilisation malveillante du DNS.

Il y a ensuite parmi ces domaines des noms de domaines qui sont créés au moyen d'algorithmes à des fins de commande et de contrôle. Et à notre avis, cela peut être remédié au niveau du DNS. Et les intermédiaires qui doivent agir se trouvent à ce niveau-là, au niveau du DNS.

Par rapport au contenu malveillant, il peut être distribué au moyen de domaines enregistrés à des fins malveillantes, par exemple des domaines destinés au hameçonnage. Dans ce cas là, les mesures de correction doivent être faites au niveau de l'hébergeur et au niveau du DNS. Cela est dû au fait que cette atténuation de cette utilisation malveillante à un seul niveau ne serait pas efficace.

Pour ce qui est de la distribution de contenus malveillants par l'intermédiaire d'un domaine compromis, par exemple des domaines compromis qui distribuent un contenu de hameçonnage, ce ne serait pas utile de résoudre ce type de d'utilisation malveillante au niveau du DNS, parce que cela pourrait provoquer des dommages collatéraux aux titulaires de nom de domaine légitimes et les utilisateurs. Donc nous proposons pour ce cas-là que la remédiation soit faite au niveau de l'hébergeur. Pour ce qui est de l'utilisation malveillante pour ce qui est des opérations malveillantes, il doit être abordé au niveau du DNS. Donc nous voyons que la définition que nous avons proposée permet aussi de présenter des mesures de remédiation.

Parlons maintenant de l'ampleur de l'utilisation malveillante du DNS. Laureen a mentionné dans l'un de ses schémas, elle l'a décrit, c'est l'un des schémas de l'étude, nous faisons une mesure dans le TLS et nous avons vérifié si l'utilisation malveillante a lieu dans des noms de domaine malveillants. Aussi, cela implique la réputation du bureau d'enregistrement ou d'autres acteurs pour ce qui est des TLD comme Laureen l'a dit et comme on peut le voir sur ce graphique où l'on compare la participation sur le marché de ces groupes de TLS.

Et notre conclusion est la suivante. Les ccTLD de l'Union européenne sont ceux qui sont les moins soumis à l'utilisation malveillante dans les deux cas. Et nous pouvons le voir sur le graphique, sur le camembert. Nous voyons que les ccTLD de l'Union représentent 14,44 % de parts de marché et moins de 21 % d'utilisation malveillante. En termes relatifs, les nouveaux TLD comme Laureen l'a dit ont une part de marché que nous voyons sur le graphique et sont ceux qui sont les plus souvent affectés par l'utilisation malveillante. Nous voyons aussi d'autres résultats de l'étude et cela ne signifie pas que tous les nouveaux gTLD soient soumis à l'utilisation malveillante. Nous voyons que la plupart de ces TLD représentent environ 41 % du total de l'utilisation malveillante. Prochaine diapositive.

Nous voyons maintenant la distribution des domaines compromis et enregistrés de manière malveillante. Nous voyons qu'environ 24 % et 41 % des noms de domaine où il y a du hameçonnage et du logiciel malveillant sont compromis au niveau de l'hébergeur alors que la vaste majorité de ceux qui sont destinés aux pourriels ou aux réseaux zombies ont été enregistrés de manière malveillante. Nous voyons ici

la distribution des domaines compromis enregistrés de manière malveillante au niveau des TLD. Prochain diapositive.

Comme je vous l'ai dit, nous avons fait une [distribution] de la réputation des bureaux d'enregistrement et nous avons pu remarquer que les bureaux d'enregistrement soumis à l'utilisation malveillante représentent 48 % de tous les noms de domaine enregistrés de manière malveillante. Nous avons observé aussi que parmi les fournisseurs d'hébergement, il y a une concentration disproportionnée de noms de domaine consacrés aux pourriels. Nous voyons que les extensions de sécurité du DNS, leur niveau d'adoption, ainsi que les protocoles de protection de courriels continuent d'être à un niveau faible. Prochaine diapositive.

Enfin, après avoir analysé toutes les procédures au niveau international, au niveau de l'ICANN, au niveau de l'Union européenne ainsi que des normes de réglementation, nous avons identifié des bonnes pratiques de différentes catégories. Nous les avons analysées, nous les avons catégorisées entre préventives, réactives et aussi des bonnes pratiques en matière de transparence et d'information.

Nous avons identifié des intermédiaires que vous pouvez voir dans les exemples. Nous avons des exemples de ccTLD et de quelques opérateurs de registre de gTLD aussi. À cause du temps qui est disponible, je ne rentrerais pas dans le détail par rapport aux bonnes pratiques. Cette étude inclut une analyse exhaustive à cet égard. Maintenant, je vais passer à la prochaine diapositive.

Enfin, dans l'étude, nous avons établi ou formulé 27 recommandations groupées dans six domaines pour améliorer les mesures d'atténuation de l'utilisation malveillante du DNS. Nous avons des recommandations aussi à caractère technique que je ne peux pas mentionner dans leur totalité, ainsi que des recommandations en matière de politiques. Par exemple, il y a des recommandations concernant les intermédiaires.

Pour ce qui est des revendeurs, des bureaux d'enregistrement, des opérateurs de registre, nous recommandons un système de signalement d'utilisation malveillante qui soit centralisé pour identifier des données d'enregistrement du domaine pertinent et pouvoir ainsi agir et faire un suivi des indices d'utilisation malveillante, ainsi qu'appliquer des sanctions et proposer des incitations pour que les niveaux de l'utilisation malveillante se trouvent au-dessous d'un seuil prédéterminé. Pour ce qui est fournisseurs de services d'hébergement, nous avons des recommandations semblables, c'est-à-dire contrôler les niveaux d'utilisation malveillante qui devraient se trouver au-dessous d'un seuil déterminé.

Pour le dernier domaine, nous voyons la question de la collaboration. Nous recommandons une unification de l'opération des ccTLD dans le cadre des bonnes pratiques permettant de collaborer avec les institutions gouvernementales, avec les autorités d'application de la loi et avec des notificateurs fiables. Donc cela signifie que nous avons plusieurs recommandations comme Laureen l'a dit et elles se rapportent à différents types d'études et d'analyses. Dans ce cas

particulier, cette étude vise à présenter un aperçu complet de ce phénomène observé en 2021.

Voilà donc ma dernière diapositive. Dans la prochaine diapositive, vous pouvez voir les liens pour accéder à cette étude pour la télécharger. Et bien sûr, vous pouvez nous contacter, moi ou la personne qui a rédigé le rapport avec moi qui n'a pas pu être présente parmi nous parce qu'elle se trouve dans une séance de l'unité constitutive des utilisateurs commerciaux.

Merci beaucoup de votre temps et de votre attention.

LAUREEN KAPIN : Merci.

Je vois qu'il y a des questions dans la salle de chat. Je vois qu'il y en a qui veulent prendre la parole. Nous allons nous concentrer sur les questions ayant trait à l'étude présentée et nous allons vous demander d'être conscients des sujets abordés.

Je crois qu'il y en a qui posent des questions. Finn demande s'il y a quelque chose concernant les recommandations qui serait particulièrement facile pour pouvoir prendre des mesures dès que possible. Ivette, je crois que la question vous concerne.

IVETT PAULOVICS : Oui, merci Laureen.

La question n'est pas simple, clairement. Cette étude a été demandée par la Commission européenne. Par exemple, pour la Commission européenne, ce serait bien plus facile de s'adresser aux ccTLD de l'Union européenne afin d'unifier les opérations et le fonctionnement des ccTLD et d'adopter les bonnes pratiques. Au sein de l'ICANN, il doit y avoir peut-être d'autres priorités et d'autres recommandations, des recommandations qui pourraient être adoptées plus facilement. Pourquoi ? Parce qu'il y a d'autres domaines de travail en parallèle.

Merci.

ÉTATS-UNIS : Merci Laureen de l'étude sur l'utilisation malveillante du DNS. C'est une ressource très importante pour ceux qui élaborent les politiques pour pouvoir mieux comprendre la partie technique et commerciale, ainsi que les activités juridiques qui se passent au sein de l'ICANN. Mais je crois qu'en ce moment, la définition de l'utilisation malveillante du DNS très vaste pour qu'elle soit utilisée à l'intérieur de l'ICANN, parce que nous avons des activités illégales qui se passent aussi en dehors de l'ICANN et en dehors des statuts constitutifs de l'ICANN. Mais je crois qu'on peut faciliter l'échange et les experts du gouvernement peuvent intervenir sur des questions liées à l'internet. Il y a des questions qui sont en dehors des statuts constitutifs de l'ICANN. Nous sommes très reconnaissants de cette étude. Nous savons bien quelle est son utilité. Nous savons aussi que la définition de l'utilisation malveillante du DNS est correcte et elle est utilisée à l'intérieur et à l'extérieur de l'ICANN.

Merci beaucoup.

LAUREEN KAPIN : Je passe la parole à Gemma.

GEMMA : J'espère que vous m'entendez bien parce que j'ai quelques problèmes audio et je me vois moi-même.

Merci Ivett de ta présentation. Et aussi, [inaudible] a parlé dans d'autres séances en parallèle.

En premier lieu, merci beaucoup pour la diffusion du travail réalisé et de notre côté, ceci a représenté un encouragement pour participer au dialogue avec la communauté de l'ICANN sur différents forums, sur le plus grand nombre de forums possible. Merci donc Ivett. Et comme Laureen l'a bien dit au début, il y a eu une présentation très importante du PSWG. J'ai eu une réponse positive au résumé de Laureen du début de la séance parce qu'en fait, il y a des questions qui ont été débattues au sein du PSWG qui peuvent être considérées parce que vraiment, c'est quelque chose que l'on peut voir dans le contexte des contrats avec l'ICANN et ceci, à travers l'utilisation malveillante du DNS avec l'ICANN. Et aussi, c'est quelque chose sur laquelle le PSWG travaille.

Je voudrais mentionner deux choses. En premier lieu, notre méthodologie ou notre approche signifie que c'est une étude indépendante. Nous l'avons demandé à des experts en dehors de la

Commission européenne. Je dirais que nous avons voulu faire cette étude même sans un délai spécifique parce que le sujet est très important pour nous. Nous voulons éviter l'utilisation malveillante du DNS qui est quelque chose de central pour ce ayant trait à la stratégie de cybersécurité européenne de 2020.

Pour donner plus de visibilité, notre vision a trait au fait de savoir que l'ICANN, c'est comme le DNS pour dire quelque chose de simpliste. Nous savons que l'ICANN est le site où il faut débattre sur le DNS et où il faut prendre des décisions par rapport au DNS. Voilà pourquoi nous voulions que l'étude soit très visible pour l'ICANN. Il est très important que les différentes unités constitutives aient la possibilité de faire des commentaires là-dessus. C'est une étude indépendante simplement ; voilà pourquoi il y a des éléments qui doivent être révisés et même parce qu'il y a des différences. Mais ce n'est pas une étude sur l'ICANN, pas du tout. Je crois que c'est la deuxième ou la troisième fois que cette étude est présentée, mais je veux arrêter l'histoire de ce que peut faire l'ICANN ou non.

Je crois que tout le monde au sein de la communauté est intéressé à éviter l'utilisation malveillante du DNS. C'est une question très complexe parce que comme Ivett l'a bien présenté, cela ne commence pas et ne finit pas avec un enregistrement malicieux d'un nom de domaine. Ceci peut se passer après l'enregistrement du nom de domaine, bien longtemps après. Je crois que les efforts des parties contractantes en analysant l'utilisation malveillante du DNS manière holistique, je crois que c'est la principale valeur ajoutée

Nous regardant l'utilisation malveillante du DNS de la part des victimes. Il y a une définition stricte sur ce que c'est exactement l'utilisation malveillante du DNS, si cela peut être arrêté pour dire : « Voilà ce qui se passe sous le parapluie de l'utilisation malveillante du DNS ou de l'enregistrement malicieux du DNS. Et voici les acteurs qui participent. On peut les voir clairement. » On ne peut pas le présenter entièrement dans ce contexte. On voit explicitement ce que font les revendeurs, les opérateurs de registre, les bureaux d'enregistrement. C'est un environnement vraiment complexe. Mais tout ceci est identifié dans l'étude.

Aussi, ce que font les fournisseurs d'hébergement, parce qu'on classe l'utilisation malveillante en catégories et en premier lieu, il faut voir quelle est l'applicabilité des acteurs pour les informer de ce qui se passe. Ceci a trait à ce qui surgit de tous cela. C'est une petite recommandation très claire qui établit des différences, quelle est la responsabilité de l'organisation, savoir ce qu'elle fait avec ces demandes et si les acteurs veulent communiquer au niveau du DNS, on peut se mettre en contact avec les responsables.

Il est clair aussi qu'il y a le besoin d'avoir de bons registres de WHOIS. C'est une des conclusions claires de l'étude. C'est un problème long, une question longue à aborder. J'apprécie beaucoup la présentation d'Ivett, mais je veux dire que les gens de la communauté de l'ICANN doivent prendre de l'étude ce qui leur paraît utile. Et pour les opérateurs, la Commission européenne et nous comme élaborateurs de politique, nous voyons ce que nous faisons de notre côté, nous évaluons les recommandations de ce point de vue, mais nous voulons

voir si la communauté peut vraiment prendre quelque chose de valable et voir ce qui se passe au fil du temps avec ceci, s'il y a des améliorations ou pas.

Mais vraiment, je veux vous dire, voyons ce que l'on peut faire au lieu de nous concentrer dans le domaine de l'ICANN. Ceci a trait à tout le DNS et pas à l'ICANN spécifiquement.

LAUREEN KAPIN : Merci Gemma.

Manal, je ne sais pas si on peut prendre quelques minutes de plus parce qu'il y a des questions et des déclarations sur l'étude qui sont vraiment utiles. Et lorsque les choses sont utiles, cela nous prend davantage de temps. Vous n'avez pas à répondre à ma question en ce moment.

Nous allons revenir aux diapositives. On va ordonner un peu les choses. On peut aller directement à mon collègue du Japon pour voir son document et voir si l'on peut faire une présentation des documents qu'il nous reste. Je passe donc la parole à mon collègue du Japon. Merci de votre patience.

SUMITAKA SHIRAKABE : Merci Laureen.

Je tiens à vous remercier de l'opportunité de pouvoir participer à cette réunion avec vous. Je sais que le temps est limité, alors très

rapidement, je vais partager avec vous cette image et je vais vous raconter quelque chose de bref.

Pendant la réunion de l'ICANN72, nous avons parlé de ce que nous appelons le hopping, le passage d'un bureau d'enregistrement à un autre, que fait un titulaire de nom de domaine pour pouvoir utiliser le même nom de domaine tout en passant d'un bureau d'enregistrement à un autre bureau d'enregistrement.

La question est maintenant que nous voudrions partager un cas du titulaire de nom de domaine qui semble être le même et qui continue à faire une utilisation malveillante en utilisant des noms de domaines différents enregistrés avec le même bureau d'enregistrement. Voilà donc le thème actuel de notre point de vue, du point de vue japonais, où nous pouvons suggérer deux choses.

L'une d'elles concerne le fait de garantir une conformité entre l'ICANN et le bureau d'enregistrement ou l'opérateur de registre. Certains collègues ont déjà mentionné ce thème. Et il faut corriger cette information par rapport à l'exactitude de cette information au moment de l'enregistrement du domaine. Il faut aussi mener à bien un audit constant et efficace de ce qu'est la conformité de la part des bureaux d'enregistrement quant à ce qui concerne la conformité contractuelle de l'ICANN.

D'autre part, nous pouvons considérer quelques mesures quant à l'utilisation malveillante qui est faite des noms de domaines. Nous pouvons penser à utiliser un programme de notificateurs fiables. Je crois que ce serait utile, surtout pour le cas où nous parlons d'un

contenu malveillant particulièrement. Je pourrais suggérer aussi la compréhension et la coopération avec d'autres comités consultatifs et d'autres organisations de soutien de l'ICANN. Je crois dans la réunion du GAC de l'ICANN72, il y a eu une réunion avec l'ALAC où on a parlé de la promotion de ce thème. Il s'agirait peut-être d'un petit groupe du GAC et de l'ALAC. Nous espérons voir cette action.

Ce matin, on a mentionné aussi dans le groupe de la ccNSO qu'il pourrait y avoir une action plus vaste, plus ample, au sein de ces groupes-là et l'idée est de collaborer avec le GAC et avec d'autres groupes.

Certains collègues ont déjà mentionné que la question de l'authentification est importante aussi et que nous pouvons voir l'ICANN prendre des mesures plus importantes, même si elle est limitée dans certains cas.

Je vous remercie de m'avoir donné la parole.

LAUREEN KAPIN : Merci de la présentation.

PRÉSIDENTE MANAL ISMAIL : Mes excuses pour vous avoir interrompu parce que je travaille en ce moment. Et à vrai dire, j'ai déjà parlé avec Luisa et Jorge, vous aurez quelques minutes de plus.

LAUREEN KAPIN : Je voudrais revenir un petit peu en arrière. Voilà, c'était la diapositive que je voulais montrer. Voilà. Je ne sais pas si Gabe veut nous donner cette vision générale sur ce matériel qui est présenté ici.

GABRIEL ANDREWS : C'était une excellente présentation sur l'étude de la Commission européenne, mais ce n'est pas la seule étude récemment publiée avec des données récentes. Donc je veux parler justement de ce travail concernant l'initiative de facilitation de sécurité du DNS et le groupe d'analyses techniques. C'est quelque chose que le directeur général de l'ICANN a demandé en 2020 et c'était en réponse à plusieurs attaques de haut niveau qui ont eu lieu en 2018-2019 dans le DNS. C'était le cyberespionnage que vous avez lu dans les nouvelles. Le groupe d'analyses techniques s'est centré non seulement sur ces attaques, mais sur d'autres. Et nous avons des exemples pris de ces incidents.

L'une des meilleures pratiques communes qui peut être considérée pour aborder ces incidents pourrait être la suivante. Les recommandations concernent ce qui a été envoyé au bureau du directeur technique de l'ICANN. Il peut y avoir une autre communication après cette étude, mais il n'y a pas d'action ou de mesures urgentes que le GAC doive prendre à cet égard. Voilà ce que je voulais dire.

Si vous vous en souvenez correctement, l'année dernière, le comité consultatif sur la sécurité et sur la stabilité a publié le SSAC115. C'était un rapport sur l'approche de l'utilisation malveillante et comment

traiter cette utilisation malveillante. Il y avait une recommandation qui parlait de la création d'un facilitateur de réponse commune face à l'utilisation malveillante. Une année plus tard, nous commençons à voir un candidat possible pour ce facilitateur de réponse face à l'utilisation malveillante et il peut s'agir justement de l'Institut sur l'utilisation malveillante du DNS.

En ce moment, ils essaient ce qu'ils appellent l'outil de signalement d'utilisation malveillante centralisé. Je pense que ce n'est pas le nom officiel, mais c'est ce nom qu'on lui donne pour le moment. Il a été présenté en juin, cet outil, et cela pourrait automatiser le routage et même améliorer l'information sur ces utilisations malveillantes. C'est quelque chose de nouveau et d'intéressant et nous croyons que dans la prochaine réunion de l'ICANN, nous pourrions peut être approfondir sur cet outil.

Pour donc clore à propos de ce thème, il y a une petite équipe qui a été créée sur le l'utilisation malveillante du DNS. Ils ont commencé à partager les questions sur cela avec le GAC pour mieux comprendre quelles sont les attentes de la GNSO. C'est une citation textuelle et comment les politiques futures pourraient contribuer dans des initiatives. Je ne vais pas approfondir à propos des questions sur l'écran, mais je veux que tout le monde en tienne compte parce que ce petit groupe de la GNSO cherche peut-être des réponses avant le 21 mars. Donc si quelqu'un veut y participer, veuillez répondre à ces questions-là.

Enfin, nous sommes là. Demain, il y a une séance plénière sur les domaines compromis versus ceux qui ont été enregistrés de manière malveillante. On va parler de l'étude de la Commission européenne, mais on verra comment on peut travailler avec les outils dont nous disposons. Et c'est un panel qui va approfondir la question et je crois que cela va être intéressant.

Je rends la parole à Laureen maintenant.

LAUREEN KAPIN : La prochaine est la dernière, il me semble. Voilà le travail pour l'avenir. Nous venons de souligner les points sur lesquels nous continuons à travailler. L'idée est d'améliorer les exigences contractuelles. Il y a aussi un texte que nous avons inclus dans le dernier communiqué et qui sera porté à des dispositions dans les statuts. L'ICANN peut aussi négocier des accords incluant des engagements liés à l'intérêt public. Cela peut être fait avec les parties prenantes et l'ICANN pourra améliorer donc les dispositions contractuelles pour que l'on puisse mieux répondre face à l'utilisation malveillante du business.

Il y a aussi des évaluations sur l'utilisation du DNS qui doivent être faites et qui concernent ce qui a été recommandé par le comité consultatif sur la sécurité et la stabilité avant le lancement de la nouvelle série de nouveaux gTLD. Je crois que cela est lié aussi à la prochaine séance, parce que lorsque nous considérons une nouvelle série de nouveaux gTLD, nous devons toujours voir ce que nous avons appris sur l'utilisation malveillante du DNS lors de la dernière série et en général.

Ceci dit, je vais m'excuser parce que nous n'avons pas plus longtemps pour les questions que vous voudriez poser, mais je vous invite à travailler dans le groupe de travail sur la sécurité publique et à nous parler non seulement pendant les réunions, mais à tout moment pour pouvoir avoir des conversations avec vous tous.

Maintenant, je suis à temps pour céder la parole au prochain groupe.

PRÉSIDENTE MANAL ISMAIL : Oui, merci beaucoup Laureen, Chris, Gabriel, Sumitaka et Ivett. C'était plusieurs présentations qui étaient très intéressantes. Nous vous sommes vraiment reconnaissants du soutien que vous nous donnez.

[FIN DE LA TRANSCRIPTION]