ICANN76 | Forum de la communauté – Discussion du GAC : Utilisation malveillante du DNS
Mardi 14 mars 2023 – 10h30 à 12h00 CUN

JULIA CHARVOLEN : Bonjour. On va aborder les questions malveillantes du DNS, à 10 h 30.

Tenez compte que cette séance est enregistrée. Elle est régie par les normes de conduite de l'ICANN. Dans cette séance, les questions et les commentaires présentés dans le chat seront lus à haute voix s'ils sont dans le format correct. Si vous êtes sur Zoom, levez la main et souvenez-vous de dire dans quelle langue vous allez parler si ce n'est pas l'anglais.

Parlez à un rythme raisonnable pour permettre une interprétation correcte. Mettez en muet tous les autres dispositifs. Et vous trouverez les questions disponibles sur la barre de Zoom.

Et je passe la parole à Manal Ismaïl.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Merci, Julia. Bonjour, bon après-midi et bonsoir à tous. Soyez tous les bienvenus.

Ici, on va aborder l'utilisation malveillante du DNS. Ce sera une séance d'une heure, et nous allons continuer à parler des initiatives de la communauté de l'ICANN et de l'organisation ICANN pour prévenir et atténuer l'utilisation malveillante du DNS. Et on va vous donner les nouvelles actions, les efforts des membres du GAC pour soutenir l'élargissement des dispositions contractuelles et des possibles

processus d'élaboration de politiques, pour aborder l'utilisation malveillante du DNS.

Je vais maintenant passer la parole aux responsables des différents sujets. Dans ce cas, nous avons Gabriel Andrews, du Bureau fédéral de recherche des États-Unis, du FBI. On a aussi Laureen Kapin, de la Commission de commerce fédéral des États-Unis et coprésidente du PSWG, et Chris Lewis-Evans, président du—

CHRIS LEWIS-EVANS : Bonjour à tous. Nous allons passer à la diapo suivante, s'il vous plaît, directement.

Nous avons une séance sur l'utilisation malveillante du DNS. Et il y a une présentation externe. Et je vois qu'il y a ici la personne responsable du réseau de politiques en matière de juridiction de l'Internet, dans un coin. Et j'espère que nous annoncerons la diapo avec l'aide du personnel de soutien au GAC.

Je vais expliquer pourquoi il est important d'aborder l'utilisation malveillante du DNS. On va donner des statistiques, et son lien avec l'utilisation malveillante du DNS. On verra d'autres activités qui ont lieu au sein de la communauté. Nous allons faire une clôture avec certaines considérations qui [puissent] être tenues en compte pour notre communauté dans la partie de l'avis ou des questions d'intérêt pour le GAC.

Suivante, s'il vous plaît.

Je sens que nous avons parlé de l'utilisation malveillante depuis longtemps. On a eu deux séances très enrichissantes sur la question.

Nous avons toujours parlé de l'atelier sur le renforcement de capacités de mardi sur l'utilisation malveillante du DNS. Et vous pouvez [la] revoir.

Il y a aussi une série de liens auxquels vous pouvez accéder, et vous pouvez faire une recherche dans le site Web du GAC avec le terme « utilisation malveillante du DNS », et cela vous amènera aux sections du communiqué. Le personnel de soutien au GAC, Benedetta, et le reste des membres ont fait un excellent travail pour avoir ceci à disposition.

Il y a une série d'éléments que nous avons soulignés. Ceci est une partie très importante du travail du PSWG. Nous avons un plan de travail qui a été ratifié [et est ratifié] dans cette réunion. Et cela permet que tous les fonctionnaires des organismes d'application de la loi puissent travailler, mieux travailler avec les communautés pour atténuer l'utilisation malveillante du DNS, et avec d'autres parties de la communauté.

Il y a beaucoup de délibérations, des consultations avec le Conseil, du courrier que l'on échange avec la communauté des entrepreneurs, etc., pour voir l'importance que tout cela a pour eux.

Il y a l'équipe de la révision de la CCT, le RDS-WHOIS2, [le] SSR2, pour ne mentionner que quelques-uns, et aussi l'EPDP sur les procédures pour des séries ultérieures, qui font aussi référence à l'utilisation malveillante du DNS

L'autre point que l'on va aborder pendant la présentation concerne les parties contractantes. On a envoyé une lettre au Conseil d'administration, concernant l'ouverture des négociations

contractuelles pour aider à aborder l'atténuation de l'utilisation malveillante du DNS. Cela démontre que la communauté veut agir. Et cette question a été considérée depuis longtemps.

Très rapidement, je vais voir si je peux faire une pause, et voir—

Laissez-moi voir. Je vais peut-être passer la parole à Gabriel.

LAUREEN KAPIN : Ici, on veut s'adapter aux circonstances pour faire ce qu'il faut.

CHRIS LEWIS-EVANS : Merci. Gabriel, maintenant, à toi. Très bien. Nous allons passer à la présentation sur les tendances actuelles. Je crois qu'on peut avancer deux diapos, si je ne m'abuse.

GABRIEL ANDREWS : Je suis Gabriel. Je parle à titre personnel, comme membre du PSWG.

Et ce que nous pensons faire, en ce moment, c'est quelque chose que nous essayons de faire annuellement s'il s'agit de comprendre l'échelle de l'utilisation malveillante du DNS.

En plus, de comprendre cela comme une partie du délit, il est important de savoir qu'on n'a pas de faits parfaits ; on a différents points de vue.

Et comme les aveugles que vous voyez sur l'image que vous connaissez déjà, nous faisons notre meilleur effort pour parler de ce que l'on perçoit en attendant qu'en collaborant, on puisse avoir une meilleure idée de ce qui est vu là.

Il y a beaucoup d'initiatives dans la communauté qui sont [adressés] à apporter des données, des observations, etc. Et nous pensons, par exemple, au rapport Campus de l'année dernière, l'OCTO et toutes les études sur l'utilisation malveillante du DNS. Et il y a deux jours, on a parlé avec le personnel exécutif. Et John Crain a dit que nous attendons les rapports de l'utilisation malveillante au niveau des registres, mais il a aussi quelques idées sur l'incorporation de l'analytique prédictive et de l'apprentissage automatique pour voir ce que l'on peut obtenir. Alors, tous ces perspectives et points de vue que nous pouvons apporter, et les organismes d'application de la loi peuvent contribuer aussi. Les dénonciations des victimes, qui nous arrivent, servent aussi.

On ne suggère pas que tous les délits ont trait à l'utilisation malveillante du DNS. Ce que nous disons, c'est que nous essayons de comprendre quelle est l'échelle du préjudice pour les victimes qui font les dénonciations. C'est une perspective que l'on devrait considérer au cours de cette délibération et voir comment ces rapports et ces dénonciations peuvent être traduits pour l'utilisation malveillante du DNS.

Je crois qu'avec ça, j'ai couvert la première partie, Chris.

CHRIS LEWIS-EVANS : Passons à la diapo suivante, maintenant.

Dans la dernière réunion du PSWG, nous avons [convoqué tous les membres à nous donner] des statistiques qu'ils avaient sur le cyberdélit et leur relation avec utilisation malveillante du DNS.

Pour le moment, on a reçu des informations des États-Unis et du Royaume-Uni. Alors, si vous travaillez avec vos propres agents d'application de la loi ou des agents de protection des consommateurs, n'hésitez pas à nous faire parvenir ces informations. Nous serons heureux de voir ce que d'autres pays font là-dessus et essayer que cette révision soit un peu plus vaste au niveau des statistiques. On a l'intention de le faire une fois par an pour avoir une idée du panorama général.

Si on va donner des données du Royaume-Uni, eh bien, là, on a un organisme unique qui s'occupe non seulement de la fraude, mais du cyberdélit. Après, ils ont ajouté le cyberdélit. Et les quatre statistiques principales n'informent pas le suivi de l'abus du DNS. On a l'hameçonnage, les virus, les logiciels malveillants. Et ceci n'est pas en ligne avec ce que nous [considérons l'utilisation] malveillante du DNS. On parle de l'hameçonnage au niveau personnel ou d'extorsion.

Comme vous le voyez dans cette diapo, les données viennent de 2014. Il y a une tendance ascendante dans les rapports et les dénonciations de ce type de délit.

Diapo suivante, s'il vous plaît.

Une des choses que vous faites aussi, c'est des enquêtes auprès des entreprises d'organisation bénéfique, pour voir comment ils se sont vus affectés, et savoir comment elles ont géré la question. Ce que l'on analyse ici a trait au nombre d'organisations qui ont identifié un certain type [d'irruption] ou d'attaques sur leur système. Ceci est assez statique. La tendance est légèrement descendante. Mais pour les organisations bénéfiques, il y a une tendance à la hausse. Ceci a été fait

avant le RGPD, alors peut-être cela n'était pas préparé pour analyser leur propre réseau. Et une fois que l'on commence à chercher quelque chose, normalement, on le trouve.

Voilà une des questions pour lesquelles on voit cette augmentation, parce qu'ils cherchent quelque chose et finalement ils le trouvent. Ils la trouvent. C'est difficile à dire, toute cette question des attaques. Nous voyons la tendance, ce qui est important.

Dans cette diapo, de tous ceux qui ont souffert un type quelconque d'attaque ou d'infraction, nous voyons comment ils l'identifient, quel est le vecteur d'attaque initiale. Et le long des années, la réponse pour le 80 % des fois, c'était l'hameçonnage. L'hameçonnage affecte l'utilisation malveillante du DNS, bien évidemment. Le 80 % est lié à l'hameçonnage. Si l'on réduit l'hameçonnage, on réduit le préjudice des autres délits que nous abordons au quotidien.

En deuxième lieu, il y a une attaque plus focalisée, avec des domaines qui semblent de vrais domaines, ou de faux e-mails. Et là, il peut y avoir un peu de superposition aussi.

Diapo suivante, s'il vous plaît.

Nous avons fait la même chose pour les entités de charité. 80 % correspondent à l'hameçonnage. Ici, il y a une analyse qui montre que l'on peut aider à aborder l'hameçonnage et l'utilisation malveillante du DNS. Et finalement, on réduira les délits qui affectent ces entités de charité.

Dans le Royaume-Uni, nous avons un service qui s'appelle le service de dénonciation de courrier suspect. Ici, les personnes physiques ou les

sociétés peuvent dénoncer les courriers suspects au gouvernement. Ils doivent donner certains détails, et aussi pour les messages de texte. Ils peuvent le faire par messages de texte qui sont à l'origine de dénonciations sur l'hameçonnage. Au cours de 2022, on a reçu 6 400 000 dénonciations dans notre service. Nous voyons qu'il s'agit d'une question à grande échelle, avec un grand nombre de victimes. Au Royaume-Uni, il y a un grand nombre de personnes qui font de dénonciations à cet égard.

Et en 2020, lorsqu'on a lancé ce service, nous avons une partie des réponses par la pandémie, mais depuis le lancement, on arrive à plus de 15 millions de dénonciations, 15 800 000.

Alors, c'est bien de pouvoir voir ceci dans un graphique au fil des ans.

Au sein du gouvernement, ce que l'on voit à partir de ce rapport sur les dénonciations, ce que l'on voit, c'est que l'on essaie de simuler que ces acteurs sont des entités gouvernementales. Parmi ces attaques de l'hameçonnage, ils essaient de feindre par exemple qu'ils font partie du service de santé ou des organismes qui ont une licence pour l'exploitation de télévision, ou l'administration des douanes, ou des entités de ce type, ou des conseils sur le COVID données par le gouvernement ou les permis de conduire. Donc il y a beaucoup d'attaques concernant des entités gouvernementales. Et ce service essaie de récupérer l'information à cet égard.

Alors, il est évident que lorsqu'on parle des individus et des utilisateurs d'Internet, bien sûr, ils sont affectés quand ces délits sont dénoncés ou sont rapportés.

Il y a une révision téléphonique d'un grand nombre de victimes qui a été rapportée pour comprendre quel était l'effet au point de vue financier. Comme vous pouvez le voir ici, il s'agit d'un graphique épouvantable. Je vous demande de m'excuser, mais c'est ce qu'on m'a donné. Mais comme vous pouvez le voir, il y a une fourchette allant de 20 à 250 livres. Et c'est le montant des pertes. Mais quand on y réfléchit, ce n'est pas beaucoup d'argent. Mais on a ensuite 6,4 millions de personnes qui ont dénoncé ce délit. Et si chacune de ces personnes ne perd qu'au moins 20 livres, multipliez par 6,4 millions ; c'est vraiment beaucoup d'argent en fin de compte. Donc c'est plus qu'une journée de travail. Donc cela peut être vu à une grande échelle. Et en particulier avec la crise et le coût de la vie que nous voyons dans beaucoup de pays. C'est vraiment extraordinaire et c'est vraiment terrible que les personnes puissent perdre tout cet argent.

Prochaine diapo.

Nous parlons beaucoup aussi de l'argent par rapport au cyberdélit. Ce n'est pas seulement un effet négatif pour les personnes quant à l'argent. Les entreprises sont aussi affectées. Au niveau individuel, l'impact peut être différent. Il se peut que les gens se sentent mal à l'aise au point de vue émotionnel. Nous avons eu un cas d'étude à cet égard. Nous avons reçu une certaine information concernant une victime âgée de 17 ans où le pirate informatique demandait beaucoup plus d'informations sur ses mots-clés pour accéder à ses réseaux. Nous avons pu identifier le suspect. Nous avons vu qu'il avait un historique de piratage dans les réseaux sociaux sur un grand nombre de personnes. Nous avons trouvé son adresse personnelle pour aller le voir

et nous avons trouvé un grand nombre de téléphones actifs qu'il utilisait pour commettre ces délits. C'est là que nous avons vu. Nous avons pu voir une évidence, enfin, des preuves très nombreuses d'hameçonnage.

Prochaine diapo. Donc, nous avons là un exemple de l'une des communications de la sorte. Nous voyons ici que la personne se présente comme si c'était quelqu'un qui avait trouvé l'information sur un individu et qui disait « Ben voilà, j'ai trouvé ceci. Ceci ». L'autre personne répond et donne le lien pour aller sur une page. Et donc la personne met un autre lien pour que la personne victime puisse avoir accès à ces liens. Lorsque nous avons revu ces numéros de téléphone, nous avons trouvé des centaines de messages qui consistaient en des attaques à des petites filles ou à de jeunes filles pour avoir accès à leur compte. Donc un domaine où une personne peut avoir des centaines de victimes. Alors, nous pouvons dire qu'un nom de domaine avec des centaines de victimes, cela dépend du type de logiciel malveillant, du type d'attaque qui est menée à bout.

Nous avons regardé ce site Web aussi pour voir comment l'individu se servait de ces éléments pour enfin faire du chantage à ces personnes.

Excusez-moi. Les diapos ont beaucoup de diapo-- pardon, beaucoup d'informations avec une typographie très petite. Mais bon. Mais c'est petit pour une raison spécifique. En haut, à gauche de l'écran, on voit un service d'hameçonnage, où l'on voit que la personne peut acheter des pages d'hameçonnage pour qu'il puisse avoir cela sur Internet. Il clique là. Cela peut être Netflix, Facebook, Snapchat, où d'autres applis, et on peut même choisir la langue. C'est tout petit ici, mais cela existe

en anglais, en espagnol, en français et en russe, je crois. Et je pense, on peut choisir la langue. D'après ce que je comprends, vous payer pour ce service. Et dans la partie de gauche en bas, lorsque vous cliquez là, cela va créer un [domain] malveillant qui envoie un message et qui collecte les détails. À droite en bas, vous trouvez le *dashboard* qu'il crée, où l'on voit toutes les accréditations qu'ils ont pu obtenir. Et à partir de là, ils peuvent enfin faire du chantage à de personnes. Parfois, il se peut qu'il s'agisse d'un Google Drive n'est pas partagé dans les médias, dans les réseaux sociaux.

Nous avons pu enfin mettre ceci doit hors service avec l'aide du bureau d'enregistrement. Et cette personne a dû faire face à des procès judiciaires dans le mois suivant. Mais pour le moment, il a été enfin mis sous arrêt, parce que c'est une menace pour un grand nombre de victimes.

Bien sûr, nous avons communiqué avec chacune de victimes que nous avons pu identifier pour leur dire que nous avons récupéré ces données et que nous les avons stockés dans un endroit sûr pour qu'ils puissent changer leur mot de passe et pour savoir quel a été l'impact pour ces personnes-là. Nous avons reçu des commentaires qui disaient « Ah, merci. Je ne savais pas comment résoudre ce problème ».

C'est donc une question clé que de savoir comment résoudre ce problème et éliminer ou enfin ces dommages que l'on cause à d'autres personnes.

Je cède la parole à Laureen.

LAUREEN KAPIN : Je me demande où nous en sommes, pour voir si notre collègue Bertrand est [préparé] pour faire sa présentation. Que faisons-nous ?

CHRIS LEWIS-EVANS : Excusez-moi, j'ai encore une diapo. C'est juste pour faire un résumé de ce qui concerne les données des sociétés commerciales, des entreprises.

Le rapport récent est un rapport de 2020-2021.

Au Royaume-Uni, on a reçu 875 000 rapports concernant la fraude, de cyber -– pardon, de cyberdélit. Cela représente une perte de 3,5 milliards. 80 % de cette fraude était facilité par des questions cybernétiques, qu'il s'agisse d'hameçonnage ou d'autres points.

Une bonne partie de ces pertes était due à un certain type d'activités qui étaient basées sur l'informatique. Ces courriers électroniques d'hameçonnage représentaient 80 %. Cela facilite aux criminels ou aux délinquants de, disons, effectuer ces attaques informatiques et ces fraudes.

GABRIEL ANDREWS : Pouvons-nous voir le prochain-- la prochaine diapo ?

[Au point de vue] des États-Unis et comme Chris l'a dit, nous espérons qu'il y aura d'autres personnes parmi lesquelles vous puissiez encourager vos organismes d'application de la loi pour qu'elles partagent-- pour qu'ils partagent l'information dont ils disposent.

Le FBI a présenté son rapport de l'année 2022 sur le cyberdélit. Ces données sont un résumé de toutes les plaintes portées par les victimes,

qui parviennent à notre centre de cyberdélit. C'est un portail central où nous recevons ces chiffres-là. Et ensuite, [ils publient ou ils préparent] des rapports sur cette base. Bien sûr, ce n'est pas un tableau complet de tous les cyberdélits qui existent.

Dans cette diapo, voilà, au cours des cinq dernières années, l'IC3, qui est le centre de dénonciation du délit, a reçu une moyenne de 200 dénonciations quotidiennes. Mais cela ne représente pas la vérité ou la réalité du délit qui se produit ou qui a lieu. Parce que nous n'avons pas toujours des dénonciations.

Excusez-moi. C'est 650 000 dénonciations par an qui peuvent arriver jusqu'à 2000 dénonciations par jour. Le volume des pertes a augmenté. Et je voudrais avoir une bonne explication par rapport à la raison de cela. Mais nous n'en avons pas pour le moment. Mais c'est important et c'est intéressant de faire remarquer cela. Et cela prouve que les dommages continuent d'exister, même si le nombre de dénonciations reste stable.

Comme Chris l'a dit, dans sa catégorie de délit, nous ne faisons pas de suivi de l'utilisation malveillante du DNS comme une catégorie, mais il y a des catégories qui sont suivies dans nos rapports d'IC3.

Ici en bas, on parle de l'hameçonnage. Quand nous voyons les premières cinq catégories où l'on voit les dénonciations. Et nous voyons que l'hameçonnage fait partie des cinq premières. Et nous voyons que, au cours des cinq dernières années, pour une raison ou

[l'autre], l'hameçonnage a énormément augmenté au cours des cinq dernières années d'après les dénonciations que nous avons reçues.

Encore une fois, c'est quelque chose qui montre toutes les catégories de délits, non seulement les cinq principales et comment l'hameçonnage est lié à tout cela. Comment cela est lié.

L'hameçonnage, même s'il est suivi dans sa propre catégorie, c'est, à l'origine, la méthode initiale que les délinquants utilisent pour engager les victimes dans d'autres types de délits. Comme un exemple, le logiciel-- le [*Ransom* logiciel] est un type de problème. On finit par payer pour le [*Ransom*] logiciel. Mais si on reçoit un [*Ransom* logiciel] propagé par l'hameçonnage, oui ; la réponse est oui. On a reçu un rapport de Royal Ransmoware. C'est l'une des agences qui fonctionnent comme nous. Et on disait que 67 % de ces infections de rançon logicielle venaient d'hameçonnage.

Donc, nous faisons un dépistage des catégories initiales, mais cela a un impact [à un aval] pour, disons, pour parler clairement de cela, lorsque nos collègues au niveau des bureaux d'enregistrement ou des titulaires de nom de domaine, quand il faut prendre des mesures pour voir comment résoudre le problème lorsqu'il est un hameçonnage, ils se servent non seulement du rapport qui nous parvient quotidiennement ou couramment, mais aussi d'autres catégories qui sont disponibles pour ce faire.

En plus du partage des statistiques sur le rapport annuel, j'ai demandé à un grand nombre de mes collègues quelle est la nouveauté. Qu'est-ce qui se passe, qu'est-ce qui arrive maintenant ? Quelles sont les tendances au cours de ces derniers mois.

Et ce qu'on nous a dit, c'est qu'on appelle cela *malvertising* ou publicité malveillante. C'est une espèce de combinaison de logiciels malveillants et de publicité.

Cela a suscité l'attention l'année dernière. Et ainsi que pour l'hameçonnage, le délinquant obtient un réseau, un nom de domaine, qui lui permet d'avoir un nom de domaine qui regarde ou qui ressemble à une marque fiable, et ils se servent de cela pour le courriel. Et dans les moteurs de recherche. Et ils achètent des publicités.

Comme vous pouvez le voir dans la diapo, ceci vient du feed de Twitter de CH. Le délinquant se fait voir là comme s'il avait une page Web semblable au vrai site Web. On ne le partage pas, parce que c'est des [braves jaunes]. C'est tout simplement qu'ils vont au site publicitaire de ce délinquant, en haut, et on recevrait ce même logiciel avec le logiciel malveillant. C'est une espèce de trojan. Si l'on s'inscrit ou l'on rentre dans ce logiciel, on peut enfin trouver l'argent ou les données de quelqu'un, si c'est par exemple un compte bancaire. C'est une nouvelle tendance. Ce n'est pas de l'hameçonnage, mais cela ne vient pas d'une connexion e-mail. Mais bien sûr, le résultat final est lui-même.

Pourquoi je parle de ça ? D'abord, parce que c'est quelque chose de nouveau. Et parce que c'est directement lié au DNS et son utilisation malveillante. Et enfin, parce que nous devons faire quelque chose d'agile et de rapide par rapport à ce qui se passe partout dans le monde, et tenir compte de ces nouvelles tendances pour la manière dont nous combattrons ce type de problème.

Mais comme je l'ai dit tout à l'heure, les bureaux d'enregistrement responsables qui prennent des mesures par rapport à ces enregistrements de noms de domaine, c'est important.

Pour moi, c'est ma dernière diapo. Je veux mettre l'accent sur ce point. Je veux faire remarquer que l'hameçonnage, comme tous les membres le connaissent, le savent ici au sein de l'ICANN, c'est une partie de l'utilisation malveillante du DNS. J'ai appris dans un rapport que c'est le premier et le plus important par le nombre de cyberdélits qui sont enfin dénoncés.

Une action rapide pour ces domaines enregistrés de manière malveillante, c'est très important.

Je vous remercie de votre attention. Et je crois que nous sommes prêts pour changer.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Allez-y, Bertrand. Merci beaucoup à l'équipe de juridiction de l'Internet. Merci de [ton] travail lié à l'utilisation malveillante du DNS. C'est une question qui nous intéresse beaucoup.

BERTRAND DE LA CHAPELLE : Merci, Manal. C'est un plaisir d'être encore une fois ici, au GAC. Je venais il y a des années comme représentant de la France. J'ai même été vice-président du GAC. Je vois beaucoup de visages très connus de l'époque, et c'est un plaisir de pouvoir faire cette présentation.

Je suis le directeur exécutif du Réseau de politiques Internet et juridiction. C'est une organisation fondée il y a 10 ans. Et j'ai le plaisir, je répète, de venir vous parler du débat qui a [créé intérêt] dans la communauté de l'ICANN.

Je veux vous raconter à quoi nous avons travaillé pour avancer dans notre tâche et trouver des solutions. Notre réseau, eh bien, ici, il y a le directeur du programme. Et en réalité, c'est une initiative multipartite qui convoque les gouvernements, les entreprises, les opérateurs techniques, les membres du secteur universitaire, la société civile, les organisations internationales, pour aborder les questions de juridiction liées à l'Internet.

Dans cette diapo, vous voyez que nous avons trois programmes ; je ne vais pas m'arrêter dans les deux premiers, mais l'un d'eux correspond à la question des domaines et des juridictions et quand ils correspondent au travail au niveau du DNS pour éviter l'utilisation malveillante. Il y a un groupe de contact qui a travaillé pendant plus de cinq ans avec 40 membres de différentes communautés. Manal et d'autres membres ont participé activement à cette activité-là. Et je suis vraiment reconnaissant à Manal de la haute responsabilité qu'elle a assumée avec sa participation très importante.

Vous passez à la diapo suivante, s'il vous plaît. Ce qu'il faut souligner c'est que, ici, on parle de la manière dont on travaille contre l'utilisation malveillante du DNS. Ces types d'abus sont différents.

Dans la présentation que nous venons de voir, on montre que l'astuce humaine n'a pas de limite. Tous les moyens pouvant faciliter l'utilisation malveillante seront utilisés pour ça.

S'il s'agit d'un problème transnational, il est intéressant de le souligner ici parce que, vous, vous êtes des représentants des gouvernements. Moi-même, j'ai été un représentant gouvernemental. Et nous savons tous que la raison pour laquelle nous avons un problème pour ce qui concerne l'utilisation malveillante en ligne, c'est que nous n'avons pas les outils de coopération entre les gouvernements pour pouvoir agir au niveau transnational. On a une architecture internationale basée sur les différentes souverainetés. Alors, un des programmes dont nous disposons fait référence à l'accès transfrontalier de « l'évidence électronique », et cela est vraiment problématique. Nous avons travaillé pendant des années pour faire la diligence raisonnable en utilisant les preuves électroniques.

Alors, on se voit face à cette situation. Non seulement il s'agit d'un réseau mondial. Non seulement les acteurs ont des fins malveillantes et travaillent au-delà des frontières, mais il faut aborder cela de cette manière. Et on n'est pas efficace. Alors là, on a besoin de faciliter la coopération entre les gouvernements.

Pour pouvoir résoudre ces problèmes, il faut mieux comprendre comment fonctionne l'Internet. Lorsque l'on parle du système, c'est-à-dire du DNS, il y a un manque de connaissances dans certains sites. Vous avez vu que, bien des fois, on ignore le fonctionnement de cette architecture. Alors si on veut savoir comment contacter un bureau d'enregistrement, nous allons trouver la fonction WHOIS pour arriver au bureau d'enregistrement. Et ce n'est pas si simple que ça.

Il y a quelque chose d'important aussi. Je parlais du manque d'outils, mais il y a une question qui a trait aux compétences. Les opérateurs du

DNS mettent à disposition les noms de domaine. Et ils n'ont pas de compétences pour analyser si c'est de l'hameçonnage, du logiciel malveillant ou quoi que ce soit. Lorsque l'on parle de contenu ou des utilisations malveillantes liées au contenu, comment on fait pour gérer toute la question de la légalité des contenus avec ce mélange juridictionnel, si l'on veut. Et pour travailler sur une si grande question, cela prend du temps.

En conséquence, cela devient un problème pour tous les acteurs. Pour les gouvernements, parce que vous, vous êtes légitimement préoccupés. C'est un problème que l'on ne peut pas résoudre. C'est un problème pour les entreprises, parce qu'elles ont la responsabilité aussi d'aborder la question. Et aussi pour les utilisateurs.

Alors, nous devons comprendre quelque chose qui est assez simple et que vous connaissez, mais je veux le partager avec vous. Normalement, je le partage avec des personnes en dehors de notre environnement. La relation entre le titulaire, le bureau d'enregistrement, l'opérateur de registre et les utilisateurs. Les consultations qui vont d'une entité à une autre et les règles que les différents secteurs utilisent pour que l'Internet fonctionne de la manière dont elle doit fonctionner.

Voici une architecture que je peux expliquer, mais il y a quatre actions que les opérateurs de DNS peuvent prendre.

La première, c'est de bloquer le domaine. En fait, on ne peut pas modifier l'information donnée par le titulaire du nom de domaine. On ne peut pas faire de transfert, des suppressions, des modifications. Et on ne peut pas changer non plus le serveur ou l'adresse IP.

Il est important de signaler que cette action ne fait pas en sorte que le contenu soit inaccessible. On peut le bloquer, c'est bien. Mais ça ne change rien par rapport au fonctionnement.

Le deuxième élément, c'est la suspension. En ce sens, c'est-à-dire le mettre en pause. On l'enlève. On le supprime du fichier de la zone racine du TLD. Alors il n'y a pas de résolution. On ne peut pas modifier non plus l'information dans le serveur. Mais le système continue à fonctionner. On utilise l'adresse IP. Et alors là, on peut accéder à cet élément qui est mis en pause. Puis on a le redirectionnement. Cela, pour pouvoir faire du *sinkholing* du domaine, où l'on édite le fichier de zone pour faire le redirectionnement dans un autre serveur et ainsi identifier les victimes et analyser le comportement.

Le troisième et quatrième éléments ont trait au transfert. Lorsque l'on passe cela à un autre bureau d'enregistrement. Par exemple, l'enregistrement a été mal [faite] chez un bureau d'enregistrement particulier, alors on fait le transfert. Et on l'envoie à un bureau d'enregistrement de dernière ressource. Et Benedetta travaille très activement là-dessus.

Nous pouvons savoir aussi l'élimination ou la suppression, mais ce n'est pas une action recommandée pour plusieurs raisons. Agir au niveau du DNS avec ces quatre actions, c'est justement le traitement correct pour aborder la question du DNS. La réponse est oui dans certains cas, et non dans d'autres cas. Ce n'est pas la panacée. Il y a des gens en dehors de nos communautés qui ont tendance à considérer cela comme un grand panel de contrôle. S'il y a un problème, on fait clic quelque part et on

l'arrange. Ce n'est pas comme ça. Mais bon, il y a des actions disponibles.

Les questions clés à résoudre sur les suivantes. Ceci, c'est un instrument qui sert non seulement pour le [service d'accéder] à un site, à un nom de domaine, mais aussi à bien d'autres services auxiliaires comme le courrier électronique, etc. C'est un instrument qui a un impact à l'échelle mondiale. Ceci affecte tout le monde. Il n'y a pas de blocage géographique. Là, on peut avoir une fonction ou un défaut. Si c'est un défaut, eh bien, peut-être il n'y a pas d'impact global.

Mais que se passe-t-il quand il n'y a pas de coopération internationale ? Bien des fois, le fait d'avoir cet effet global peut être bénéfique. Puis, on peut accéder à la plupart des services à travers l'adresse IP. Les opérateurs DNS font partie de l'écosystème, et il faut tenir compte de l'architecture dans son ensemble. Les fournisseurs de services Internet et d'autres fournisseurs qui peuvent mener des actions et agir au niveau correct, c'est quelque chose de très important.

Dans les contrats d'accréditation de bureau d'enregistrement et de registre, on établit les obligations par rapport aux points d'identification d'utilisation malveillante et [mener] des requêtes. Il faut préciser ce qu'il faut faire.

Alors ceci nous amène à une situation où nous avons été témoins pendant longtemps qu'il y a eu un débat prolongé au sein de l'ICANN, il y a quelques années, sur le terme « utilisation malveillante du DNS » et quelle est la signification. Il y a eu différentes positions à cet égard. Nous avons eu pas mal de séances pour définir l'utilisation malveillante du DNS. Il y a eu des critiques mutuelles entre unités constitutives, des

tensions au sein de ces unités. Et il ne suffit pas de dire que ce sont des agents malveillants ou des délinquants. Ça, on le comprend bien. Mais il n'y a pas une manière claire de parvenir à un consensus ici. Si l'on fait la question incorrecte, nous n'aurons pas la réponse correcte.

Alors là, il faut reformuler le problème. Et reformuler le problème veut dire voir quand est-il approprié d'agir au niveau du DNS pour aborder l'utilisation malveillante en ligne. En fait, on peut être tous d'accord avec cette formulation, mais il faut analyser les différents éléments.

Comme partie de cette reformulation, nous avons travaillé avec le groupe de contact pendant longtemps. Nous avons essayé de réduire les possibilités pour comprendre l'utilisation malveillante du DNS, que nous avons appelé utilisation malveillante technique. Mais avec l'aide de plusieurs acteurs, nous disons que l'utilisation malveillante du DNS devrait être considérée comme ces cinq situations : logiciels malveillants, réseaux zombie, hameçonnage, *pharming*, et spam.

Et nous pouvons trouver davantage de détails sur la définition de ces cinq situations dans les approches opérationnelles que notre réseau a produites en 2019, et [qui a] amené à l'incorporation de ces définitions sur l'utilisation malveillante du DNS dans le cadre du travail sur l'utilisation malveillante pour les agents au sein de la communauté en décembre 2019 et, par la suite, le rapport du SSAC, le SAC-115 de 2021, qui incorporait cette définition de l'utilisation malveillante du DNS.

La définition peut ne pas être parfaite. Mais c'est un élément très important pour distinguer entre ceci, que l'on peut définir comme l'utilisation malveillante du DNS, où tous les acteurs comprennent qu'il

y a une raison pour mener la recherche. Et ceci, c'est de la compétence des opérateurs de registre. On peut faire la différence.

Alors, nous avons produit -- et je ne vais pas rentrer dans les détails, mais on a produit un ensemble d'outils en 2021 pour aider les opérateurs du DNS, les législateurs, les organismes d'application de la loi, pour qu'ils comprennent les différents paramètres et qu'ils possèdent les éléments pour travailler ensemble.

Dans la diapo suivante, on mentionne un élément important, à savoir un flux de travail avec quatre éléments, qu'il faut considérer lorsque l'on aborde l'utilisation malveillante.

Donc l'identification de l'utilisation malveillante peut se faire par les notifications par les opérateurs eux-mêmes. Le deuxième élément concerne l'évaluation de cette utilisation malveillante. Est-ce que cela justifie une action au niveau du DNS. Ensuite, quelle est l'action qui doit être mise en œuvre sur ces quatre que j'ai mentionnés -- parmi ces quatre que j'ai mentionnés.

Il y a une cinquième mesure qui doit être prise, que je n'ai pas encore présentée, à savoir quelles sont les voies pour avoir des ressources quand il faut changer une décision. Il peut, bien sûr, y avoir des erreurs.

Pour chacune de ces étapes, nous avons produit un grand nombre de points, comme par exemple une meilleure définition de type d'utilisation malveillante, la mention des éléments concernant le type de notificateurs qui doivent être utilisés par rapport à la diligence raisonnable pour documenter ces éléments. Il ne s'agit pas seulement de donner une notification sans avoir des preuves qui soient

consistantes. Quelles sont les conditions [pour donner] au bureau d'enregistrement ou au titulaire de nom de domaine quand il y a ce type de délit ? La question clé est aussi celle qui concerne le critère des seuils pour ce type d'action : de quoi on a besoin pour parvenir à ce seuil.

Quant au type d'action, il y a un document qui explique très précisément les images que je vous ai montrées tout à l'heure.

Et enfin, quant à la ressource et au recours, il y a une question concernant les canaux pour le recours et les éléments concernant la transparence. Voilà pour le processus. Tout ce qui est lié aux recherches pour identifier et remédier à l'utilisation malveillante concerne la coopération entre les différents acteurs.

Dans ce contexte, nous avons produit un groupe [inaudible] qui a produit une série de documents dont j'espère que vous pourrez vous servir en tant que communauté, mais dont on pourra débattre aussi.

D'abord les notifications doivent être composées par quelle série d'éléments. De quoi a-t-on besoin pour avoir des preuves ?

Deuxièmement, quels sont les types de notificateurs ? Est-ce que c'est la même chose que d'être un notificateur d'images d'abus sexuels pour les enfants ou le fait qu'il y ait des manquements à certaines règles concernant des marques déposées, par exemple ? Et quelle est la diligence raisonnable des notificateurs pour s'assurer que la charge de valider cela n'est pas seulement du ressort des opérateurs ? Quels sont les types d'accord qui peuvent être passés entre les notificateurs fiables ?

Maintenant, je veux clarifier cela. Personne ne peut dire pour son propre compte que lui ou elle est un notificateur fiable. Il peut dire qu'il a une expertise dans ce domaine, qu'elle fait cela comme un notificateur expert, mais un rapport avec un notificateur fiable doit être une communication bilatérale. On peut être un notificateur fiable pour un opérateur et pas pour un autre. C'est une distinction importante qu'il faut établir.

Un document dédié s'occupe aussi de la question des réseaux zombie. Je n'ai pas le temps pour rentrer dans le détail, mais c'est un thème très important concernant des domaines qui ont été générés par des algorithmes. Il faut trouver une meilleure coopération entre les organismes d'application de la loi, l'ICANN et les opérateurs du DNS autour de ce thème, et c'est quelque chose de très important. Je pense que nous pouvons en parler dans l'avenir.

Nous avons enfin l'hameçonnage et le logiciel malveillant. Nous avons parlé avec les groupes de contact pour avoir un organigramme clair des différents rôles dans les différentes étapes entre les bureaux d'enregistrement et les titulaires de nom de domaine et le canal d'information dont ils se servent.

Je me sens très heureux de pouvoir mentionner, puisque Graeme Bunton est ici et vous l'avez vu tout à l'heure. Cela a mené-- a débouché sur de bonnes initiatives, et j'en suis bien heureux, qui ont été enfin bâties sur la base du travail que nous avons dans le I&J [PN] et le PIR. C'est une information dont nous avons parlé dans le groupe de contact, où l'on parle du rapport de cette utilisation malveillante, appelé NetBeacon.

Brian et son collègue ont été responsables pour cela et ils sont les coordinateurs de ce groupe de contact disponible dans I&G [PN]. C'est le résultat de cinq années de travail qui ont donné lieu à des éléments concrets, quelque chose opérationnel. Ce n'était pas seulement du papier ou des discussions ; c'est quelque chose de vraiment opérationnel. Et je tire mon chapeau pour eux d'avoir fait ce travail. Ceci est important parce que cela a donné lieu à des discussions qui ont eu lieu ici, à l'ICANN 76, concernant les améliorations qui ont eu lieu pour les contrats d'accréditation.

On est en train de parler de l'utilisation malveillante du DNS. Et cela doit être compris comme les cinq éléments dont nous avons parlé et dont nous sommes en train de parler.

Prochaine diapo.

Pour résumer, il y a un accord entre les acteurs responsables, en ce sens que l'utilisation malveillante du DNS ainsi comprise, c'est quelque [sorte] qui est vraiment justifié pour agir au niveau du DNS lorsque l'on a suffisamment de preuves, à moins que l'on est-- enfin, que le site soit compromis ou qu'il y a d'autres choses. Mais nous pensons que nous sommes dans la bonne voie, dans la bonne direction, pour avoir une coopération qui puisse être mise en œuvre.

Enfin, je veux aborder la question du contenu de l'utilisation malveillante, qui se rapporte [inaudible]. C'est plus complexe parce que c'est un peu comme si cette image était une espèce de mirage.

Au niveau du DNS, ce n'est pas bon de voir cela par rapport à la conclusion. Comme ce n'est pas suffisamment détaillé, c'est difficile de

le mettre dans la catégorie des questions légales ou illégales où que l'on soit. La compétence par rapport à ce qui est une utilisation malveillante, c'est difficile et les opérateurs ne le savent pas facilement. Ce n'est pas un outil efficace parce que le contenu est toujours disponible pour beaucoup de cas. Il y a certaines situations où il y a un travail exceptionnel— enfin, où c'est exceptionnel lorsque l'on a à justifier l'action au niveau du DNS.

Ce que nous avons mis en œuvre en 2019, avant la conférence mondiale que nous avons organisée à Berlin, il y avait quatre éléments qui pouvaient être pris en compte pour savoir quand il faut pour évaluer, pour savoir quand il faut agir au niveau du DNS, en ce qui concerne l'utilisation malveillante par rapport au contenu et pour comprendre comment le contenu est illégal ; si le contenu est illégal.

Est-ce qu'il y a eu un accord au niveau mondial ? Il y a une diversité par rapport à la législation partout dans le monde pour ce qui est de ce qui est légal ou pas. La proportion du site qui est consacrée à un contenu qui enfin est illégal ou qui enfreint les lois, le propos de cela concernait la bonne foi ou la mauvaise foi du titulaire du nom de domaine ou de l'opérateur du site. Et il faut savoir aussi si d'autres niveaux ont été utilisés en ce qui concerne l'opérateur du site ou le titulaire d'enregistrement ou le fournisseur d'hébergement. Il faut faire donc la différence entre ces deux catégories ; les deux sont importantes, mais il ne faut pas les aborder de la même manière.

L'un des grands défis à relever, c'est que nous n'avons pas d'espace pour pouvoir aborder le deuxième problème. L'ICANN est le lieu approprié pour discuter de l'utilisation malveillante du DNS, comme

nous l'avons dit tout à l'heure. Mais il a été vraiment clair que, selon les mandats -- et la communauté en ligne sur cela, c'est que l'ICANN n'est pas le lieu pour parler de l'utilisation malveillante concernant le contenu. Et il y a eu des publications de posts en ce sens que l'ICANN n'est pas une police qui s'occupe du contenu. Et ceci est complètement compréhensible. Le problème est qu'il n'y a pas d'autres lieux où l'on puisse parler de ce type de choses. C'est pourquoi, en mai 2022, une partie significative de ceux qui ont participé au groupe de contact de l'I&J nous ont demandé d'être le lieu où l'on aura des discussions concernant l'utilisation malveillante liée au contenu pour voir comment trouver les seuils, les mécanismes et les critères pour remédier à cela, et c'est ce que nous avons fait cette année.

Ce n'est qu'une action préliminaire. Cela ne fait que commencer. Mais je crois que c'est important pour cette communauté du GAC d'avoir un panorama plus vaste pour comprendre que l'ICANN fait des progrès par rapport au travail que nous avons fait sur l'utilisation malveillante du DNS. Ce n'est pas parfait ; il faut le mettre en œuvre, il faut le renforcer, mais il y a des progrès qui sont faits à cet égard : plus de clarté, plus de mécanismes, plus de coopération.

Et par rapport à l'utilisation malveillante concernant le contenu, même si ce n'est pas au sein de l'ICANN, nous, en tant qu'[IGPN], nous travaillons sur cette activité sur la base des éléments qui sont dans la diapo.

Le premier, les étapes d'utilisation concernant l'utilisation malveillante liée au contenu sont motivées par le fait parce que c'est le lieu où l'on va ou c'est le dernier recours que l'on peut avoir quand on est passé par

ce type de problème. La question est de savoir comment on communique avec l'opérateur du site, le titulaire de nom de domaine, le fournisseur de l'hébergement.

Le deuxième élément concerne la manière de définir le seuil pour ces exceptions pour se dire pour savoir si tout le site est consacré à l'activité illégale ou si l'on peut dire qu'il n'y a pas d'autres contenus illégaux sur le site. On peut dire que la tentative de l'opérateur du site est de faire ceci, ceci et cela. Donc nous facilitons les discussions à cet égard.

Enfin, il y a la notion d'atteignable, de quelque chose qui est atteignable. Lorsque nous avons une possibilité d'accéder à quelqu'un, comment faisons-nous pour communiquer avec le titulaire de nom de domaine, le bureau d'enregistrement, l'opérateur du site ou le fournisseur d'hébergement.

Nous allons chercher. Nous allons faire davantage de recherches, parce qu'il n'y a pas une clarté du WHOIS quant aux fournisseurs, quant aux hébergeurs, etc. C'est un peu plus compliqué quand on compare cela avec le bureau d'enregistrement.

Enfin, j'ai parlé des désaccords avec les notificateurs fiables. C'est un point très important, en particulier pour ce qui est de l'utilisation malveillante liée au contenu pour l'hameçonnage. Mais pour l'utilisation malveillante liée au contenu, il n'y aura pas de solution sans la coopération des trois catégories d'acteurs, à savoir les organismes d'application de la loi, les notificateurs des différentes ressources et recours qui doivent amplifier ou faire remonter leurs efforts, et les accords qui sont en vigueur.

Si vous vous rappelez la [formulation] de l'affirmation d'engagement entre NTIA et l'ICANN, il y a quelques années, il y a une notion du cadre de travail qui concerne une affirmation mutuelle des engagements. Nous avons besoin de mécanismes pouvant réunir les notificateurs, les organismes d'application de la loi et les opérateurs, pour qu'ils puissent tous aborder ces cas-là, quand il faut le faire au niveau du DNS.

Et je veux donc souligner que nous parlons non pas de la régulation de ces grandes plates-formes. Ce n'est pas les Facebook ou les Twitters de ce monde. Vous n'allez pas demander de désactiver facebook.com parce qu'il y a un contenu dans l'un des sous-groupes qui y sont présents. Mais lorsque quelqu'un établit un site Web derrière un nom de domaine avec une intention malveillante, le fait de chercher ces personnes, le fait de trouver ces personnes et de les arrêter, non seulement dans un seul site, mais chercher les personnes qui sont derrière ce site-là, voilà ce que nous devons faire. Voilà le type de coopération dont nous avons besoin.

Alors, il s'agit d'une responsabilité partagée qui demande la coopération des différents acteurs. Et ce modèle intersectionnel [est un modèle multipartite sert] à faciliter le travail entre les multiples parties prenantes. Et nous sommes heureux de dire qu'il y a eu des progrès dans l'environnement de l'ICANN. C'est la seule manière d'aborder ce type de problème.

J'ai perdu mon image. Bon. Mais il y a une diapo qui montre tous les liens pour voir les documents dont je vous ai parlé. Ici, dans cette dernière diapo, vous avez l'information de contact, les coordonnées de contact de Francis si vous voulez en parler avec nous après la séance.

Je vous remercie de l'occasion qui m'a été fournie.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Merci de votre présentation. Et je veux aussi remercier la personne d'Iran qui a levé la main. Après, je passerai la parole—

D'abord, je passe la parole à Chris.

CHRIS LEWIS-EVANS : Oui, on a eu beaucoup de contributions, beaucoup de participation. Si vous avez des questions ou des commentaires par rapport aux dernières présentations, nous pouvons le faire maintenant. Et on va aborder des activités en continu du monde de l'ICANN, et aussi voir ce que l'on va insérer dans le communiqué. Mais bon, si vous avez des questions, n'hésitez pas à les poser.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Kavouss, vous voulez dire quelque chose de la dernière partie de la séance ? C'est comme vous voudrez.

IRAN : Merci, Manal. Permettez-moi d'exprimer mes sincères remerciements à tous ceux qui sont ici dans le podium. À mon avis, c'est une des présentations les plus intéressantes que nous avons eues sur l'utilisation malveillante du DNS, bien que je ne souhaite pas faire de comparaison.

Mais à mon avis, la dernière partie a été extrêmement intéressante. Comme je l'ai mentionné hier, on a des problèmes. Et nous avons reçu certaines. Mais je recommande, très chère présidente et Nico le futur président du GAC, que dans l'ordre du jour du GAC de la prochaine réunion, on octroie davantage de temps pour aborder ce thème.

On ne peut pas le voir d'une manière superficielle sans approfondir comme il faut.

On n'a pas le temps. J'ai quelques suggestions. Je crois que nous pouvons avancer de cette manière.

Mais je voudrais faire référence à un point. Le collègue à droite du podium parlait de la coopération intergouvernementale. Cela a été discuté pendant très longtemps. Ce n'est pas une question de la compétence de l'ICANN, parce que l'ICANN n'est pas une organisation intergouvernementale. Le GAC non plus. Les gouvernements, c'est-à-dire, je suis très sincère avec vous ; beaucoup de fois, on veut aborder ce thème. On parle de la coopération intergouvernementale. Il y a toujours un gouvernement qui s'oppose.

Quand on parle du cyberdélit, on considère que c'est une question nationale qui ne doit pas être traitée à l'échelle internationale. Et on dit que toute coopération intergouvernementale pourrait être utile si cela aboutissait à un traité. Ce n'est pas possible d'avoir un traité en la matière. Alors il faut penser à approfondir la situation, pas dans cette séance, parce qu'on arrive presque à la fin. Mais très chère présidente du GAC, je vous propose d'accorder plus de temps pour la discussion de ce sujet parce que l'on a abordé quelques points très intéressants. Mais surtout, on a présenté les problèmes.

Jusqu'à présent, on n'a pas de solution proposée. Et ça, c'est important. Bien des fois, c'est plus facile de poser le problème, mais ce n'est pas facile du tout de suggérer la solution. Où sont les solutions ? Et il est nécessaire d'avoir une approche pragmatique. Pas voir ce que l'on peut faire suivant la législation, mais plutôt hiérarchiser ce que l'on peut faire. La coopération intergouvernementale n'est pas si simple que ça en ce moment, mais il y a bien d'autres aspects que nous pouvons traiter.

Nous avons reçu le rapport du Royaume-Uni et des États-Unis. Mais il faudrait demander aux membres du GAC où sont vos rapports. Moi personnellement, j'ai confronté ce problème. Il y a eu des plaintes, des dénonciations.

Hier, on a mené un appel diplomatique avec 10 % du prix. N'ouvrez pas ce genre de communication, parce que si vous avez une adresse de courrier et vous ne connaissez pas celui qui vous l'envoie, ne l'ouvrez pas, parce qu'immédiatement vous pouviez avoir des problèmes.

Et il y a d'autres approches pour les courriers ou les fournisseurs de courriers qui ont une double sécurité. C'est-à-dire, si le mode passe est pris ou séquestré par quelqu'un en plus de votre ordinateur de bureau, on ne peut pas l'utiliser avec un autre dispositif parce qu'il y a un autre. Le deuxième facteur de sécurité.

Donc il faut conseiller les individus, leur montrer les précautions qu'ils peuvent prendre pour réduire ce problème. Il y a bien d'autres questions à aborder. Je m'excuse d'être si franc, mais bon, c'est ce que je voulais dire. Merci.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Merci, l'Iran. Si vous me permettez, Chris, on a d'autres demandes de parole. Et peut-être vous pourrez répondre à tous. Il ne nous reste que 20 minutes, et j'ai la République démocratique du Congo et les États-Unis. Allez-y, s'il vous plaît.

RÉPUBLIQUE DÉMOCRATIQUE DU CONGO : Merci beaucoup, Manal et tous les membres du panel.

Comme Kavouss, je voudrais mentionner l'importance de cette présentation. Parce que depuis la perspective du gouvernement, pour la plupart des gouvernements, notamment les gouvernements de l'Afrique, les attentes vis-à-vis des représentants délégués auprès du GAC [a trait] au fait de pouvoir résoudre la question de l'utilisation malveillante.

Bien entendu, on parle d'utilisation malveillante, mais je voudrais demander s'il y a des actions à prendre au niveau gouvernemental pour la prévention. Parce qu'on parle ici de remédiation, mais, en français, on utilise une phrase pour ceci, et voir s'il y a des actions que nous puissions mener à bien.

Bien entendu, nous parlons de la cybersécurité où il y a des questions qui mettent en risque la souveraineté des nations. Mais il faudrait voir quel est le conseil pour les entreprises, pour les gouvernements. Que peut-on faire ? Parce qu'on a reçu une présentation du FBI aussi, du Royaume-Uni avec leurs expériences, mais je crois qu'il y a eu des études et des statistiques qui peuvent nous aider à comprendre pourquoi on a ce type d'utilisation malveillante.

Nous savons que pour les utilisateurs finaux, en général, le problème, c'est les courriers malveillants, l'hameçonnage, mais que peut-on faire pour prévenir tout ce type de problèmes.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Merci, le Congo. Je passe la parole à Chris d'abord.

ÉTATS-UNIS : Merci, Manal. Je n'ai pas de problème pour attendre la réponse du collègue.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Merci, les États-Unis. [Inaudible].

France : […] cette intervention plutôt pour nourrir les discussions. Voilà, je suis nouveau au GAC et j'ai cette impression qu'on ne prend pas le temps de resoulever certaines questions qui auraient pu être soulevées. Et peut-être qu'on va trop rapidement. Donc, je voulais simplement soulever quelques points, disons d'un point de vue d'un nouvel arrivant ici et explorer des pistes pour limiter certains abus. D'un point de vue extérieur, j'ai l'impression que la politique assez agressive et les prix avantageux proposés par certains acteurs conduisent à certains abus de noms de domaine. Et peut-être qu'il y a quelque chose à faire là-dessus. Par exemple, observer le taux de renouvellement. Des pistes qui pourraient créer un faisceau d'indices et peut-être aider la communauté à travailler dessus. Tous ensemble, on sait quels sont les

acteurs qui ne jouent pas véritablement au jeu. Et je pense qu'il faut aussi être capables de le dire et de trouver des moyens de les cibler et d'aller un peu, peut-être pas à la source du problème, mais certaines des difficultés qu'on observe, essayer de les mettre en évidence. Ça me semble être quelque chose d'intéressant à faire. Je vous remercie.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Merci beaucoup, la France. Je vois que le Rwanda a levé la main. Pourriez-vous, s'il vous plaît, être bref ?

Rwanda : Merci beaucoup. Je voulais tout simplement remercier les membres du panel, les orateurs, des rapports présentés par le Royaume-Uni et les États-Unis sur le cyberdélit.

Je crois qu'il faudrait une certaine précision. Nous sommes ici face à certains défis qu'il faut relever, provenant du cyberdélit, par rapport aux cryptomonnaies en particulier. Il y a des domaines qui sont fermés. Les personnes qui ont fait des investissements dans ce domaine-là perdent leur argent. Comment peut-on faire un suivi de ce type d'investissement ? Comment est-ce qu'on peut coopérer en ce sens ? Merci beaucoup.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Merci beaucoup, le Rwanda. Chris, je vous cède la parole. Excusez-moi d'avoir fait un peu de pression sur le temps [inaudible].

CHRIS LEWIS-EVANS : Merci, Manal. Et merci de la collaboration. Je vais essayer de résumer.

Par rapport au conseil de notre collègue de la France, nous n'allons pas ouvrir ceci ici. Il y a beaucoup de choses qui peuvent être faites. Vous pourriez peut-être vous servir de l'atelier de renforcement des capacités pour en parler dans l'avenir. [Ce serait peut-être que le GAC pourrait considérer]. Nous aurions besoin d'une séance beaucoup plus longue pour vous donner toute cette information. Mais vous pourriez peut-être considérer cette option.

Par rapport à ce que nous pouvons faire, NetBeacon, comme on l'a dit tout à l'heure, ici, est un outil de dénonciation. C'est un mécanisme d'action pour combattre ce fléau.

Mais nous savons qu'il y a de nombreuses activités en cours. Et je voudrais souligner certaines initiatives au sein de la communauté qui nous aident à travailler contre l'utilisation malveillante du DNS. Elles sont là dans ces diapos,

Et par rapport aux cryptomonnaies, je crois que cela se rapporte à ce que Bertrand a dit. Nous sommes passés de l'hameçonnage dans un courriel à l'utilisation malveillante du DNS, ou bien on est en train de parler d'une question liée au contenu ? Donc, quels sont les mécanismes qui sont impliqués dans cette situation ?

Si nous parlons des activités de la communauté, il y a beaucoup de travail en cours. Les opérateurs de registre qui travaillent pour partager leurs statistiques d'une manière volontaire. Les opérateurs de registre et les registres soutiennent, tous, cette tâche.

Il y aussi acidtool.com qui est un outil permettant d'identifier les fournisseurs d'hébergement et de courriels, les bureaux d'enregistrement et les titulaires de nom de domaine. C'est un outil qui permet de voir à quel point exact il faut s'adresser pour mener à bien des mesures efficaces. Il est important d'identifier ce point-là, voir s'il s'agit d'un revendeur, un registre, un bureau d'enregistrement. Je pense que c'est extrêmement important.

Nous faisons, encore une fois, référence à NetBeacon comme une méthode possible pour prendre des mesures. Et ceci est vraiment fortement aligné avec la recommandation du SAC-115. Nous avons eu une présentation très intéressante sur cela. Il s'agit d'activités qui nous aident à atténuer ce qui se passe en ce moment par rapport à l'utilisation malveillante.

L'Institut de l'utilisation malveillante du DNS a partagé son travail d'analyse en collectant de l'information sur les dénonciations d'utilisation malveillante du DNS.

Il se peut que je parle un peu trop vite pour les interprètes. Je leur demande de m'excuser. Je vais enfin essayer de réduire un peu ma vitesse.

L'équipe réduite de la GNSO s'est occupée des utilisations malveillantes du DNS. Elles ont été très actives. Et leurs trouvailles par rapport à ce type de problème concernent aussi ce qui a été dit dans le communiqué du GAC de La Haye. Par rapport à l'utilisation malveillante du DNS, il faut personnaliser cette recherche et ce travail pour que l'on ait des résultats qui soient utiles.

Comme cela a été dit tout à l'heure, je sais qu'il y a une frustration par rapport à ce qui se passe et que les mesures et les remédiations ne sont pas suffisamment rapides.

Au sein de l'ICANN aussi, il y a l'équipe de l'OCTO, qui travaille avec le système DAAR. Cela concerne l'analyse des données concernant 1145 gTLD. J'étais étonné du nombre de gTLD. Et il y a eu aussi 25 ccTLD. Et encore une fois, cela nous permet de mieux comprendre ce qui se passe pour pouvoir prendre des mesures efficaces.

Voilà donc un aide-mémoire concernant la voie qu'il faut prendre pour savoir avec qui il faut communiquer. C'est un espace un peu complexe. C'est une espèce de schéma de l'ICANN. Et c'est heureux de pouvoir utiliser cela ici parce que je ne serai pas capable de faire un schéma comme celui-ci. Mais il faut savoir à qui il faut s'adresser pour prendre la bonne mesure au moment approprié.

Donc, de mon point de vue, si nous faisons cela, nous allons réduire les dommages qui sont causés. Et ceci est très important quand on utilise des outils tels que NetBeacon, Acid Tool, et cela nous aide énormément.

Le panorama est un peu complexe. À droite, il y a le bureau d'enregistrement et le revendeur. Parfois, il y a un seul revendeur. Parfois, il y en a plus d'un. Donc c'est important de bien comprendre cela aussi pour trouver le point exact auquel il faut avoir recours.

Prochaine diapo, s'il vous plaît.

Pour marquer ce que nous avons dit à propos du revendeur pendant l'étape 1 du travail de l'EPDP, l'on avait recommandé ceci. Le bureau

d'enregistrement doit créer un élément des données du revendeur qui soit directement corrélé au titulaire de nom de domaine. À un moment donné, [il y a] un champ du revendeur. Mais cela n'existe pas toujours ni partout. Il faut que nous puissions trouver une manière de donner une réponse plus rapide et plus efficace. On a vu cela aussi dans la révision de la CCT.

Je cède maintenant la parole à Laureen. Excusez-moi d'avoir parlé aussi vite, mais je voulais bien sûr parvenir jusqu'à la séance des questions-réponses.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Laureen, nous avons déjà une question de la salle. Nous allons d'abord prendre cela si vous êtes d'accord. Nigel ?

Royaume-Uni : Laureen peut d'abord parler, et je peux poser ma question après.

LAUREEN KAPIN : Merci, Nigel. Je m'appelle Laureen Kapin, et je parle en tant que coprésidente du Groupe de travail sur la sécurité publique. Et l'un des thèmes dans ces thèmes très importants.

Prochaine diapo. Même si je suis heureuse de voir que cette séance a été interactive, même avant ce même moment, il y a eu beaucoup de discussions et beaucoup de points de vue et beaucoup d'informations, je vais reformuler ceci. Il y a beaucoup d'informations et de points de vue partagés. Et maintenant, nous en sommes au point où nous

voulons-- nous pouvons parler de ce que le GAC veut souligner dans le communiqué par rapport aux problèmes potentiels. Il faut répéter à plusieurs reprises, et c'est important, qu'il y a une catégorie sur les négociations de contrat entre les bureaux d'enregistrement et les registres et l'ICANN. Encore une fois, l'objectif de ce processus est d'améliorer les obligations contractuelles en ce qui concerne la prise de mesures pour atténuer ou diminuer les utilisations malveillantes du DNS. Et on parle d'obligation, non pas d'effort volontaire. Et on parle de cela, de ces obligations, parce qu'il faut refléter une obligation qui sera respectée par tous. Et cela concerne aussi les acteurs malveillants, ce qui permettra à l'ICANN d'avoir davantage d'outils légaux pour pouvoir lutter contre ces situations concernant l'utilisation malveillante du DNS.

Ce n'est que le premier pas, et il peut y en avoir d'autres dans l'avenir. Mais il se peut que ce soit un moment opportun pour que le GAC reconnaisse et que le GAC applaudisse ces efforts continus, ces efforts qui ont été le résultat des initiatives des parties contractantes. C'est une attitude proactive que nous acceptons toujours et que nous saluons toujours. C'est le premier pas parmi d'autres qui pourront être faits. Nous avons donc beaucoup de travail à faire en ce qui concerne la politique.

Et je veux enfin donner mon soutien à ce qu'a dit mon collègue de l'Iran. Il faut donner la priorité à ce thème pour pouvoir appliquer ces deux principes d'orientation pour tout PDP. Je sais que cela n'a pas toujours été fait comme une action rapide et focalisée, mais cela peut être fait dans ce contexte.

Nous pouvons avoir aussi des occasions pour davantage de négociations entre les parties contractantes et l'ICANN. Alors il y aura une occasion pour faire des commentaires publics, une fois que les parties contractantes auront présenté les résultats de leurs efforts que nous attendons anxieusement. Et il y aura ensuite des occasions pour que le GAC décide du type de contribution qu'il voudra présenter ou diffuser.

Prochaine diapo, s'il vous plaît.

Pour ce qui est des revendeurs, on a identifié aussi les problèmes. Et la raison pour laquelle cela est lié à l'utilisation malveillante du DNS, c'est par rapport à ce qu'a dit notre collègue Bertrand, c'est important de pouvoir avoir recours à l'entité pertinente, lorsque nous travaillons ou lorsque nous faisons face à un problème d'utilisation malveillante du DNS.

Nous avons aussi la contribution dans différentes formes concernant le rapport final de la CCT, et plus récemment, la première étape des recommandations des données d'enregistrement des noms de domaine.

Maintenant, je cède la parole à mes collègues du GAC pour qu'ils fassent leurs contributions et leurs commentaires par rapport à leurs idées par rapport à ce que l'on pourra inclure dans le communiqué du GAC. Et je sais que, comme nous avons peu de temps là-dessus, nous avons des séances de rédaction du communiqué. Mais ce serait le moment approprié pour savoir à quoi vous pensez, quelles sont vos idées à cet égard.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Merci beaucoup, Laureen. Il y a le Royaume-Uni, l'Iran et la Commission européenne. Et nous avons trois minutes. Donc j'espère bien que vous pourrez être brefs. Le Royaume-Uni.

ROYAUME-UNI : Merci beaucoup, Manal, et à vous tous qui êtes au podium. Vous avez présenté cette séance exceptionnellement utile, ainsi que d'autres membres du GAC l'on fait remarquer.

D'abord, quatre points que je veux marquer très rapidement.

Notre position par rapport aux négociations des contrats a été vraiment très positive. Nous avons eu la séance avec les bureaux d'enregistrement et les titulaires de nom de domaine. Cela a été une séance excellente. Nous attendons, nous espérons qu'il y aura cette consultation publique. Nous ne voulons pas interférer dans ces négociations. Nous attendons cette information mise à jour. Et comme je l'ai hier, c'est le premier pas. Et comme l'on dit d'autres collègues, il se peut qu'il y ait d'autres initiatives concernant l'EPDP lorsque nous considérons d'autres aspects de l'utilisation malveillante du DNS.

Pour ce qui est du communiqué, je crois que nous devons être clairs en ce qui concerne l'acceptation de ces initiatives. Mais nous devons aussi voir comment enfin marquer ces différentes idées qu'il faut enfin donner par rapport à l'utilisation malveillante. Et il y a certaines mesures à prendre avant de continuer avec le processus SubPro. Merci.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Merci beaucoup, le Royaume-Uni. Maintenant, il y a l'Iran. Et ensuite, nous allons finir avec le Japon.

IRAN : Merci, Manal. J'ai discuté avec des collègues très distingués, comme vous l'êtes, sur la question de l'utilisation malveillante du DNS. C'est une question qui s'étend sur le long terme pour l'ICANN. Et c'est quelque chose d'important.

Mais tout le monde, le Conseil d'administration, l'organisation de l'ICANN, les membres, tous ceux qui étudient la question savent que l'on n'a pas besoin de l'avis du GAC à cet égard. Permettons aux gens de réfléchir là-dessus, de disons analyser cela, et ne pas les pousser. Ils savent de quel problème il s'agit.

D'autre part, ce qui est important pour le GAC, c'est de mentionner d'abord qu'il faut reconnaître les négociations en cours entre le Conseil d'administration de l'ICANN et les parties contractantes des bureaux d'enregistrement et des opérateurs de registre.

Ensuite, il faut mentionner que nous avons besoin d'un progrès, un rapport de progrès, pour notre prochaine réunion de l'ICANN -- ICANN 77, à Washington DONC. Nous espérons que le rapport final sera présenté à l'ICANN 78 ou 79 ou 80, mais avec des mesures suffisantes pour pouvoir conseiller le GAC, aux gouvernements ou aux personnes du GAC, comment combattre ce problème, comme mon collègue l'a mentionné, et comment expliquer la situation ainsi que d'autres éléments qui apparaissent dans le rapport, ainsi que Laureen, Chris et Gabriel l'ont dit.

Il faut essayer de mettre l'accent sur l'importance de ces thèmes. Il faut travailler sur le texte pour que ce soit plus clair, plus précis et plus concis, et pour prendre des mesures de suivi à cet égard. Je ne pense pas que nous devions inclure quoi que ce soit sur l'utilisation malveillante du DNS dans l'avis du GAC en ce moment. Merci.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Merci, l'Iran. J'ai la Commission européenne et puis le Japon. Soyez brefs, s'il vous plaît. Bien.

COMMISSION EUROPÉENNE : Je serais brève. Je veux aborder les points [considérés] pour le communiqué tel que Laureen l'a demandé. Nous sommes définitivement d'accord sur ce fait en ce sens que nous avons demandé pendant longtemps tout cela. Donc, c'est quelque chose que nous devons soutenir.

Pour ce qui est de l'information additionnelle, il faudrait peut-être le faire dans la séance concernant l'utilisation malveillante du DNS. Nous pourrions ajouter d'autres questions importantes, comme par exemple l'importance des mesures de prévention. Nous sommes préoccupés en ce sens que ce que nous avons entendu jusqu'ici concerne les mesures actives, mais la prévention sur l'utilisation malveillante du DNS est fondamentale aussi. Et je l'ai entendu dire de deux autres collègues.

Et la possibilité d'explorer la question des incitations, qui a été soulevée par des collègues du PSWG à plusieurs reprises. Enfin, par rapport à ce que Nigel a dit concernant la prochaine série de nouveaux gTLD, nous voulons nous assurer que le travail précédent ne sera pas oublié, et en

particulier de ce qui est de mesures raisonnables pour empêcher l'utilisation malveillante du DNS.

Le GAC a fait un travail très important, en établissant le lien entre l'exactitude des données de nom de domaine et l'utilisation malveillante du DNS dans les communiqués 71, 72 et 73. Et je suis sûre qu'il y en a davantage. Essayons donc de ne pas perdre tout cela, lorsque l'on parle de la prévention du travail sur l'utilisation malveillante du DNS. Merci.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : [Cède la parole au Japon].

JAPON : Bonsoir pour vous tous. Bonne nuit, c'est le soir chez nous. Bonjour et bon après-midi pour tous les autres. Je m'appelle Nobu Nishigata. Je prends la parole au nom du Japon. Je remercie l'organisation de cette merveilleuse séance que nous avons eue aujourd'hui. Je veux répondre à la présentation de Laureen sur le communiqué.

Le Japon veut donner son soutien par rapport aux négociations des contrats qui sont en cours. Nous acceptons le travail qui a été fait jusqu'ici.

D'autre part, le Japon veut soulever une question concernant le contrat d'accréditation des registres, selon l'article 3.18.1, qui demande au bureau d'enregistrement de dénoncer des activités illégales.

Le gouvernement japonais continue à demander une amélioration de cela par rapport aux termes utilisés quand il s'agit de dénoncer ces

activités illégales. Il y a encore beaucoup de preuves qui peuvent être demandées, comme par exemple le rapport d'audit de l'ICANN, les rapports de la GNSO.

Le Japon s'attend à la présentation de ce rapport préliminaire et nous souhaitons pouvoir en discuter pendant la période intersessions à propos du progrès de ce travail et pouvoir exprimer nos inquiétudes.

Je voudrais de toute façon remercier de l'information mise à jour sur les négociations. Et nous sommes anxieux de pouvoir poursuivre cette discussion avec vous. Merci beaucoup.

MANAL ISMAÏL, PRÉSIDENTE DU GAC : Merci beaucoup, le Japon. Merci Bertrand, Gabe, Chris et Laureen. Merci à vous tous. Nous allons nous réunir un 3 heures, heure locale de Cancún. Soyez ici à temps pour la séance bilatérale. Merci beaucoup.

[FIN DE LA TRANSCRIPTION]