ICANN74 | Forum de politiques – Discussions du GAC : utilisation malveillante du DNS
Mardi 14 juin 2022 – 15h00 à 16h00 AMS

MANAL ISMAIL, PRÉSIDENTE DU GAC : Bonjour. Veuillez bien prendre place. Nous allons commencer dans quelques minutes.

Bien. Il est l'heure prévue. Bonjour, bon après-midi, bonsoir à tous. Bonjour à tous ceux qui sont dans la salle du GAC et à ceux qui sont connectés à distance. Bienvenue à la séance du GAC consacrée à l'utilisation malveillante du DNS et son atténuation, qui est censée durer 60 minutes.

Aujourd'hui, nous allons considérer les initiatives communautaires et de l'ICANN, et nous aurons des mises à jour à propos des évènements les plus récents, mais ce sera également l'occasion de continuer nos discussions par rapport aux initiatives les plus récentes du GAC pour pouvoir maintenir des rapports avec le reste des parties prenantes.

Comme vous le voyez à l'écran, nous avons un panel distingué. Il y a des présentateurs du GAC appartenant au Groupe de travail consacré à la sécurité publique, Gabriel Andrews, du Bureau fédéral d'investigation des États-Unis, Cathrin Bauer-Bulst, de la Commission européenne, coprésidente du PSWG du GAC, Laureen Kapin, de la Commission fédérale du commerce des

États-Unis et coprésidente du PSWG du GAC, et Chris Lewis-Evans, de l'Agence nationale du crime ou du délit du Royaume-Uni, également coprésident du PSWG du GAC. Nous aurons, par ailleurs, le représentant du Japon [près du Gabon] qui se connectera à distance, à savoir Teruyuki. On vous remercie beaucoup Teruyuki. J'espère que l'heure n'est pas trop dure pour vous, chez vous. Monsieur Teruyuki appartient au Ministère des affaires internes et des télécommunications. Finalement, mais non pas des moindres, bien sûr, nous avons un présentateur invité, Graeme Bunton, du DNS Abuse Institute, l'institut qui étudie l'utilisation malveillante du DNS.

Sans plus, je vais céder la parole aux membres de notre panel. Chris, je pense que c'est bien vous qui allez lancer la discussion.

CHRIS LEWIS-EVANS : Oui. Merci, Manal. Bonjour à tous, encore une fois. Chris Lewis-Evans ici, coprésident du PSWG.

L'utilisation malveillante du DNS est un sujet très important et dont nous discutons depuis un certain moment.

L'ordre du jour pour aujourd'hui est assez chargé. On a de très bons présentateurs et je ne vais donc pas prendre trop de temps pour présenter les sujets que nous allons aborder aujourd'hui.

Nous présenterons donc encore une fois l'importance de ce sujet pour nous.

Nous avons beaucoup discuté des tendances à propos de l'utilisation malveillante du DNS. Et puis nous allons céder la parole à notre collègue du Japon qui fera une présentation par rapport à l'utilisation malveillante du DNS chez lui.

Puis nous verrons les perspectives opérationnelles et les initiatives en cours. Et cela sera une bonne transition pour passer à la présentation sur le signalement centralisé de l'utilisation malveillante de Gabriel, et puis on verra les rôles de la communauté de l'ICANN au moment de lutter contre l'utilisation malveillante du DNS.

Sur ce, je vais céder la parole à Laureen.

LAUREEN KAPIN : Bonjour à tous, je suis Laureen Kapin, encore une fois, mais cette fois-ci je parle en tant que coprésidente du PSWG du GAC. Et je suis contente que les trois coprésidents, nous puissions être réunis autour d'une même table cette fois-ci. Donc c'est vraiment une raison pour en être heureuse.

Alors, je vais expliquer pourquoi cela est important pour nous. Si vous parlez de l'importance d'un sujet, d'abord, il faut commencer par présenter le sujet très souvent.

Ce sujet a différentes perspectives, mais il existe des définitions communes de ce qui constitue l'utilisation malveillante du système des noms de domaine. Le GAC les a recueillies dans une ressource formidable. Si vous ne l'avez pas, je vous encourage à la lire, parce que vous apprendrez plus à ce sujet.

Nous avons donc émis, au GAC, une déclaration consacrée à l'utilisation malveillante du DNS. Et il y a eu beaucoup d'échanges de la communauté à ce propos. Si vous ne l'avez pas lue, je vous encourage encore une fois à lire cette déclaration.

Entre autres, dans la définition, on inclut le concept des menaces à la sécurité qui sont apparues à partir de l'avis de sauvegarde de Beijing qui est devenu une partie du contrat de base pour les noms de domaine. Et on y comprenait l'hameçonnage, les logiciels malveillants et les réseaux zombie.

Il y a également une équipe consacrée à la révision de la confiance, la concurrence et le choix des consommateurs. Et au moment d'évaluer la confiance des consommateurs, le groupe a défini l'utilisation malveillante du DNS comme des activités qui sont intentionnellement décevantes ou non sollicitées, et qui utilisent activement le DNS et/ou les procédures utilisées pour enregistrer les noms de domaine.

La révision de cette équipe appelée CCT contient également une bonne définition de ce qu'est l'utilisation malveillante du DNS, et un historique du travail de la communauté à ce sujet.

Souvent on discute des contours de la définition. Or, je pense que le concept clé au moment de parler de l'écosystème de l'ICANN et que tout travail qui soit accompli doit être en conformité avec les statuts constitutifs de l'ICANN et ce qui est défini.

Le GAC a abordé la question dans sa déclaration au sujet de l'utilisation malveillante du DNS. Si vous téléchargez la présentation, vous pourrez accéder à la déclaration en cliquant sur les constructions qui apparaissent en bleu clair et qui sont soulignées.

Donc, le GAC définit l'utilisation malveillante comme une menace pour les utilisateurs Internet et les consommateurs individuels et commerciaux et leur confiance au DNS, mais également comme une menace pour la sécurité, la stabilité et la résilience de l'infrastructure du DNS. On devrait bien connaitre ces concepts étant donné qu'ils sont consacrés dans les statuts constitutifs de l'ICANN et sont une partie essentielle de sa mission.

Le groupe de travail consacré à la sécurité publique existe entre autres pour reconnaitre que les menaces au DNS sont des menaces à la sécurité publique. Le rôle consultatif est d'aider, et c'est ça le rôle du GAC en tant que comité consultatif. En 2015,

nous avons formellement établi le Groupe de travail consacré à la sécurité publique. Et je dis qu'il a été créé formellement, parce que les gens qui travaillaient à la protection des consommateurs et à la confiance des consommateurs s'étaient déjà penchés sur la question, mais un groupe de travail spécifique a été créé au sein du GAC pour se pencher en particulier sur ces sujets qui sont de grande importance pour nous.

Il n'y a pas que le groupe de travail consacré à la sécurité publique et le GAC qui s'intéressent à ces questions. Au sein de la communauté de parties prenantes de l'ICANN, il y a un bon nombre de groupes de travail qui accordent une priorité à la lutte contre l'utilisation malveillante du DNS. J'y inclus les parties prenantes du côté des opérateurs de registre et des bureaux d'enregistrement. Il y a beaucoup de personnes qui viennent participer en tant que parties contractantes, qui s'inquiètent énormément de leur réputation, de leurs clients, et qui accordent la priorité à ce travail, y compris les initiatives volontaires qui sont entreprises dans ce domaine.

Il y a énormément d'unanimité par rapport à cette notion qu'il s'agit d'un problème. On considère que l'on peut mieux faire. Et d'ailleurs ce matin même, au sein du PSWG, il y a eu des discussions. On a entendu parler certains des collègues de l'ICANN qui ont reconnu relativement que les contrats qui s'occupent de ces questions sont à la base de ce que nous

devrions attendre de la part des entités, au moins de répondre et d'aborder l'utilisation malveillante du DNS. Et que cette base pourrait bien sûr être plus élevée. On pourrait s'améliorer à ce niveau-là.

On se concentre beaucoup sur ces questions. On y consacre beaucoup d'attention. Et il y a beaucoup de travail à faire.

La question des contrats en particulier est d'importance. Les contrats prévoient les règles de l'écosystème de l'ICANN et définissent les rôles de tout un chacun pour savoir ce qui devrait se produire.

Le Conseil d'administration de l'ICANN et l'équipe de conformité contractuelle de l'ICANN ont reconnu que les contrats pourraient être améliorés. Ils sont insuffisamment clairs, à leur dire, et ils ne créent pas des obligations suffisantes qui puissent être appliquées pour lutter contre l'utilisation malveillante du DNS. Vous le verrez dans les discussions communautaires et dans les déclarations et dans les procès des réunions précédentes. Il y a beaucoup de correspondances avec le Conseil d'administration du 12 février 2020 qui reconnait en particulier les fossés des contrats actuels, les lacunes qui créent des incertitudes pour l'équipe de conformité contractuelle de l'ICANN. Et cela a été abordé au sein de différentes équipes de révision, à savoir au sein de l'équipe de révision de la confiance, le choix des

consommateurs et la concurrence du RDS WHOIS 2, du SSR2, mais également au sein du PDP de la GNSO consacré aux procédures pour des séries ultérieures de nouveaux gTLD.

Tant d'acronymes, n'est-ce pas ? Bref. Voilà une présentation du contexte par rapport à l'importance de ce sujet et des reconnaissances de la communauté par rapport au travail qui reste à faire. Divers groupes de travail et diverses équipes de révision reconnues qui il y a beaucoup qui peut être fait pour faire, du système de noms de domaine, un système plus sûr que ce qu'il est à l'heure actuelle. Et ce, en particulier, à propos de l'utilisation malveillante du DNS.

Je vais maintenant céder la parole à Gabriel.

GABRIEL ANDREWS : Bonjour à tous. Je m'appelle Gabriel et je vais reprendre cette idée de l'importance de l'utilisation malveillante du DNS pour le GAC.

Le PSWG l'a déjà présenté au GAC auparavant. Certaines des formes les plus nuisibles et prévalentes qui existent aujourd'hui d'utilisation malveillante du DNS sont les compromis des sociétés et le logiciel malveillant qui utilisent l'hameçonnage pour pouvoir capter des victimes.

Autrement dit, nos efforts accomplis ici pour lutter contre l'utilisation malveillante du DNS, que ce soit de l'hameçonnage ou de la rançon logicielle, aident à protéger tous nos citoyens contre les formes les plus prévalentes et puissantes d'utilisation malveillante du DNS qui existent aujourd'hui. Et certains des outils les plus utiles pour les fonctionnaires de la sécurité publique et les forces de l'ordre sont les données, c'est-à-dire que les enregistrements doivent être liés aux titulaires de nom de domaine. Et ces politiques existent parce que l'ICANN les a créées et les applique.

Passons à la diapo suivante.

Alors, passons à quelques mises à jour et un rapport des tendances par rapport à l'utilisation malveillante du DNS. Nous avons récemment discuté. Comme vous le saurez, l'organisation ICANN a publié et récemment informé le GAC d'un rapport qui a été élaboré, qui s'appelle les « Quatre dernières années en rétrospective », une mise en revue des tendances à propos de l'utilisation malveillante du DNS. C'est la raison pour laquelle l'ICANN a pris beaucoup de domaines et de comptes associés à ces domaines qui font partie des listes de blocage, c'est-à-dire que ce sont des noms de domaines qui ont été identifiés comme faisant des activités malveillantes. Et donc ici, ils se penchaient notamment sur le spam, sur l'hameçonnage, sur les rançons logicielles, sur la commande et contrôle des réseaux zombie,

c'est-à-dire des ordinateurs qui sont utilisés par des acteurs à des fins malveillantes.

Et l'ICANN a souhaité répondre à la question de savoir ce qui se passerait s'ils n'arrivaient pas à identifier tous ces acteurs. Ils ont senti à travers leur analyse qu'il y avait énormément d'acteurs qui étaient bien identifiés. Et donc ils ont publié ce rapport qui a suscité énormément d'intérêt de notre côté, parce qu'on sentait que le partage de fait est essentiel pour pouvoir générer les conversations dont on a besoin.

Nous avons vu que, dans les rapports, le constat immédiat était que le spam dépassait de loin les trois autres catégories toutes ensemble, toutes confondues.

Donc, comme vous le voyez, le spam apparait en rouge à l'écran. Il y a eu une tendance à la diminution du spam au cours des dernières années. Mais étant donné que le spam est tellement volumineux, il est différent pour nous de voir quelles sont les différentes catégories qui y sont comprises.

On a essayé de discriminer tout en bas, entre le jaune, le bleu et le rouge, les différents types d'activités malveillantes. Mais il est difficile de pouvoir extraire des tendances à partir de ces données. Et on n'a pas pu vraiment déterminer cela à partir des données que nous avons, mais heureusement et très généreusement les auteurs de ce rapport de l'ICANN ont proposé

de partager les données avec nous pour que l'on puisse évaluer ces tendances potentielles individuellement, chacune dans leur catégorie.

Et on a vu que l'hameçonnage suivait les mêmes tendances que le spam et la rançon logicielle. Et cela est important parce que c'est ce qu'utilisent les sociétés commerciales qui sont compromises, qui sont exposées à des pertes de 20 milliards de dollars en 2020. Encore une fois, la rançon logicielle utilise l'hameçonnage également pour attaquer des victimes.

Ce sont des questions très importantes auxquelles il faut apporter une réponse, et c'est pour cela que nous voulons avoir ces discussions.

Ensuite, dans ce rapport, l'ICANN indique qu'ils essayent de déterminer les causes des pics et des creux des différentes catégories de menaces. Cela apparaitra dans un rapport dans l'avenir. Nous espérons donc pouvoir étudier en profondeur les causes, donc, de ces variations. Merci beaucoup.

LAUREEN KAPIN : Je pense que notre collègue du Japon est le suivant intervenant. Nous allons vous donner la parole, et nous allons demander donc à ce que l'on affiche les diapos de notre collègue qui va faire la présentation.

TERUYUKI SHIBATA : Est-ce que je peux parler ?

MANAL ISMAIL, PRÉSIDENTE DU GAC : Allez-y.

TERUYUKI SHIBATA : Merci beaucoup. Bonjour à tous. Je m'appelle Teuyuki Shibata. Je suis représentant du Japon. Je travaille au Ministère des affaires intérieures et communication du Japon.

J'aimerais tout d'abord vous remercier de m'avoir donné cette opportunité de partager donc ces informations avec vous.

À l'ICANN 72, nous avons partagé des informations sur le *hopping* de noms de domaine. Aujourd'hui, j'aimerais vous présenter certaines tendances que nous avons pu constater dans le domaine de l'abus du DNS. J'aimerais donc partager ces informations par rapport au *hopping*.

Comme vous voyez à gauche du diagramme, plus de la moitié des domaines abusés sont liés à des abus liés à du *hopping* en février 2022.

Certains de ces domaines ont été fermés, mais on a vu apparaitre d'autres qui ont ouvert. Ensuite, comme vous le voyez dans le diagramme, dans la partie de droite, l'abus de noms de domaine

a tendance à se concentrer dans un certain nombre de bureaux d'enregistrement, en l'espèce dans trois bureaux d'enregistrement. Et donc nous avons pu constater que certains noms de domaine avaient été enregistrés à des fins d'abus.

Nous aimerions proposer certaines suggestions pour répondre à ce problème du point de vue des bureaux d'enregistrement. D'un côté, donc, mesurer le taux d'application des exigences de la part des titulaires de nom de domaine. Les données que les titulaires de nom doivent fournir, c'est leur nom, leur numéro de téléphone et leur e-mail. Et donc ces informations doivent être vérifiées par les bureaux d'enregistrement. Par exemple, dans le contrat entre les titulaires et les bureaux d'enregistrement, le bureau d'enregistrement doit vérifier les informations qui sont fournies par le titulaire.

En ce qui concerne les actions à long terme, les bureaux d'enregistrement doivent, à long terme, vérifier ces informations. Et ensuite, les bureaux d'enregistrement ont l'obligation de signaler tous les cas d'abus.

Ensuite, nous voudrions proposer que le service de la conformité contractuelle de l'ICANN continue à mettre en place des audits. Il est important de continuer à étudier les possibilités qu'a l'ICANN d'améliorer donc l'environnement concernant ce type d'abus. Et

c'est pour cela que nous sommes ravis de pouvoir parler de ces sujets à cette réunion de l'ICANN.

Diapo suivante, s'il vous plait. Merci beaucoup.

Et donc nous aimerions partager le concept de circulation de données transfrontalière et de ce que c'est que la confiance dans la libre circulation de données.

Le G20 s'est réuni à Osaka. Et donc la libre circulation de données génère une meilleure productivité. Et il faut donc continuer à faciliter cette circulation libre de données pour renforcer la confiance des commerces et des consommateurs.

Pour pouvoir construire cette confiance et faciliter la circulation des données, nous aimerions partager donc trois points qui devraient être considérés ; donc, la liberté d'expression, la libre circulation de données doivent être assurées pour pouvoir protéger un Internet global et sûr. Nous espérons que ce concept est bien compris.

Merci beaucoup de votre attention.

CHRIS LEWIS-EVANS : Merci beaucoup. Une présentation très intéressante. Très bien. Donc diapo suivante par rapport aux perspectives

opérationnelles et aux initiatives en cours au sein de la communauté.

La Commission européenne nous a donné la possibilité de nous réunir avec nos collègues des forces de l'ordre. Et Europol se trouve ici à côté. Nous avons pu avoir des discussions très intéressantes sur l'abus du DNS et les difficultés auxquelles les forces de l'ordre sont confrontées pour pouvoir répondre à ces cas d'utilisation malveillante du DNS.

Et un des éléments importants concerne non seulement ces entités criminelles qui sont à l'origine de ces cas d'abus, mais aussi le fait de pouvoir identifier et protéger les victimes du cyberdélit, de la fraude et de toutes ces activités malveillantes qui sont mises en place sur Internet et qui, en quelque sorte, rompent avec la confiance que l'on a sur Internet.

L'un des éléments qui a été évoqué pendant la réunion, c'est la réduction du nombre de domaines qui ne nous [donnent] pas une idée holistique de ce qui se passe au niveau de l'abus du DNS de manière globale. Et nous devons donc voir quelles sont les causes de cette utilisation malveillante, le nombre de victimes. Ce sont des informations que l'on peut obtenir à travers des méthodes de collecte d'informations ordinaires. Mais ces informations, elles ne sont pas accessibles pour les membres des forces de l'ordre. C'est pour cela qu'il faut voir comment nous pouvons travailler autour

des statistiques concernant l'abus du DNS, pour voir combien, ou pour analyser quelle est l'efficacité des mesures qui sont mises en place et voir si elles contribuent à la réduction de l'abus du DNS.

Si vous avez fait des statistiques intéressantes ou des signalements de la part de certaines agences de vos pays ou des statistiques, nous serons ravis de les recevoir de votre part. Nous aimerions bien collecter ce type d'information des différents pays.

Et maintenant, si nous passons aux initiatives actuelles et futures, une des initiatives de l'ICANN qui a été finalisée il n'y a pas longtemps - j'ai toujours du mal avec l'acronyme, mais c'est l'initiative de facilitation de la sécurité du système des noms de domaine ou le Groupe d'études techniques sur l'initiative de facilitation de la sécurité du système des noms de domaine, DSFI-TSG.

Et donc la recommandation 5 de ce rapport concerne une plateforme de partage d'information.

Nous-- les groupes qui se chargent de la sécurité publique sont assez habitués à partager des informations. Nous avons des activités de partage d'information et d'analyse de ces informations, car cela nous permet de partager des informations sur les différentes tendances, les manières dont on peut répondre à certains abus et le partage de stratégies.

Donc, il s'agit d'une recommandation qui nous permet d'avancer vers la création d'une telle plateforme à travers le travail entre, pardon, les parties contractantes de l'ICANN et les unités constitutives pour pouvoir donc répondre au cas d'abus. Nous voyons cette recommandation comme étant l'une des plus importantes de ce rapport rédigé par le Groupe d'études.

Graeme va nous parler également d'une autre initiative. Je ne vais pas donc empiéter sur sa présentation. Mais il y a également un cadre volontaire qui est en cours de mise en place. Tout cela aura un impact positif sur notre capacité à répondre en cas d'abus.

Or, il y a également des limitations, car toutes ces mesures ne s'appliquent pas forcément à toutes les parties contractantes. Nous voyons qu'il faut encore améliorer les dispositions contractuelles et le travail de politiques, afin que tout cela puisse s'appliquer à toutes les parties contractantes pour que l'on puisse répondre aux abus du DNS de manière efficace.

Maintenant, Graeme, je vais vous passer la parole.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Excusez-moi. Je vois qu'il y a une main levée de Kavouss dans le chat. Kavous. Et c'est ce qu'on peut poser des questions à ce stade ?

CHRIS LEWIS-EVANS : Oui, s'il vous plait.

IRAN : Est-ce que j'aurais la parole ?

MANAL ISMAIL, PRÉSIDENTE DU GAC : Allez-y.

IRAN : Tout d'abord, j'aimerais remercier l'ICANN pour ce rapport sur cette question très importante. Nous apprécions tous les efforts qui sont consentis pour aboutir à ces recommandations.

Madame la Présidente, je vous demande de bien vouloir prendre en considération ce rapport pour les actions à mettre en place, notamment en ce qui concerne des avis futurs ou des suivis concernant les avis que nous avons donnés en matière d'abus du DNS. Je pense que cela pourra répondre à certaines de nos inquiétudes, car nous avons une certaine réponse ; peut-être qu'elle ne répond pas à toutes nos inquiétudes, mais je pense que, dans une large mesure, c'est une initiative qui est satisfaisante.

Donc je pense que l'on pourrait prendre en considération ce rapport dans notre communiqué ou bien dans la partie concernant le suivi d'autres avis du GAC. Merci beaucoup.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Merci beaucoup, Kavouss. C'est bien noté. Et je tiens à attirer l'attention de tout le monde sur le chat. N'oubliez pas de regarder le chat. Je vois que l'Indonésie veut prendre la parole. Allez-y.

INDONÉSIE : Pardon-- merci, Manal.

La sécurité et l'utilisation malveillante du DNS et autre sont très importants aujourd'hui. Pas comme il y a quelques années, mais peut-être plus, parce qu'on dépend plus de l'Internet grâce aux problèmes de confinement qu'on a dû traverser.

Donc, pour moi, la question serait de savoir s'il serait possible pour l'équipe de l'ICANN responsable de la sécurité ou pour le groupe qui s'occupe de l'utilisation malveillante du DNS de coopérer davantage avec l'Union internationale des télécommunications. Comme vous savez, ils ont également l'agenda de cybersécurité globale, GCA, qui a été publié il y a quelques années.

IRAN : Pardon, Manal, mais vous discutez de quelle question ?

INDONÉSIE : Ce n'est peut-être pas exactement lié à la question.

IRAN : Donc lorsqu'on passera au 5.2, on reviendra à vous. Mais moi j'ai une suggestion sur ce point-là.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Pardon, Kavouss. On a cédé la parole à l'Indonésie pour faire sa présentation, son intervention.

IRAN : Oui. Pardon. Est-ce que vous m'entendez maintenant ?

MANAL ISMAIL, PRÉSIDENTE DU GAC : Oui, mais si possible, Kavouss — Kavouss ?

IRAN : On ne devrait pas transformer le comité en un groupe de rédaction. Merci.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Merci, Kavouss. Pardon, Ashwin, allez-y.

INDONÉSIE : Oui, je voulais dire que peut-être une meilleure coopération pourrait générer de mes résultats, parce que l'UIT a publié son document GCA sur la cybersécurité il y a beaucoup d'années. Et c'était également discuté à Dubaï en 2012.

Donc on a vu comment améliorer la gouvernance de l'Internet et comment faire en sorte que la gouvernance d'Internet permette d'améliorer la cybersécurité. Donc, peut-être qu'à la lumière d'une cybersécurité un peu plus conservative, on pourrait également discuter à nouveau ce type d'opération. Merci.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Merci beaucoup, Ashwin. Je vois que les États-Unis lèvent la main également. Susan, allez-y.

ÉTATS-UNIS : Merci, Manal. Je félicite les coprésidents du Groupe de travail consacré à la sécurité publique pour la présentation qu'ils viennent de nous faire qui était très exhaustive et très claire.

Nous croyons que la solution pour lutter contre l'utilisation malveillante du DNS peut se reposer sur différentes exigences contractuelles. Chris l'a clairement dit. Les initiatives volontaires diffèrent des exigences contractuelles et des programmes de conformité qui s'appliquent aux bureaux d'enregistrement.

Nous croyons également que les solutions pourraient inclure des incitations pour pouvoir atteindre des mesures de lutte contre l'utilisation malveillante du DNS et pour mettre en œuvre d'autres mesures.

Du point de vue de l'USG, et donc du gouvernement américain et des mesures de lutte contre l'utilisation malveillante, il nous a semblé qu'on essayait de mettre en lien l'utilisation malveillante du DNS avec tout ce qui pourrait être nuisible sur Internet. On a essayé de tracer un rapport entre les deux. C'est ce que j'ai compris à travers la transcription. Mais l'activité nuisible et illégale sur la couche de l'Internet en dehors du DNS n'est pas dans la portée de la mission de l'ICANN, même si on devrait s'en occuper de manière urgente, que ce soit à travers des processus juridiques ou à travers d'autres solutions intercommunautaires volontaires et collaboratives, telles que les notifications et les initiatives de meilleures pratiques. Merci.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Merci beaucoup, les États-Unis. Je vois que nous avons une autre main de levée. Allez-y.

PAYS-BAS : Merci. Merci, Présidente, et merci collègues. Je représente les Pays-Bas et je voudrais reprendre ce qu'a dit le collègue de l'Indonésie par rapport au document GCA.

On pourrait très bien examiner et considérer la coopération avec d'autres organisations, mais je pense qu'il faudrait que l'on trouve une solution ici même, en interne, dans le cadre du modèle multipartite. On ne devrait pas trop regarder à l'extérieur. Surtout je ne vois pas l'intérêt à revenir sur les discussions qui ont été tenues en 2012, qui datent d'une décennie déjà. Je pense que le monde a beaucoup évolué depuis. Merci.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Merci. En l'absence d'autre demande de prise de parole, Graeme, je vous recède la parole. Désolée de vous avoir interrompu. À vous.

GRAEME BUNTON : Merci, Manal, et merci à tous de m'avoir invité. Cela me plait énormément de pouvoir venir vous parler du lancement de NetBeacon.

J'ai des diapos à présenter, mais je pense que la conclusion claire est que, avec le soutien de PIR et Clean DNS, l'Institut contre l'utilisation malveillante du DNS a lancé un service de signalement de l'utilisation malveillante pour simplifier le processus de signalement de l'utilisation malveillante du DNS et pour faire en sorte qu'il soit plus simple pour les opérateurs de registre et les bureaux d'enregistrement de prendre des mesures là-dessus.

Alors, l'Institut DNSAI a été créé l'année dernière par le registre d'intérêt public (PIR) qui opérait le TLD. ORG.

PIR a une mission à but non lucratif et s'est rendu compte que l'utilisation malveillante du DNS est un problème mondial compliqué et que son atténuation, au niveau des bureaux d'enregistrement et des opérateurs de registre individuels, n'augmente pas, qu'on a besoin de résoudre ce problème et de lutter contre l'utilisation malveillante du DNS. Voilà pourquoi l'Institut consacré à la lutte contre l'utilisation malveillante du DNS a été créé : pour le faire d'une manière qui puisse être coordonnée entre tous les acteurs du DNS.

Diapo suivante.

NetBeacon, le service de signalement centralisé, est une réponse à différentes initiatives communautaires. La recommandation 13.1 du groupe SSR2 demande que l'on crée un

portail centralisé pour les plaintes d'utilisation malveillante. Le document SSAC15 du SSAC demande que l'on crée un facilitateur de signalement de l'utilisation malveillante qui soit centralisé également, et la révision CCRT, dans la recommandation 20 du rapport final, se concentre également sur un système pareil.

Diapo suivante.

Il y a des problèmes fondamentaux qui sont liés au signalement de l'utilisation malveillante à présent, ou au moins il y avait des problèmes.

D'une part, on sait qu'il est difficile de signaler les cas d'utilisation malveillante pour la communauté de cybersécurité et pour tous ceux qui l'ont fait auparavant. Il est difficile de mettre en œuvre des normes qui soient les mêmes partout dans l'écosystème. Et il faut des connaissances techniques. Vous devez pouvoir identifier un bureau d'enregistrement, trouver leur page consacrée au signalement d'utilisation malveillante, et il n'existe pas de normes cohérentes pour la présentation de preuves, pour la mise en œuvre de ces fonctions de signalement. Donc, c'est vraiment très difficile de le faire.

D'autre part, et on ne l'apprécie pas souvent, mais il y a le fait que les bureaux d'enregistrement et les opérateurs de registre reçoivent des rapports qui sont horribles. Ils n'ont aucune structure. Ils n'incluent pas des preuves. Souvent, ce sont des

plaintes pour un DNS qui n'appartient pas à ce fournisseur. Et ils ne peuvent rien faire là-dessus. Donc ils passent beaucoup de temps à séparer des tickets qui ont peu de valeur, et sans pouvoir vraiment améliorer la sécurité de l'Internet.

On a senti qu'il existait une solution qui pouvait résoudre les deux problèmes en même temps. Et il s'agit de NetBeacon.

Diapo suivante.

NetBeacon est un outil gratuit, tant pour les personnes qui veulent présenter des plaintes comme pour les opérateurs de registre et les bureaux d'enregistrement qui souhaitent interagir vite. Il est utilisé pour signaler l'utilisation malveillante, améliorer la qualité des rapports, réduire les barrières d'action. On centralise les signalements et les plaintes à travers un outil qui accepte des rapports d'hameçonnage, de rançon logicielle, de réseaux zombie, de spam, qui normalise les exigences et les formats, qui prend les renseignements par rapport au domaine et qui enrichit les rapports. Est-ce qu'on peut trouver d'autres informations à propos de ce domaine ? Est-ce qu'on peut voir d'autres activités malveillantes ou illégales qui étaient entreprises par ce domaine ? Et puis cela est attaché au rapport d'utilisation malveillante.

Et c'est là qu'on trouve l'incitation pour que les opérateurs de registre et les bureaux d'enregistrement utilisent cet outil. À

présent, ils reçoivent plus d'informations grâce à cet outil et, en une certaine mesure, une partie de cette charge de l'enquête est passée au service et ne dépend plus des bureaux d'enregistrement et des opérateurs de registre. Et pour eux, il est donc plus simple de recevoir un rapport d'utilisation malveillante normalisé, solide et bien informé, qui leur permette de décider de ce qui est nuisible ou pas et de décider de comment y répondre.

Par ailleurs, ces rapports sont distribués automatiquement. C'est-à-dire que la personne qui envoie la plainte n'a plus à décider où l'envoyer, mais c'est nous qui les distribuons.

Diapo suivante.

Il est important de comprendre l'échelle du problème auquel nous nous attaquons ici. Il y a une certaine quantité d'utilisation malveillante du DNS sur Internet, dont une partie est effectuée à travers les listes et les *feeds*. Donc on a les listes de blocage et c'est là qu'on mesure l'utilisation malveillante du DNS en général, mais il y a également des cas d'utilisation malveillante qui sont informés manuellement. Et c'est ça qui demande beaucoup de cycles de travail et beaucoup d'heures de travail pour les opérateurs de registre et les bureaux d'enregistrement. C'est là qu'ils doivent faire la part des différents rapports reçus pour voir quels sont ceux qui doivent être abordés.

Voici un exemple d'un rapport pour hameçonnage.

Vous pouvez accéder à NetBeacon.org et créer un rapport pour une utilisation malveillante dans le cas de l'hameçonnage. Il est facile de compléter les informations. On a essayé d'apporter des outils qui expliquent l'importance des informations et le type d'information qui devrait être envoyé à chaque pas. Il est facile pour les utilisateurs de l'utiliser. Très convivial.

Et je sais qu'il y a un peu de friction, ici. Il y a des personnes qui n'aiment pas les formulaires. Mais malheureusement, lorsqu'on leur donne des champs de texte libre, on ne peut pas l'utiliser sur Internet. Les bureaux d'enregistrement et les opérateurs de registre ont besoin d'avoir des informations plus structurées pour pouvoir prendre des mesures.

Par ailleurs, il vous faut une adresse e-mail d'une compagnie, d'une société, de votre travail. Parce qu'on est un intermédiaire. Nous, on reçoit les rapports. On les normalise. On les améliore. Mais on les envoie là où ils doivent aller. Et les opérateurs de registre et les bureaux d'enregistrement doivent pouvoir contacter la personne ayant envoyé le rapport s'ils ont besoin de plus d'informations. Donc voilà pourquoi on ne prend en charge que ce type d'adresse e-mail dans notre service.

Alors, quelques autres fonctionnalités. Il existe une API pour la présentation de rapport, pour que les acteurs de cybersécurité, les forces de l'ordre, les personnes qui pourraient signaler

l'utilisation malveillante à l'échelle puissent le faire. On ne l'a pas activé. Il faut toujours définir quels seront les règles et le flux pour pouvoir le faire. Mais il va falloir que l'on puisse garantir que la qualité des rapports soit très élevée, pour que les bureaux d'enregistrement trouvent une valeur à cet outil. Mais nous allons habiliter cela dans un avenir proche.

Il y a également une API pour la consommation des rapports, pour que les opérateurs de registre et les bureaux d'enregistrement puissent les utiliser et les intégrer à leur système de traitement d'utilisation malveillante, et non pas simplement les recevoir par e-mail. Les formulaires peuvent être intégrés sur le site Web de tout un chacun pour que l'on ait des formulaires normalisés, enrichis, et sans que chacun doive faire le travail de son côté. Ces formulaires seront donc envoyés à NetBeacon automatiquement s'ils sont intégrés aux autres sites.

Ici, j'ai ajouté des informations importantes.

NetBeacon n'est pas un outil de gestion de l'utilisation malveillante. Les opérateurs de registre et les bureaux d'enregistrement vont recevoir ces rapports dans le système qui leur convient le mieux. Ça peut être une solution par e-mail ou autre. Et ce n'est pas un endroit où ils vont accéder pour gérer l'utilisation malveillante. Ils vont devoir s'en occuper ailleurs.

On ne prend pas de décision, non plus. Cela appartient à l'opérateur de registre et au bureau d'enregistrement de déterminer s'il s'agit d'un cas d'utilisation malveillante ou pas, et de comment y répondre.

En même temps, on n'a pas un annuaire des cas d'utilisation malveillante. Les bureaux d'enregistrement et les opérateurs de registre ne voudraient pas se sentir menacés si on gardait les données au long terme. Donc on ne va pas les conserver sur le long terme.

Et en même temps, on ne fournit pas accès aux informations des titulaires de nom de domaine ni des consommateurs. Ici, on se penche vraiment sur l'utilisation malveillante du DNS. Ce n'est pas question de pouvoir garantir l'accès aux informations et octroyer l'accès à qui que ce soit.

Diapo suivante.

On a un programme ambitieux pour ce service. On voudrait vraiment pouvoir en faire un outil central et robuste, qui soit un bien public pour faire en sorte que l'Internet soit plus sûr. Et cela inclut l'intégration des ccTLD, de l'hébergement, des réseaux de distribution de contenu, les fournisseurs de services de courrier électronique, pour pouvoir traiter des rapports ou recevoir des rapports qui signalent l'abus d'autre cas de dommages également et pour que l'abus puisse être distribué aux

entreprises d'hébergement et puis être envoyé au bureau d'enregistrement approprié.

Le meilleur exemple en serait celui des sites Web compromis où quelqu'un a été attaqué sans le savoir et où il serait inapproprié de traiter le problème d'abord avec le bureau d'enregistrement. Tout d'abord, on l'enverrait au responsable de l'hébergement et la chaine devrait suivre.

Et on vise également à améliorer la réputation, pour que ceux qui signalent un cas d'utilisation malveillante du DNS et qui veulent améliorer leur réputation du fait d'avoir signalé cette utilisation malveillante puissent avoir un tiers, comme NetBeacon, qui garantisse qu'ils font un bon travail à ce niveau-là.

Et en même temps, les opérateurs de registre et les bureaux d'enregistrement veulent être surs que ceux qui signalent l'utilisation malveillante le font de bonne foi et de manière qui a une grande qualité et qui est robuste.

Diapo suivante. Questions fréquentes.

Est-ce que c'est facile à utiliser pour les utilisateurs finaux ? Oui, c'est assez facile. Nous devrons peut-être travailler un petit peu plus, mais de manière générale, je pense que tout le monde peut l'utiliser pour le moment.

Ensuite, il est uniquement en anglais. Mais à terme, nous allons le traduire dans plusieurs langues pour qu'il puisse être utilisé partout dans le monde.

On me pose la question de savoir si l'on va publier des données ou sous la forme de rapports. Et la question courte, c'est que nous allons probablement produire des statistiques agrégées, mais je pense que l'utilisation de cet outil ne vise pas forcément à signaler du doigt des bureaux d'enregistrement. L'idée, c'était un petit peu de mesurer l'utilisation malveillante et l'utiliser aussi pour des cas d'études.

Ensuite, pour les notifications, nous pouvons clôturer des tickets des bureaux d'enregistrement avec une certaine possibilité d'affiner ce travail.

Ensuite, les bureaux d'enregistrement doivent se connecter ? Non. Nous envoyons donc par défaut aux bureaux d'enregistrement et aux opérateurs de registre. Les bureaux ou les opérateurs peuvent créer un compte et utiliser ce service, mais ils ne sont pas obligés de le faire.

Et ensuite, pourquoi nous faisons ceci. Il est important de répondre à cette question. Quand nous voyons les signalements d'abus sur Internet, nous voyons une espèce de tendance pour voir que, pour pouvoir agir de manière efficace, il faut travailler en coopération avec d'autres bureaux d'enregistrement, d'autres

opérateurs de registre. Et très vite, on sort de la mission de l'ICANN. Et c'est pour cela que nous voulions-- nous sommes bien positionnés pour essayer d'agir en tant qu'intermédiaire dans toute cette communauté.

Ensuite les bureaux d'enregistrement, les opérateurs de registre, les hébergeurs ont plusieurs moyens de signaler des abus. Si c'était une initiative de l'ICANN, on finirait par créer une certaine confusion pour les gens qui essayent d'utiliser les réseaux et soutenir de ce travail.

Donc, on a vu certaines définitions de ce projet. Nous avons travaillé avec le projet de juridiction Internet. Merci à eux. Ensuite PIR, l'Institut de l'abus du DNS et Clean DNS qui a été un partenaire très généreux. Ils ont donné la technologie, ils ont apporté la technologie ainsi que la customisation du processus.

Diapo suivante, s'il vous plait.

Ce sont des sites Web que vous pourrez visiter. Vous pouvez créer un compte, si vous voulez signaler un abus. Si vous voulez me contacter directement pour plus d'informations, n'hésitez pas à le faire. Et je suis toujours intéressé à contacter les organisations qui souhaitent travailler dans la lutte contre l'abus du DNS.

C'est tout de ma part. J'espère qu'il y aura des questions et je serais ravi d'y répondre.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Je vois qu'il y a une main levée dans la salle Zoom. Alors, allez-y. Excusez-moi si je n'ai pas bien prononcé votre nom. Et après, il y a Nigel Hickson.

INTERVENANT NON IDENTIFIÉ : Bonjour. Est-ce que ce serait possible pour les titulaires de nom de domaine de recevoir de rapports de NetBeacon. Par exemple, nous avons des domaines très bien qualifiés et nous serions intéressés à voir s'il y a des signalements par rapport à ces domaines qui sont enregistrés. Est-ce que ce serait possible pour nous d'avoir un flux d'informations pour voir ce qui est signalé par rapport à certains domaines ?

GRAEME BUNTON : Merci pour cette question très intéressante. On n'y a pas forcément pensé.

La similarité est un problème, bien sûr, et je vais donc l'ajouter à ma liste de fonctionnalités. Et nous allons nous y pencher. Merci.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Nigel, s'il vous plait.

Royaume-Uni : Merci beaucoup, Graeme, pour cette présentation, et merci à tout le panel, bien sûr, qui ont fait des présentations excellentes. Et je vous félicite pour ce travail que vous faites à l'Institut du DNS.

IRAN : Excusez-moi, Madame la Présidente. J'ai une proposition.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Kavouss, s'il vous plait. Nous avons une intervention. Vous êtes en train d'interrompre une intervention. S'il vous plait, pouvez-vous attendre que Nigel finisse son intervention ? Je vais vous donner la parole après. Excusez-moi, Nigel.

ROYAUME-UNI : Pas de problème. J'ai un peu perdu le fil, mais je voulais vous remercier pour ce que vous faites à NetBeacon. Ça a l'air extrêmement positif. C'est très important d'avoir ces informations. C'est très positif.

J'ai une question et je sais que vous y avez répondu en partie.

Vous travaillez beaucoup pour analyser les données signalées et revenir vers le bureau d'enregistrement pour leur donner des informations. Et bien sûr, en fin de compte, il faut savoir ce qu'ils

feront avec ces informations. Mais notre question en tant que gouvernement, nous serons intrigués à savoir quel est le résultat positif qui a lieu, c'est-à-dire savoir si ces informations permettent qu'un domaine soit fermé ou pas. Merci beaucoup.

GRAEME BUNTON : Merci, Nigel. J'apprécie vos propos. Nous essayons de voir quelles sont les mesures que nous pour mettre en place pour voir les résultats de ces signalements, c'est difficile de le faire.

Et il se pourrait que le signalement ne soit pas correct et que la fermeture de domaine ne soit pas la mesure à mettre en place. Nous essayons de faire en sorte que le service fonctionne pour rendre l'Internet plus sûr et tout cela bien sûr figure dans notre liste.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Merci beaucoup. J'ai Kavouss, Rwanda, et après nous allons devoir clore cette séance. Kavouss, s'il vous plait.

Et pour m'aider à faire un meilleur travail, je vous demande Kavouss de bien vouloir lever votre main sur Zoom quand vous voulez prendre la parole. Allez-y, Kavouss.

Kavouss, est-ce que vous m'entendez ? Rwanda, s'il vous plait.

RWANDA : Merci beaucoup. Merci à l'Institut DNS Abuse. Nous apprécions ce travail qui est fait. J'aimerais demander quelques précisions.

Si vous avez des efforts de renforcement des capacités pour aider les pays en développement en matière d'abus du DNS. Comme vous le savez, il y a le DNSSEC qui se met en place. Mais ma question vise à une coopération avec ces pays en développement pour qu'ils puissent former leurs ingénieurs afin qu'ils puissent mieux lutter contre les abus du DNS. Par exemple, à travers le DNSSEC.

Et finalement, je voulais savoir quelle est la fréquence à laquelle vous allez publier vos rapports. Il s'agit de rapports annuels ou bien ? Donc à quelle fréquence publiez-vous ces rapports, où allez-vous publier ces rapports ?

GRAEME BUNTON : Merci pour ces questions. Pour ce qui est du renforcement des capacités, l'Institut du DNS mène des activités de formation. Nous publions des informations pour les titulaires, pour les bureaux d'enregistrement, des conseils pour qu'ils puissent préserver la sécurité du DNS. Et bien sûr, nous allons continuer à mettre en place ce type de mesure. Et je peux bien sûr

m'entretenir avec vous par rapport à la possibilité qu'il y a de coopération.

Et pour ce qui est du rapport, je ne suis pas très sûr encore de quel type de rapports nous allons publier. Mais si nous le faisons, nous le ferons aux alentours du mois de septembre. Aout-septembre.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Merci beaucoup. Je vois qu'il y a une main des États-Unis. Est-ce qu'on a encore des diapos ? D'accord, les États-Unis, très brièvement si vous souhaitez poser une question.

ÉTATS-UNIS : Merci beaucoup, Madame la Présidente. Merci Graeme, de cette présentation. Les États-Unis reconnaissent l'introduction des initiatives [DIC], l'initiative que vous venez de nous présenter. Nous prenons bien note de cette initiative et nous espérons qu'il y aura d'autres développements par rapport à l'utilisation de ce nouvel outil pour l'ICANN 75, et de manière plus générale, pour ce qui est des rapports en matière d'abus du DNS.

Nous espérons pouvoir accéder à des activités de rapports plus granulaires, plus détaillés, afin de savoir quels sont les types d'abus du DNS, que l'on puisse les mesurer, et que l'on puisse

également pouvoir accéder à des données agrégées que l'on puisse mettre en coordination avec les contrats.

GRAEME BUNTON : Merci beaucoup pour ces propos. Je dois dire que le service fonctionne déjà et qu'il y a un premier flux d'information qui est déjà en place et ces informations sont très très utiles.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Merci beaucoup. Cathrin, merci de votre patience. Allez-y.

COMMISSION EUROPÉENNE : Merci beaucoup. Nous passons à quelque chose de très facile à utiliser. C'est très bien. Je m'appelle Cathrin Bauer-Bulst, et j'appartiens à la Commission européenne. Je suis vraiment ravie de voir autant de personnes que je connais en présence. Alors bonjour, chers collègues du GAC.

Nous allons donc revenir au rôle de l'ICANN. Quel est le rôle de l'ICANN dans tout ceci et quel devrait être ce rôle ?

Nous avons fait des progrès pour être plus transparents à l'ICANN et en dehors. L'ICANN a contribué avec le DARR et l'initiative DNS sticker. Nous avons également un système automatique pour

aider l'écosystème à être plus efficace pour répondre à des cas d'abus.

Pour répondre à la première remarque de Laureen en ce qui concerne les contrats. L'ICANN doit intervenir lorsque les titulaires ne respectent pas les contrats, pour contribuer à une infrastructure Internet qui soit sure. Et donc ce statuquo n'est pas reflété dans la mission de l'ICANN.

Nous avons entendu des commentaires par rapport à cela dans la communauté. Nous savons que nous devons faire davantage et nous saluons le soutien de ces initiatives qui sont en cours au sein de l'ICANN et en dehors. Nous devons construire d'un côté plus de transparence, partage d'information, et nous devons renforcer tout cela et mieux comprendre les facteurs qui sont à l'origine de l'abus du DNS. Nous devons soutenir les bureaux d'enregistrement et les opérateurs de registre dans leurs mesures qui sont mises en place et comprendre les données du point de vue également des autorités de sécurité publique ainsi que pour comprendre l'impact que cela a sur les utilisateurs du DNS. Et cela est en ligne avec le rôle de l'ICANN en tant qu'organisme qui doit remplir la mission qui est mandatée dans ses statuts constitutifs.

Pour cela, il faut des encouragements. Parce que finalement, prendre une mesure contre les abus DNS a un cout. Et même si

l'on réagit à un signalement-- il faut au lieu de réagir à des signalements, il faut agir de manière proactive. Il ne s'agit pas en général des parties contractantes. Quand on parle de soutien de l'industrie, beaucoup de ces parties contractantes sont engagées et veulent faire plus. Et en général, ce sont ceux qui ne participent pas ici. Et l'exemple évoqué par le Japon est très clair. Ce sont eux qui peuvent avoir un problème.

Donc il peut s'agir d'une question d'un problème de renforcement de capacités. Mais il faut également créer des encouragements. Et ici, on revient à une des interventions qui a été faite, et Laureen va nous parler également des étapes futures pour pouvoir encourager le soutien de l'industrie.

LAUREEN KAPIN : Dernière diapo.

Et donc les contrats sont la base de la conformité contractuelle de l'ICANN et tout le monde sera d'accord pour dire que les contrats doivent être appliqués. Donc, la question est de savoir qu'est-ce qu'il y a dans les contrats. Et est-ce qu'on peut améliorer ce qu'il y a dans les contrats. Parce que le pouvoir du service de conformité contractuelle de l'ICANN vient des contrats.

Et donc, on voit qu'il y a une disposition concernant les engagements d'intérêt public. Et il y a une disposition qui

concerne l'interdiction de distribuer des logiciels malveillants, etc. Et cela est tiré exactement des contrats de registre.

Et en voyant cela, on croit que cela veut dire, bon, tous ces comportements sont interdits. Alors, si cela a lieu, alors on peut faire valoir les dispositions du contrat. Mais non, ce n'est pas comme ça. Il s'agit de ce que l'on appelle une exigence *downstream*. C'est-à-dire que cela oblige les registres à dire aux bureaux d'enregistrement, car c'est les bureaux qui traitent avec les titulaires de nom, on leur dit, il faut vous assurer que les titulaires de nom sachent cela.

Et donc, l'ICANN et les opérateurs de registre ont une promesse entre eux par rapport à ces exigences qui doivent figurer dans les contrats avec les bureaux d'enregistrement. Mais il n'y a pas d'obligation pour les opérateurs de registre de s'assurer que les bureaux d'enregistrement incluent cela dans leurs exigences.

Et donc, ce sont des problèmes qui devraient être analysés dans le cadre plus large du travail qui est fait pour nous assurer qu'il y a des dispositions appropriées pour lutter contre l'abus du DNS. Car ce n'est pas au GAC tout seul, ou ce n'est pas à une partie prenante en solitude, d'identifier et de répondre à ces questions. C'est en coopération que nous devons pouvoir lutter contre les abus du DNS. Et dans ce sens, il faut améliorer les contrats. Et pour cela, il faut une conversation entre toutes les parties

prenantes, et notamment celles qui se trouvent du côté commercial, parce que nous, nous savons des choses qu'ils ne savent pas ; eux, ils savent des choses que nous ne savons pas. Et donc, il s'agit d'un dialogue qui doit être constructif pour que nous puissions travailler ensemble.

Un autre exemple où il peut y avoir des écarts dans les contrats, ce sont les analyses techniques pour voir s'il y a des menaces à la sécurité. Mais les contrats ne disent pas ce qui va se passer après, une fois que ces menaces sont identifiées. Et donc encore plus de questions.

Et puis le contrat de registre de bureaux d'enregistrement demande au bureau de répondre de manière appropriée aux abus du DNS. Mais avant, il faut reconnaitre que le contrat de bureau d'enregistrement n'a aucune spécificité par rapport à ce que cela représente. Qu'est-ce que c'est que des mesures raisonnables pour répondre à des abus du DNS ?

Et donc il y a eu des discussions. Il y a eu des initiatives volontaires. Il y a eu beaucoup de bonnes intentions. Mais nous devons avoir ces discussions sur la question plus large du signalement et de la gestion et de la réponse à des abus du nom de domaine et comment les dispositions des contrats peuvent être appliquées et améliorées de manière proactive.

Merci, mais nous avons dépassé un peu l'heure de conclusion de cette séance. Je m'excuse parce qu'on n'a plus beaucoup de temps pour répondre à des questions.

MANAL ISMAIL, PRÉSIDENTE DU GAC : Merci beaucoup à tous ceux qui sont ici et à ceux qui sont à distances et qui ont fait leur présentation. Merci aux collègues du GAC pour la participation active et pour leur intérêt. Collègues du GAC, soyez de retour, s'il vous plait, à la demie.

[FIN DE LA TRANSCRIPTION]