FR

ICANN85 Mumbai | Forum de la communauté – Séance plénière d'At-Large : progression du programme de réduction de l'utilisation malveillante du DNS
Mardi 10 mars 2026 – 10h30 à 12h00 IST

MICHELLE DESMYTER

Bonjour et bienvenue à cette séance de plénière de l'At-Large « Progression de l'atténuation de l'abus du DNS ». Je m'appelle Michelle DeSmyter. Je suis la responsable de la participation à distance.

Veuillez noter que cette séance est enregistrée et qu'elle suit les normes de comportement attendues de l'ICANN et aussi les politiques antiharcèlement de l'ICANN. Les questions et les commentaires ne seront lus à voix haute que s'ils sont soumis dans la fenêtre questions-réponses. Il y a de l'interprétation aujourd'hui. Cela comprend de l'anglais, du français et de l'espagnol. Si vous souhaitez parler, veuillez lever la main sur Zoom. Les participants à distance auront le droit d'activer leur micro lorsqu'ils seront appelés. Les participants sur place utiliseront un micro physique pour parler. Donnez votre nom pour la transcription, et la langue que vous allez utiliser si vous ne parlez pas l'anglais. Et veuillez, s'il vous plait, parler à un rythme raisonnable.

Avec cela, je vais repasser la parole à Justine Chew.

JUSTINE CHEW

Merci Michelle et bienvenue à tous, toutes les personnes qui sont là et toutes les personnes qui sont en ligne. J'espère que nous allons avoir le plus de participants possible, parce qu'à la fin de la séance, nous allons faire participer l'audience.

Je m'appelle Justine Chew, je vais donc modérer la séance d'aujourd'hui de la part de l'ALAC. J'aimerais remercier les panélistes qui sont avec nous ici dans la salle et aussi en virtuel. Je voudrais noter que nous avons reçu des excuses de certains des panélistes qui avaient été invités. C'est pour cela -- vous allez vous en rendre compte lorsque nous allons vous montrer notre présentation.

Donc, du côté du groupe des représentants des opérateurs de registre, du groupe des représentants des bureaux d'enregistrement, les représentants du GAC, ce n'est pas très grave. Nous allons continuer la conversation de toute façon. Avec cela, peut-être que nous pourrions passer à l'ordre du jour, s'il vous plait.

Très bien. Donc, nous avons peu de temps, mais nous allons essayer de parler -- de discuter de trois thématiques. Comme vous le voyez, la première partie de l'ordre du jour, nous allons essayer d'obtenir les réflexions de nos panélistes. Certains d'entre eux sont des participants du PDP numéro 1.

Sandra, pouvez-vous mettre votre micro en sourdine, s'il vous plait ? Merci.

Donc, sur la vérification des domaines associés. Nous avons eu quatre sessions sur ce PDP. En attendant, j'aimerais inviter certains des panélistes afin qu'ils puissent nous dire s'ils ont trouvé des problèmes, si les choses se passent bien, etc. Ensuite, nous allons passer un peu de temps sur la deuxième thématique. Il s'agit des algorithmes de génération de domaine les DGA. Et pour cela, nous avons quelqu'un du groupe de travail de la sécurité publique du GAC, qui viendra nous faire une présentation et nous parler du cadre existant sur ce travail. Nous allons en discuter par la suite pour voir comment nous allons pouvoir avancer. Nous recevrons des commentaires de John et de Mukesh, qui est là aussi, Mukesh. Mukesh remplace Teresa parce que Teresa n'est pas là aujourd'hui. Et ensuite, nous allons parler des lacunes dans la lutte contre les abus du DNS.

Nous savons que la communauté nous a apporté quelques renseignements à ajouter au processus de la GNSO pour identifier les priorités dans cela, dans ce que l'on peut faire pour atténuer ces lacunes. Nous allons utiliser dans ce sens le PDP 1. Ensuite, il y aura un PDP 2, qui va arriver bientôt. Et pour ce qui est de l'âge -- des algorithmes de génération de domaine, il y aura -- enfin, on pense que cela devrait être géré peut-être par un PDP, ou, peut-être, un peu un processus de PDP externe de la communauté. Donc, on va essayer de rassembler des -- on va en parler avec les participants et les membres de la communauté, [à] savoir si cela devrait passer par un PDP ou non.

Alors, lorsqu'il s'agit de la participation de l'audience, eh bien, nous avons mis en œuvre un sondage, un questionnaire pour un peu prendre le pouls de la salle et savoir si ce PDP -- à savoir quelle est la quatrième priorité sur laquelle on devrait travailler. Donc voilà, on va commencer. Pourrions-nous passer à la prochaine diapositive, s'il vous plait ? Prochaine diapositive. La prochaine.

Alors nous allons parler de -- nous allons passer à la première partie de l'ordre du jour aujourd'hui. Alors, on voudrait savoir quelles sont vos réflexions sur ce qui se passe au sein du PDP 1. Si des personnes veulent participer ici, n'hésitez pas à lever la main sur Zoom ou ici dans la salle. Nous n'avons forcément pas beaucoup de temps. Nous avons un ordre d'appel pour nos panélistes. Si vous n'êtes pas prêts, dites-le-nous. On pourra vous demander de prendre la parole plus tard.

Alors du CSG, le groupe des parties prenantes commerciales, nous avons Ching Chiao. Donc je vais passer la parole à Ching.

CHING CHIAO Merci. Je représente la CSG et BC bien sûr. Je vous remercie de m'avoir invité. Comme l'a dit Justine, je suis un des membres, mais je ne peux pas -- je peux parler au nom de CSG et de la BC. Je vois qu'il y a d'autres membres du groupe de travail dans cette salle. Donc, bien sûr, n'hésitez pas à prendre la parole si nécessaire.

Donc, pour répondre à cette question spécifique, ce que l'on a comme point de vue au BC, ce que l'on pense, c'est qu'il y a eu un

bon début de travail pour ce groupe de travail. Donc, le démarrage a été très constructif. Les conditions du groupe de travail sont intéressantes. L'atténuation de l'utilisation malveillante du DNS reste la priorité de la communauté.

Donc, il y a une deuxième chose dont je voudrais parler, c'est le fait que nous reconnaissons aussi la fatigue au sein de la communauté, cette communauté qui gère ce thème, ce thème de la politique liée à l'abus du DNS. Donc, je dois dire que la fatigue, elle existe aussi en dehors de la communauté. C'est la fatigue des clients, des organisations et beaucoup de membres ou des professionnels de la cybersécurité, des personnels avec qui je travaille. Il y a aussi de la fatigue dans ce sens, parce que c'est vraiment compliqué de travailler sur cette utilisation malveillante du DNS. Ça prend beaucoup de temps et c'est fatigant.

Alors, par rapport à ces deux déclarations, le BC et la CSG ont tout de même des inquiétudes par rapport au calendrier. Donc, le défi -- l'enjeu que nous avons d'un côté est lié au processus des PDP qui est maintenant élaboré par le personnel. Ce PDP potentiel pourrait s'arrêter donc à la fin de 2027. Mais en fait, en réalité, on ne sait pas ce qui va se passer, quelles seront les menaces en 2027. Cette atmosphère de l'abus du DNS, ce paysage va changer. Donc, [il] va pouvoir mettre en œuvre ces politiques à ce moment-là. Donc, en attendant, nous, on regarde un petit peu un calendrier, une chronologie différente. On pense plutôt à 2029 pour la mise en œuvre, puisque cette campagne de l'abus du DNS est rapide. Bon, ça prend des journées, pas des heures. Mais vous savez, ce

calendrier nous inquiète tout de même, parce que tout cela prend du temps.

Et nous voudrions aussi souligner autre chose. Je l'ai d'ailleurs mentionné sur la liste de distribution. Quand on observe l'ADC, c'est une chose. Observer l'ADC, c'est une chose, mais faire quelque chose pour atténuer, peaufiner, c'est autre chose. Donc c'est deux sortes de détection -- donc détection et pas atténuation. S'il y a une lacune entre les deux -- il y a un fossé entre les deux. Donc, il faut vraiment se rendre compte que, dans cet écosystème, toutes les choses prennent du temps. Et il nous faut trouver l'ADC. Il nous faut nettoyer, si on peut dire. Il faut nettoyer ces acteurs qui utilisent l'ADC. Il faut se préoccuper de ces incidents d'abus du DNS. Il y a quand même un grand fossé entre les deux.

Nous avons aussi souligné un autre enjeu, quelque chose qui ne va probablement pas changer, mais je voulais vous en parler pour que vous compreniez bien pour ce PDP en particulier. Le cadre -- la portée de ce PDP est très étroite. Donc, on parle d'un opérateur de registre -- le bureau d'enregistrement. On ne parle pas de multiples ADC sous de multiples bureaux d'enregistrement. Donc, il faut faire une chose d'un coup. Il faut résoudre une question, un problème à la fois.

Je voudrais en terminer en disant que pour la CSG et pour notre participation, sachez que faire avancer ces idées sur l'utilisation malveillante du DNS, c'est bien, cela. Tout ce que l'on a fait jusqu'à présent, c'est de bonne foi. Nous voulons vraiment collaborer.

Nous comprenons très bien que l'ICANN supervise le DNS. Tout le travail qui a été fait dans le passé, qui va se faire dans l'avenir, eh bien, on sait très bien qu'à travers tout ce travail, l'abus du DNS ne va pas disparaitre et que, d'ailleurs, cela va s'intensifier dans les années à venir. On le sait déjà. Mais nous sommes là. Le CSG est là pour collaborer avec vous, pour essayer de résoudre le problème.

Nous sommes très impatients de travailler avec le groupe, de travailler avec toutes les personnes qui sont là dans cette salle. Je m'arrête ici. Merci à vous.

JUSTINE CHEW Merci, Ching, pour cette contribution. J'espère que nous pourrons ensuite poursuivre dans le cadre des questions-réponses de la discussion. Je suis désolée. J'aurais dû dire que les membres du panel doivent se contenter de parler pendant 3 à 5 minutes. Michaela, vous êtes la suivante dans la file d'attente.

MICHAELA SHAPIRO Merci beaucoup de cette occasion de prendre la parole. Et je représente le groupe des représentants des entités non commerciales. Alors, nous avons un sujet qui est donc dans le cadre du travail qui vient de commencer. Nous n'avons eu aucune discussion sur le sujet.

Donc, hier, nous avons lancé cette discussion sur la question de la charte. Qu'est-ce qui doit déclencher la vérification de domaines associés ? Nous en avons parlé, donc au sein des représentants des

entités non commerciales. Nous avons décidé qu'il ne fallait pas agir de façon hâtive. Et il faut tenir compte du paysage dans lequel il y a des préoccupations sécuritaires. Et nous voulons faire les choses comme il le faut, sans nous presser. Les solutions doivent être équilibrées, donc en tenant compte des parties prenantes, y compris les intérêts des titulaires de noms de domaine.

Donc, ce sera un processus intéressant. Ça sera un travail qui pourra commencer dès le début du processus d'élaboration de politiques. Nous souhaitons élaborer un processus, un cadre, qui pourrait couvrir les différents types d'utilisation malveillante du DNS. Et à mesure que le paysage des abus évolue, nous pourrons traiter les différents sujets qui émergent.

Donc, le champ d'application du PDP lui-même entre dans le cadre d'une charte qui est limitée, et il faut donc se cantonner donc aux attributions qui nous sont données. Et le calendrier doit être raisonnable. Et il faut surtout éviter d'être trop pressé. Je sais que j'ai peut-être manqué certains éléments, donc je vais maintenant conclure et attendre des questions éventuelles.

JUSTINE CHEW

Merci, Michaela. Oui, vous l'avez dit correctement. Nous parlons de l'abus du DNS, tel qu'il est défini par l'ICANN. Nous ne parlons pas des abus généraux qui se déroulent sur Internet. Nous restons cantonnés dans le cadre de l'ICANN. Eh bien, donc, il y a maintenant le groupe de travail relatif à la sécurité du GAC. Je ne

sais pas si vous souhaitez donc vous exprimer. Donc, le groupe de travail sur la sécurité publique du GAC.

JANOS DRIENYOVSZKI

Oui, je vais m'exprimer au nom du GAC, peut-être. Oui, comme Michaela l'a dit, nous sommes à la phase précoce du PDP 1. Et au cours des séances précédentes, il y en a une qui traitait de la substance du PDP. Évidemment, le GAC a une approche optimiste et nous avons aussi des avis optimistes. Et nous espérons pouvoir bien contribuer aux résultats de ce PDP qui est ciblé. En raison de cela, nous espérons que le calendrier sera optimal afin que nous puissions terminer ce qui nous a été confié dans les temps impartis.

Donc, c'est un champ d'application relativement étroit qui traite d'une thématique très spécifique, à savoir la vérification de domaines associés. Et ce PDP, donc, sera un exemple de la façon de livrer quelque chose de façon efficace dans le cadre de l'ICANN.

Je note aussi ce que Ching a dit tout à l'heure concernant les lacunes pour l'atténuation et le traitement des problèmes. Nous considérons que les mesures prises dans le cadre de cette nouvelle politique font évoluer toutes les mesures qui sont disponibles pour les parties contractantes. Il y a un temps de réaction qui est nécessaire — un temps de réaction suite au signalement. Et il s'agit de rester dans la conformité. Et l'idée, c'est de trouver des politiques qui traitent réellement les abus du DNS et de savoir comment les types d'utilisation malveillante qui surviennent peuvent être traités de façon efficace. C'est une politique qui doit

être utile pour vraiment traiter les questions d'abus du DNS. Il faut une approche coordonnée qui aide le comité que je représente, le comité, donc, s'occupant de l'application des lois, et aussi donc les parties contractantes. Voilà, je m'arrête ici. Merci.

JUSTINE CHEW Merci Janos. Poursuivons. Nous donnons la parole à mes collègues. Steinar ou Kathleen, l'un de vous souhaite prendre la parole ?

STEINAR GRØTTERØD Bonjour, c'est Steinar de l'At-Large. Je suis d'accord, c'est un très bon début. Et c'est très intéressant d'entendre les différentes approches venant des différentes parties prenantes.

Du point de vue d'At-Large, nous n'avons rien inscrit dans le marbre pour le moment. Mais d'après ce que je comprends — et je parle à différents bureaux d'enregistrement—, l'une des choses que nous essayons d'atteindre et de réaliser, c'est d'avoir une politique consensuelle qui, très franchement, puisse forcer les mauvais bureaux d'enregistrement à agir. Car la majorité de ces bureaux d'enregistrement font déjà des choses. Et il faut qu'il y ait une meilleure conformité de la part de ceux qui sont, entre guillemets, mauvais.

Nous avons une approche qui est davantage proactive pour parler de l'atténuation des abus du DNS. Et je suis donc heureux de voir ce qui va en résulter. J'ai hâte de voir ce qui va en résulter. Il y a des

rumeurs qui disent que cela ne peut pas être fait en un mois, mais je dirais qu'il faut rester optimiste.

Kathleen, est-ce que vous souhaitez ajouter quelque chose ? Eh bien, Justine, nous vous rendons la parole.

JUSTINE CHEW

Merci, Steinar. Je vais laisser un peu de temps pour permettre à ceux qui souhaitent faire des commentaires de le faire. Pas trop tout de même. Nous avons des commentaires en ligne qui posent des questions sur l'impact sur les droits de l'homme — les droits humains.

Alors je vois la main de Volker qui se lève. La main virtuelle de Volker. Disons que si l'un des panélistes souhaite répondre à cette question relative aux droits de l'homme, dites-le. Mais en attendant, Volker, vous avez la parole.

VOLKER GREIMANN

Volker Greimann. Donc, si je m'exprime à titre personnel. Je note les efforts qui ont été faits. Je considère qu'il y a eu beaucoup de réflexions menées sur le sujet. Et je pense que nous pensons de façon trop étriquée. Il ne s'agit pas simplement de mauvais bureaux d'enregistrement. Même les membres du BC peuvent faire quelque chose contre les utilisations malveillantes du DNS. Et il y a des acteurs qui gagnent des milliards en regroupant -- en procédant à des agrégations et en redirigeant les utilisateurs de l'Internet. Il y a des acteurs qui tirent des profits considérables. Et

cette question n'est pas traitée. Il y a de mauvais acteurs qui ont été donc radiés par les parties contractantes, et ils surgissent ailleurs. Donc, leur site est supprimé, mais il surgit ailleurs. Donc, il y a des méthodologies changeantes en fonction des marchés et il n'y a pas vraiment de mécanisme de partage des informations. Par exemple, si je prends un mauvais acteur parmi les bureaux d'enregistrement, si je le supprime, il va refaire surface ailleurs. Donc, il n'y a pas vraiment de bon mécanisme.

Nous raisonnons de façon trop étriquée. Il nous faut raisonner dans le cadre de l'ensemble de l'écosystème. Cela concerne tout le monde. Les forces de l'ordre doivent intervenir. Elles doivent arrêter ces mauvais acteurs. Je ne veux pas être grossier. Donc ce n'est que quand ils seront sortis de la circulation que leur action malveillante pourra cesser.

Nous pouvons agir dans notre petit écosystème, mais ces acteurs malveillants ne pensent pas comme cela. Ils agissent à travers l'ensemble du secteur, à travers l'ensemble des bureaux d'enregistrement. Quand je dis que nous exploitons plusieurs bureaux d'enregistrement, cela veut dire qu'il y a des campagnes. Donc, il peut y avoir un bureau d'enregistrement dans le secteur du commerce de détail qui peut traverser l'écosystème. Et donc, même si on agit de façon immédiatement, eh bien, ils vont, ces mauvais acteurs, activer un autre domaine. Et donc, tout ce que nous disons à l'heure actuelle, c'est trop étriqué.

Cela ne veut pas dire que nous ne devons rien faire, mais nous devons donc voir plus grand.

JUSTINE CHEW Merci, Volker, pour cet apport. Je pense que personne au sein de la communauté ne s'oppose à ce que vous dites, mais la question est de savoir comment y parvenir. Je ne vois personne qui souhaite se prononcer sur la question des droits de l'homme. Je dirai juste que -- quelqu'un, donc Michele, a levé la main, peut-être.

Donc, il y a la question de l'impact sur les droits de l'homme, qui intégrée dans le PDP 1. Et si j'ai bien compris, il faut que cela soit intégré, donc d'emblée plutôt qu'à la fin du processus, comme c'était le cas précédemment. Ainsi, ça sera un élément qui aura toute sa place.

Il y a la question de la protection des données à caractère privé.

Donc, il faut tenir compte -- il faut prendre en compte différents aspects et non pas simplement les abus de DNS.

MICHELE NEYLON Vous me donnez une minute ? Je pense que c'est comique. Donc, Volker a abordé pas mal de choses. Je ne vais pas y revenir.

Concernant la question des droits de l'homme, il faut être conscients, très conscients, du fait qu'il y a un risque de réactions intempestives chaque fois qu'une politique est mise en œuvre pour les petits bureaux d'enregistrement qui ne sont pas conscients, qui

n'ont pas connaissance du contexte général. Donc, ils vont peut-être essayer de se conformer. Nous avons vu qu'il y a eu des modifications de contrat. Il y avait des noms de domaine qui étaient supprimés suite à un seul signalement de la part d'un utilisateur. Et c'était très aléatoire, et c'est un peu ridicule. Il a fallu plusieurs jours pour savoir qui contacter au sein du registre, pour savoir s'il y avait donc un domaine de secours et comment réinstaurer le domaine suite à, donc, l'enquête.

Donc, on voit souvent cela comme étant une façon de nettoyer l'Internet. Et il y a des gens qui considèrent que c'est une façon de cibler les concurrents. Ils considèrent que c'est cela qui est derrière ces politiques -- donc, s'attaquer aux concurrents dans leur secteur. Et donc ils considèrent que ces politiques sont néfastes.

JUSTINE CHEW Merci, Michele. Oui voilà, c'est une position que les bureaux d'enregistrement devraient appliquer. Donc voilà, je voudrais passer au prochain sujet, s'il vous plait. Michelle, voulez-vous passer à la prochaine diapositive, s'il vous plait ? Très bien.

Comme je l'ai dit tout à l'heure, nous avons le privilège d'avoir une meilleure compréhension sur ce qui est des algorithmes de génération de domaine qui causent des abus. Donc c'est déjà -- ce sont des logiciels malveillants qui créent des milliers de noms de domaine. Ce sont des algorithmes qui sont utilisés par les mauvais acteurs pour faire des choses malveillantes. Donc j'ai demandé à Janos de venir nous parler un peu plus de cela, à savoir ce qui a été

fait et à savoir comment nous pouvons faire avancer ce travail au sein de la communauté. Janos, allez-y !

JANOS DRIENYOVSZKI

Très bien. Donc, c'est mon ami Gabe Andrews qui était derrière cette initiative. Mais moi, je vais essayer de vous la présenter au mieux possible. Donc voilà, ce cadre de travail, enfin -- donc, ma présentation, c'était de vous montrer que tout cela était compliqué de gérer [cela], surtout pour les forces de l'ordre. Et il faut donc mettre en œuvre un cadre commun pour les opérateurs de registre et les forces de l'ordre, afin de lutter à grande échelle sur ces logiciels malveillants et les infrastructures de réseaux zombies. Donc voilà.

Il faut parler du cadre qui a été visé par le comité des [RySG]. C'est un cadre de travail non contraignant qui n'a pas d'impact sur les politiques. Donc voilà. Comme l'a dit Justine, ce genre de logiciels qui sont utilisés par les criminels ne sont pas toujours détectables. Alors, ils collectent beaucoup de nombres, de chiffres et de lettres. Alors, les criminels bougent et vont de nom de domaine à un autre nom de domaine et continuent leurs activités en distribuant bien sûr des logiciels malveillants. L'intention de ces acteurs est d'éviter toutes les contremesures de la sécurité qui sont conçues pour prévenir ces mêmes criminels d'atteindre leurs victimes, comme le blocage, par exemple, de domaines sur un réseau.

Comme vous le voyez sur la diapositive, il y a une liste, à gauche, des caractéristiques du DGA. Et à droite, vous pouvez avoir la liste

des impacts qui correspondent à ces différentes caractéristiques. Donc, il n'est pas toujours facile de bloquer un domaine, car, dès lors, bloquer un nom de domaine est inutile parce que l'algorithme en génère des milliers d'autres. Voilà, donc ils peuvent en créer des milliers et retenir donc le contrôle et redistribuer des mauvais logiciels à travers des réseaux zombies.

Je pense qu'il y a un impact, car, pour les forces de l'ordre, il est compliqué de porter plainte. Parce qu'il faut passer à travers de milliers de nouveaux domaines. Ça coute cher pour créer ce cycle qui se répète indéfiniment, sans fin en vue.

Prochaine diapo. Alors pourquoi on a besoin de cette coopération ? Pourquoi veut-on que ce soit un peu plus efficace entre, donc, les forces de l'ordre et les opérateurs de registre ? Donc, le cadre de travail et le rôle de ces parties prenantes, voilà, quel est-il, surtout lorsqu'il faut gérer les mauvais -- les logiciels malveillants et les réseaux zombies, les infrastructures de réseaux zombies et de logiciels malveillants.

Alors, le DGA doit retenir le contrôle, passer au-delà des réseaux zombies. Ils doivent être utilisés pour gérer la liste -- une large liste de domaines qui n'ont pas d'algorithmes, qui ne sont pas gérés par des algorithmes.

Alors, il y a deux outils qui sont utilisés du côté des opérateurs de registre. C'est la réserve -- le côté où ces opérateurs peuvent réserver des domaines et créer un nouveau domaine. Donc, réserver un domaine, c'est quand un opérateur de registre place le

nom de domaine DGA sur une liste réservée. Donc c'est efficace, parce que ça empêche les criminels de générer ce genre d'attaque, ce genre d'abus. On n'a pas besoin d'une autorisation de l'ICANN. Les opérateurs de registre peuvent agir immédiatement, donc il n'y a pas de trop de couts au niveau administratif, si vous voulez. Ça ne permet pas le travail de ce qu'on appelle les domaines *sinkhole* sans fin, mais ça nous permet d'identifier les machines qui sont infectées et aussi d'envoyer des notifications aux victimes.

Donc alors, le *sinkholing*, ce qu'on appelle le *sinkholing*, donc, ça permet aux noms de serveurs de noms de domaines de faire participer les forces de l'ordre pour identifier les victimes de ces logiciels malveillants et d'identifier donc les machines qui sont sur ce réseau zombie. Alors donc, le trafic de ces réseaux zombies est capturé et analysé -- et peut être analysé. Ça résout quoi ? Eh bien, cela permet de réserver -- de faire des domaines de réserve. Cela aide à identifier les machines et les victimes. Et ça prend en charge la notification active des victimes et la remédiation. Et ça fournit des renseignements pour les enquêtes policières en cours.

Et bien sûr, il y a des restrictions contractuelles de l'ICANN. Bien sûr, vous avez sur la liste les sections concernées. Donc, à l'écran 2.9, 6.1, 6.3. Les opérateurs de registre doivent aussi obtenir une autorisation et des frais s'appliquent.

Le processus ERSR résout ce problème. Donc, c'est un acronyme pour ce qui est une demande de sécurité pour les opérateurs de

registre -- une demande rapide. Alors, de ce côté contractuel, les opérateurs de registre peuvent se baser sur cela pour se protéger.

Prochaine diapositive. Très bien. Le rôle du cadre, c'est de développer donc une meilleure compréhension des problèmes auxquels on fait face -- auxquels font face les forces de l'ordre et les opérateurs de registre, et donc toutes les informations liées au DGA. Donc, il faut essayer de comprendre la portée du problème, comment le soutien soit -- comment est-ce que le soutien est apporté. Donc, tout ce qui est lié à l'utilisation de ces DGA.

Vous voyez qu'il y a quatre piliers dans ce cadre. Alors, cela nous permet d'envoyer des informations à temps aux forces de l'ordre pour qu'ils puissent agir. Et aussi, ça nous permet de trouver des solutions. En fait, il s'agit de solutions à long terme qui pourraient nous permettre de créer des réactions durables pour pouvoir faire face justement à ces DGA. Je vous invite vraiment à lire toutes ces informations.

Il y a un document qui a été publié par le [RySG]. Cela vous donnerait -- il y a même des annexes aussi, je pense, qui vous permettraient d'avoir plus d'informations. Vous pouvez faire -- il y a le formulaire que nous utilisons pour faire les demandes ESRS, donc l'aide à la demande accélérée de sécurité du registre.

Et bien sûr, nous espérons que ce cadre fournira une certaine inspiration dans d'autres domaines, d'autres domaines qui auraient besoin de ce système -- de ce programme.

Nous nous sommes basés sur des exemples pratiques. Il y avait -- nous avons utilisé des cas, de vrais cas -- des cas réels que nous avons utilisés. Donc, en termes de base de recherche pour trouver des solutions. Et donc, à partir des informations fournies par les forces de l'ordre, par les opérateurs de registre, nous voulons trouver des manières pour sauver -- pour économiser du temps, pour économiser des efforts, pour économiser nos dépenses.

Voilà, je vais m'arrêter là. Bien sûr, si vous avez des questions, j'essaierai d'y répondre.

JUSTINE CHEW Merci d'avoir pris le temps de nous présenter ces informations, Janos. Je vois qu'il y a une main levée dans la salle Zoom. Volker, je vais vous demander si c'est une question ou si vous allez faire un commentaire. Enfin, allez-y Volker.

VOLKER GREIMANN La question est sur le manque de compréhension. On voit les DGA comme des outils, comme des armes, comme des scripts, comme des algorithmes. Ce sont des outils qui peuvent être utilisés à toutes sortes de fins. Alors, beaucoup d'entre eux sont utilisés à des fins malveillantes. Qu'est-ce qu'on fait comme différence entre les DGA qui sont utilisés pour de bonnes choses et ceux qui sont utilisés pour de mauvaises choses ? Est-ce qu'on met tout ça dans le même sac ? Comment est-ce qu'on fait la différence entre les positifs et les négatifs ?

JUSTINE CHEW Qui veut répondre ?

NAOUM MENGOUDIS Lorsque nous trouvons ces algorithmes DGA, on vérifie bien sûr ce qui est utilisé, à quel but ça a été utilisé. Est-ce que c'est pour des campagnes d'hameçonnage ? Est-ce que c'est pour la dissémination ? Donc, on essaie de vérifier cela et on fait ce qu'on appelle de l'ingénierie inversée. Et donc ce n'est pas fait au hasard. On a un cadre de travail pour atténuer justement et pour nous permettre d'agir plus vite.

JUSTINE CHEW Est-ce qu'on peut revenir sur notre ordre du jour, s'il vous plait. Donc maintenant, on va rentrer -- on va commencer à converser. Donc, on va commencer la conversation maintenant. Je voudrais ouvrir les micros sur Zoom et dans la salle et inviter John en premier. Ensuite, Mukesh. Donc, John en premier pour qu'il nous parle de ce dont on parle aujourd'hui. Et bien sûr, nous avons une question pour lui. Nous voulons lui demander quel est le rôle que l'ICANN pourrait jouer dans ce domaine? Est-ce que c'est un rôle de coordination ? Est-ce que le rôle pourrait être -- le rôle de l'ICANN pourrait être de coordinateur général ?

JOHN CRANE J'ajouterai une chose. Nous avons quinze ans d'expérience dans notre travail avec des personnes en dehors de la communauté sur

la façon de traiter les DGA. Donc, ce que nous pouvons faire ou devons faire dépend de la politique et des contrats. Donc, évidemment, nous ne voulons pas que le personnel, tout d'un coup, s'aventure à créer leur propre chose. Il faut une politique et suivre la politique.

Donc, en 2010, il y a une conversation qui a été assez douloureuse. À l'époque, nous n'étions pas encore au même niveau qu'aujourd'hui. Il a fallu avoir une meilleure procédure de partage des informations. Je dois dire que je suis heureux que ces discussions resurgissent. En 2010, quand nous avons émis une proposition, ce n'était pas forcément pour dire que l'ICANN devait faire ce travail, mais il était nécessaire d'avoir une coordination. La discussion était intéressante. Et cette discussion a émergé en raison de ce que faisait l'ICANN autour de 2010 autour des DGA. Et il y avait des logiciels malveillants qui utilisaient des technologies. C'était Configure, par exemple, qui était le plus connu d'entre eux, de ces logiciels.

Et nous avons travaillé. Au début donc, nous avons travaillé avec les forces de l'ordre, les groupes s'occupant de sécurité publique et différents acteurs. Et donc, quand on s'attaque à ces DGA, bien sûr qu'il ne suffit pas d'avoir une liste. Il faut savoir que beaucoup de travail doit être fait pour éviter de porter préjudice et victimiser donc des personnes ou des acteurs qui ne sont pas malveillants.

Et donc nous avons utilisé différentes terminologies. Et au cours des quinze dernières années, nous avons travaillé avec les forces

de l'ordre, les membres de la communauté de la sécurité publique et des opérations. Et ainsi, chacun sait quelle est la différence entre enregistrer un nom et supprimer un nom de domaine. Donc, nous avons parlé des *sinkholes*, de ces trous noirs.

L'ICANN, dans tous les cas, peut être un expert sur la façon dont le secteur fonctionne afin de travailler de façon efficace et obtenir les résultats que nous souhaitons tous, à savoir une meilleure sécurité publique. Donc, actuellement, nous n'entrons plus dans ce genre de discussion, car les gens comprennent la méthodologie au fil des évolutions. Nous continuerons, je l'espère, à avoir un impact. Si la communauté trouve des solutions, des solutions qui exigent des politiques, eh bien, nous les mettrons en place.

Si ce qui ressort de ces PDP est donc étendu, sachant qu'il faut un effort de coordination qui n'est pas forcément facile. Nous ne sommes pas le seul secteur qui essaie de s'attaquer à cette thématique, y compris le partage des informations. Le partage des données, comment le faire de façon sécurisée. S'attaquer à tout cela, c'est un projet multiannée et ce n'est pas dans le budget de notre plan stratégique. Mais nous souhaitons assumer notre rôle -- jouer notre rôle.

Nous avons effectué des adaptations par le passé. Nous avons obtenu beaucoup de réponses dans le cadre de ce ERSR. Ces choses ne restent pas stagnantes. Je pense que ce ERSR de 2009 a évolué. Peut-être que vous pouvez nous en parler, Mukesh.

MUKESH CHULANI

Donc, le ERSR est un service qui cible les opérateurs de registre. Nous avons vu une présentation à ce sujet. Donc nous avons noté -- c'est-ce qu'a dit John, nous avons noté l'évolution des processus existants. Le secteur évolue. Nous recevons des informations disant que les registres ne sont pas les seules exigences ERSR. Donc, ce ERSR aurait donc supprimé les frais pour l'ICANN, mais pas pour les bureaux d'enregistrement. Alors, cela crée une situation d'inégalité.

Et nous avons corrigé les choses en 2021. ERSR, c'est un acronyme qui n'est plus d'actualité. C'est donc une suppression des frais pour la réponse en matière de sécurité. Et il y a le potentiel de création d'un impact à long terme. Et il faut que l'entité agisse lorsqu'il y a une question sécuritaire.

Donc, nous avons des règles de base, et c'est donc en raison de l'évolution des choses.

JUSTINE CHEW

Merci Mukesh. Alors, voici ce que je voudrais voir. Je vais permettre de procéder à une discussion. Je vais laisser du temps pour la discussion. Et donc s'il y a la possibilité de répondre dans le chat à la question soulevée par Steinar. Donc, dans le temps imparti qu'il nous reste, je voudrais entendre des choses. Nous avons entendu parler, donc -- parler du cadre d'une manière générale. Nous

savons qu'il y a eu des mises à jour. Nous savons que c'est un thème qui existe depuis assez longtemps.

Alors, la question que je pose au panel, c'est comment prendre tous ces renseignements pour déterminer comment aller de l'avant ? L'une des questions est la suivante : est-ce qu'il faut un processus d'élaboration de politiques ou est-ce que nous devons donc agir à l'extérieur d'un processus d'élaboration de politiques ? Est-ce qu'il faut impliquer la communauté ? Qui sont les membres de la communauté qui doivent être impliqués ? Est-ce que c'est tout le monde ? Est-ce que les membres du panel peuvent répondre à ces questions-là ?

J'ai vu que Ching avait la main levée tout à l'heure. Je vais lui donner peut-être la parole.

CHING CHIAO

Ching au micro du BC CSG. Donc la réaction initiale après avoir entendu John, où il nous a dit qu'il a fallu plusieurs années pour accomplir ce travail, il a fallu donc faire adhérer les ccTLD parce que nous avons vu qu'il y a la question des DGA, non seulement pour les gTLD, mais les ccTLD, la question que je pose, c'est : pour les collègues du GAC ou les collègues des forces de l'ordre, je dois dire qu'il y a des tactiques que j'ai constatées — c'est que ces trous noirs, ces techniques, ne sont pas les plus efficaces.

Ces techniques ne sont pas les plus efficaces. Donc, les forces de l'ordre les plus performantes, est-ce qu'ils laissent de côté

délibérément ces noms malveillants, en fonction ? Et les réseaux zombies et les noms de domaine malveillants doivent être cartographiés. Il s'agit d'attendre avec patience et de, ainsi, répertorier toutes les grappes de DGA.

JUSTINE CHEW Est-ce que John voudrait répondre ?

JOHN CRANE Oui, je réponds partiellement. Donc, quand on remonte en arrière, les ccTLD donc entraient dans le cadre d'un processus volontaire de la part des registres et des bureaux d'enregistrement. Il ne s'agit pas simplement d'atténuer les DGA. Il faudrait une politique qui n'existe pas. Et donc il y a des CC qui ne sont pas couverts par la politique. Beaucoup de ccTLD avec qui j'ai travaillé souhaitaient donc une politique. Je crois qu'il y avait une question qui s'adressait aux collègues de PSWG.

NAOUM MENGOUDIS Si j'ai bien compris, la question qui se trouve dans le chat, peut-être qu'elle peut être reformulée ? Les registres réservent certains domaines donc, sachant qu'ils sont mis sur une liste réservée et puis, ensuite, ils peuvent être libérés et ne plus être dans la liste réservée concernant les forces de l'ordre, leur flux de travail qui peuvent continuer d'exploiter les DGA ou certains réseaux zombies, les laisser continuer à fonctionner afin de pouvoir les suivre et ensuite nous pouvons les contacter.

Et il s'agit de dégager des statistiques. Parfois, les forces de police, lorsqu'elles s'emparent d'un serveur, il peut y avoir un serveur malveillant. On peut laisser ce serveur malveillant continuer de fonctionner, pas pour qu'il infecte des machines, mais simplement pour l'observer. Donc, il ne s'agit pas simplement de le laisser fonctionner pour porter préjudice.

JOHN CRANE

Donc, pour résoudre ces infections, je ne peux pas dire que la méthode est sophistiquée, mais elle est plus élargie que ce que vous dites. Il y a une organisation qui s'intitule Shadow Server. Il y a là des forces de l'ordre, qui recueillent des données. Et ensuite, il y a une enquête auprès de différents acteurs pour comprendre quel est le taux d'infection.

Donc, nous, nous raisonnons de notre point de vue. Nous pensons simplement aux blocages, à l'arrêt des DGA. Mais ce que j'ai appris, c'est qu'il faut remonter à la racine de l'infection afin de faire cesser le préjudice aux utilisateurs finaux.

JUSTINE CHEW

Merci pour cette conversation. Si vous le voulez bien, levez la main sur Zoom. Il nous reste encore quelques minutes pour couvrir ce sujet. Je ne souhaite pas donc empêcher la conversation. Je vois Michele et Steinar, si vous voulez bien lever la main pour prendre la parole. Sinon, nous passons. Donc, si vous souhaitez prendre la

parole, levez la main sur Zoom, ainsi, nous aurons plus de facilité à suivre ce qui se passe. Michele, allez-y !

MICHELE NEYLON

Oui, lorsqu'il s'agit du GAC, comme l'a dit John, on sait qu'il y a eu beaucoup de coopération entre les ccTLD. Les ccTLD sont très flexibles dans la manière de faire les choses. Ils ne sont pas contraints au contrat de l'ICANN. Donc un ccTLD -- moi, je parle de la part d'un bureau d'enregistrement pour .IE, nous avons vu aussi une augmentation de certains types d'utilisation malveillante par rapport au grand nombre de domaines qui avaient été enregistrés. On a vu qu'il y avait des enregistrements pour des buts malveillants qu'il y ait un DGA ou pas.

Oui, nous remboursons. Nous ne sommes pas pénalisés financièrement pour faire la bonne chose. Et je pense que ça, c'est le point clé dont on ne discute pas, le fait qu'un bureau d'enregistrement ou un opérateur de registre sera pénalisé financièrement pour essayer de retirer des choses négatives de l'Internet ou malveillantes de l'Internet, c'est vraiment la situation la plus stupide de ce service. Franchement, ça n'a aucun sens pour moi. Et je ne comprends pas pourquoi quelqu'un, en toute bonne foi, peut défendre ce processus.

Du côté des bureaux d'enregistrement, nous avons des limites très strictes sur le nombre de noms de domaine sur lesquels on peut

agir. On a une période où l'on peut agir. Je pense qu'on a cinq jours au début et donc on a beaucoup d'éléments qui rentrent en jeu.

Donc, pour un opérateur de registre important qui a un grand volume d'enregistrements tous les mois, vous savez, le pourcentage de personnes qui sont pénalisées serait assez large. Donc, pour un petit opérateur de registre, si on cible les mauvais acteurs, ça arrive de temps en temps, le seuil est différent.

Les politiques qu'on a en ce moment sont tellement contraignantes que ça me couterait des milliers d'euros en dépenses administratives pour potentiellement retrouver un remboursement. Si je faisais ça pendant un trimestre, je ne pourrais pas le faire pendant les trois trimestres à venir. Donc, pour moi, c'est vraiment aberrant et c'est quelque chose auquel on doit faire face. Et je pense que ça va devenir un problème de plus en plus important. Et si on ne le fait pas maintenant, opérationnellement, ça va devenir impossible à mettre en œuvre.

JUSTINE CHEW

Oui, merci. Merci à Michele. C'est quelque chose -- je suis complètement d'accord avec vous là-dessus. Peut-être quelque chose que l'on peut faire en dehors du PDP, on pourrait peut-être mettre ça dans les priorités. Steinar, Siva aussi. Mais donc il faut que j'arrête de prendre des commentaires parce qu'il faut qu'on avance. Et je sais que j'avais dit que, Steinar, je lui donnerai la parole. J'avais dit ça tout à l'heure.

STEINAR GRØTTERØD Je voulais clarifier quelque chose par rapport à la question que j'avais dans le chat.

Est-ce que c'est vraiment possible de créer une liste pour les opérateurs de registre ? Est-ce que c'est une liste que l'on va devoir contrôler de façon régulière pour qu'on puisse la modifier, la réajuster, etc. Je voudrais juste essayer de comprendre ce problème à partir de là.

JUSTINE CHEW Naoum, vous voulez répondre à cela ?

NAOUM MENGOUDIS Oui, bien sûr. Alors, il faut faire de l'ingénierie inversée pour donc réajuster l'algorithme déjà. Et il faut savoir à quel point, dans le temps, quel domaine va être généré. Donc, si on sait aujourd'hui mardi à 10 h et demie, on sait que l'algorithme va générer une URL spécifique. Bon, on peut, si on le sait, on peut le bloquer. On peut peut-être le mettre sur une liste importante pour que les opérateurs de registre puissent registre gérer cette liste. Ou alors vous pouvez faire fonctionner l'algorithme vous-même pour savoir si le domaine est malveillant ou pas, et vous pouvez le bloquer.

Donc, il y a une question intéressante lorsqu'il s'agit de -- qui pourrait peut-être -- on pourrait peut-être résoudre le problème en utilisant les meilleures pratiques. On pourrait mettre en place des

politiques pour que tout le monde se coordonne et tout le monde soit conforme.

JUSTINE CHEW

Merci. Merci. Siva, je dois avancer donc je vous demande d'aller mettre vos commentaires ou votre question dans le chat de Zoom.

On passe à la prochaine diapo, s'il vous plait. Michelle, la prochaine diapo, s'il vous plait. Très bien. Je pense que nous avons quelques problèmes techniques. Est-ce que quelqu'un peut faire avancer la présentation ? La personne qui est responsable du déroulement de la présentation pourrait faire avancer. Donc à la prochaine page. Voilà, c'est la section dans laquelle on voudrait encourager le travail de la GNSO, à savoir ce que l'on pourrait mettre sur le radar, s'ils pouvaient peut-être trouver une manière de le faire, s'ils ne le font pas à travers un PDP. Donc parler d'un format de meilleures pratiques. Peut-être que le comité pourrait être impliqué et on pourrait peut-être gérer cette question en dehors d'un PDP.

Prochaine diapo, s'il vous plait. Je vais donc demander aux panélistes de nous parler d'une ou deux de leurs priorités, en dehors de celles qu'on a déjà identifiées, l'API, les noms de domaine associés, le PDP 2, donc, et aussi donc le DGA dont on vient de parler. Donc, en dehors de ces quatre thématiques, y a-t-il d'autres priorités sur lesquelles on peut parler ? Voilà, c'est donc maintenant que vous allez pouvoir nous parler de ce sur quoi on doit travailler dans l'avenir. Alors, dans l'ordre, je vais inviter les

panélistes à prendre la parole. Je ne sais pas qui veut prendre la parole pour le PSWG.

JANOS DRIENYOVSZKI. Janos au micro. Alors, au sein du groupe de travail sur la sécurité publique pour le GAC, nous sommes intéressés d'avancer un petit peu sur ce qui est de l'exactitude des données d'enregistrement. Je pense qu'on n'en est pas où on devrait en être dans ce sens. Donc, il nous faut parler de la chaine de distribution, pas forcément que des opérateurs de registre. Il nous faut qu'on discute des revendeurs, des fournisseurs de proxy de confidentialité.

Donc, il y a un rapport qui a été sorti de la GNSO en septembre 2025, qui identifiait justement ces lacunes — les lacunes dans ce domaine. Alors, on a parlé de la vérification des comptes, des données de contact, etc., des vérifications d'identité après l'enregistrement, des activités malveillantes. Encore une fois, tous ces domaines de transparence qui pourraient bien sûr être mieux faits, donc voilà, ce sont des domaines dans lesquels il nous faut travailler. Ce sont des domaines qu'on a mentionnés.

Comme l'a dit Justine, on a aussi parlé des domaines associés, du DGA. Donc voilà. Donc, ce sont les choses qui me viennent à l'esprit maintenant.

JUSTINE CHEW S'il y a des personnes dans la salle ou sur Zoom ? D'ailleurs, nous aimerions que vous fassiez attention à ce que les panélistes

proposent maintenant. Ces informations ne seront pas sur le sondage qui va arriver à la fin de cette présentation.

Donc, écoutez ce que nos panélistes disent maintenant et retenez ces informations.

NAOUM MENGOUDIS

Oui, je pense qu'il nous faut parler des sous-domaines, de l'utilisation malveillante des sous-domaines. Parce qu'on voit ce cas souvent. Il y a beaucoup de campagnes d'hameçonnage, des campagnes de logiciels malveillants sur ses sous-domaines. Et donc il y a ce problème. Il y a eu ce problème avec PayPal aussi. Donc ça, je pense que c'est une des carences, une des lacunes qu'il nous faut étudier aussi dans ce sens. Il nous faut essayer de collaborer au sein de l'écosystème, en général, comme pour ce qu'on devrait faire d'ailleurs sur les vérifications de domaines associés. Ce n'est pas juste les opérateurs de registre qui devraient faire le travail de leur côté. Donc, il y a beaucoup de travail à faire à travers tout l'écosystème en général.

MICHAELA SHAPIRO.

Je représente l'unité constitutive des parties prenantes non commerciales. Alors, quand il s'agit des priorités pour nous, il nous faudrait nous focaliser sur le processus d'atténuation des utilisations malveillantes du DNS. Et donc, il nous faut qu'il y ait des mécanismes qui soient standardisés pour tous les utilisateurs de noms de domaine. Et donc, il faudrait peut-être établir des

manières de faire les choses, des parcours à suivre pour les utilisateurs de noms de domaine. Et, par exemple, dans le cas où un domaine peut être renouvelé, il nous faudrait penser aux différents appels -- aux différents processus d'appel qui sont disponibles.

Alors, on doit travailler sur tout type de domaine et sur tout type d'abus du DNS. Je pense que, comme mes panélistes, comme Janos l'a dit, il y a des tas de choses qui -- des tas de thématiques qui nous intéressent en ce moment. Donc beaucoup de choses qui sont liées justement à ces actions liées à l'utilisation malveillante du DNS, genre de décision, de processus de décision, de transparence sur toutes sortes d'actions d'atténuation qui sont en cours qui seront mises en œuvre.

Bon, je pense que c'est tout pour moi. Merci de m'avoir donnée la parole.

JUSTINE CHEW Merci, Michaela. Ching, à vous maintenant.

CHING CHIAO Ching Chiao du BC CSG. Donc, encore une fois, au PSWG, on a mis la -- on s'est concentré sur les sous-domaines aussi parce que c'est vraiment une de nos préoccupations. On a parlé de la capacité. Et dans ce sens, je voudrais souligner le potentiel du DGA ou des domaines -- les réseaux zombies, etc., les clusters d'ADC dans ce cas-là. Vous savez, lorsqu'il s'agit des clusters d'ADC. Ça prend

beaucoup, beaucoup de temps. Il y a aussi la question des sous-domaines qui potentiellement pourraient être élaborés au-delà des ADC ou des DGA. Voilà, donc il y a des tas de questions sur, encore une fois, des tas d'enjeux au niveau des sous-domaines. C'est vraiment un point sur lequel on devrait se concentrer.

JUSTINE CHEW Allez-y, Kathleen.

KATHLEEN SCOGGIN Kathleen Scoggins Je pense qu'on va recevoir beaucoup d'informations après la publication de ce PDP et à savoir si le modèle va identifier une portée, un cadre de travail pour que l'on puisse avoir des informations, pas seulement sur les carences, les carences en elles-mêmes, mais aussi sur des mécanismes de redressements potentiels pour savoir si ces carences peuvent être résolues donc avec ce PDP.

Donc, si on décide, après le PDP, que le modèle n'est pas efficace et que l'on passe à une des mesures plus proactives, comme l'utilisation des algorithmes prédictifs, etc., de prédiction, etc., donc pour nous, à l'ALAC, ce qui est important, c'est de servir les utilisateurs finaux. Donc, il nous faut mettre -- on va peut-être devoir mettre en œuvre un cadre différent parce qu'il y a des [inaudible] des acteurs différents. On va bien voir ce qui va se passer après ce PDP, quelle direction on va pouvoir prendre et on

va voir ce qui est dans l'intérêt des utilisateurs finaux donc de l'ALAC.

JUSTINE CHEW Merci Kathleen. Maintenant, on va passer à la participation de l'audience. Et en fait, il nous reste très peu de temps. Donc, je voudrais demander à Kathleen de récolter les informations venant de Zoom et des personnes qui sont dans la salle. Allons-y Kathleen.

KATHLEEN SCOGGIN Alors, il y a des participants à distance. Nous avons cette question donc : quelle mesure préventive donc doit être dans la liste des priorités d'un PDP ? Donc, nous avons parlé des DGA, l'identification des coordonnées, la détection en temps réel, les algorithmes prédictifs et les flux, donc, concernant l'usage malveillant et les données, donc, menaçantes. Donc, qu'est-ce qu'il faudrait mettre dans la liste de priorité ? C'est ça, la question.

Je vais laisser cette diapositive à l'écran, [ainsi] que vous puissiez la lire. Et ensuite nous allons mettre le Mentimeter. Si vous avez votre téléphone, sortez-le et vous pourrez flasher le QR code.

JUSTINE CHEW Nous pouvons tout d'abord passer à cette diapositive avec le QR code. Je crois que le personnel va afficher le lien vers ce Mentimeter. Vous pouvez soit flasher le QR code ou alors utiliser le lien qui se trouvera dans le chat. On m'a dit que le lien Mentimeter est dans le chat. Nous allons vous donner quelques secondes pour

décider si vous souhaitez utiliser le QR code ou le lien Mentimeter, et nous reviendrons ensuite à la diapositive des questions.

Retournons à la diapositive précédente. Ainsi, tout le monde pourra bien comprendre les questions qui sont posées ou la question qui est posée. Nous n'avons qu'un espace limité pour expliquer ce que nous faisons. Ce sont les cinq options qui ont été sélectionnées. Donc, dans le rapport GNSO, donc, la GNSO a identifié ces lacunes qui, si elles sont comblées, eh bien, il y aura une mesure préventive. Donc, nous parlons de prévention et non pas de cure. Donc, il faut vraiment faire de la prévention. Donc, ces options sont issues de ce qu'il y a dans le rapport. Vous voyez, ce sont donc des mesures de nature préventive.

KATHLEEN SCOGGIN Alors, une fois que vous avez terminé, je crois qu'il va falloir cliquer. Ainsi, nous pourrons passer à la rubrique suivante en quelques instants avant de passer à la deuxième question.

MICHELE NEYLON Je voulais faire quelques commentaires en examinant ces options proposées. Il n'est pas très clair pour moi quand est-ce que cela prendrait place. Je ne sais pas comment ça serait utilisé. Je sais qu'il y a des chevauchements et il y a des choses qui ne sont pas dans les attributions de ce qu'un bureau d'enregistrement ou un registre doit faire. Nous n'avons pas forcément la capacité de

réaliser ces choses. Je vois le terme algorithmes, cela me fait froid dans le dos.

JUSTINE CHEW

Merci, Michele, pour ce commentaire. Donc cela provient du rapport de la GNSO et nous accueillons volontiers vos retours. Il s'agit simplement de prendre le pouls de la salle. Mais il faut savoir que ces éléments sont issus d'un processus qui s'est déjà déroulé. Nous ne sommes pas en train de commencer quelque chose depuis le début. Évidemment, il y a des doublons. Par exemple, l'option deux pourrait combiner deux lacunes. Nous pourrions consolider certains éléments. Alors nous souhaitons recueillir les retours et revenir avec vers le conseil.

MICHELE NEYLON

Je ne voudrais pas entrer dans trop de détails, mais je pense que deux ou trois personnes pourraient dégager deux ou trois thématiques à explorer. Mais quand on parle aux bureaux d'enregistrement et aux registres des questions d'atténuation, quand on leur parle de la vérification des coordonnées des titulaires, eh bien, il faut savoir qu'il y a des acteurs qui sont très forts dans l'usurpation d'identité, etc.

Par exemple, il y a quelque temps, nous avons reçu un coup de fil d'une très gentille dame qui voulait savoir pourquoi est-ce qu'il y avait de l'argent qui partait de son compte. Eh bien, nous aussi, on était très curieux de savoir pourquoi cela était. Eh bien, il s'est

trouvé qu'un acteur malveillant s'était donc immiscé dans ses comptes en banque, avait surmonté toutes les mesures de protection -- donc, la vérification des coordonnées des titulaires, je ne sais pas.

En ce qui concerne les algorithmes prédictifs, il faut comprendre comment les domaines sont vendus. Donc, Volker, par exemple, il n'a pas les données personnelles ou de cartes de crédit de quelqu'un qui achète un nom de domaine. Et il en va de même pour de nombreux canaux. Il y a de nombreuses données auxquelles nous n'avons pas accès.

Et, en tout cas, la question des algorithmes me fait très très peur. C'est un concept qui est effrayant.

JUSTINE CHEW Merci. Donc, ces éléments sont issus d'une liste qui découle d'un processus de consultation avec la communauté. Et les points que vous soulevez ont certainement été soulevés par votre groupe de parties prenantes.

Alors, qu'en est-il des résultats ? J'essaie de rester dans les temps impartis. Il nous reste sept minutes. Kathleen.

KATHLEEN SCOGGIN Oui, je crois qu'il nous faut montrer les résultats. Est-ce qu'on peut montrer les résultats du sondage ? Ainsi, nous pourrons passer à la

question suivante. Vous aurez l'occasion de proposer vos propres options.

Eh bien, en attendant, je vois Michaela.

MICHAELA SHAPIRO J'avais quelques préoccupations concernant, donc, l'utilisation des algorithmes. Donc, je sais que cela peut-être quelque chose de délicat pour le groupe des représentants des entités non commerciales. Donc, l'une des questions, c'est quelles sont les thématiques relatives, donc, à l'atténuation de l'abus du DNS ? Quelles sont les mesures préventives ? Donc, je vous encourage à réfléchir pour savoir si le PDP ou si l'ICANN sont en mesure de répondre à ces préoccupations.

JUSTINE CHEW Merci Michaela. Donc, la question, c'est de savoir qu'est-ce que l'on doit traiter comme problème dans le cadre du PDP? Quelles sont les priorités ? Donc [il s'agit du conseil de la GNSO de décider] ce qui devra être mis en place ensuite.

KATHLEEN SCOGGIN Le personnel, donc, est invité à avancer dans le Mentimeter jusqu'à la rubrique où il est possible de rédiger son retour.

JUSTINE CHEW Eh bien, pendant que le groupe est en train de rédiger et de réfléchir, j'invite quiconque a un commentaire à utiliser le temps

qui nous reste pour prendre la parole. Je ne vois pas de main levée sur Zoom. Je sais que toutes ces informations sont un petit peu difficiles à assimiler et à digérer. En tout cas, si vous avez des contributions à apporter, faites-le, s'il vous plait. Il ne s'agit pas de quelque chose qui sera inscrit dans le marbre. Il s'agit simplement de prendre le pouls de la salle.

MICHELE NEYLON Nous avons enfin trouvé un terrain d'entente, ce qui est très bien. Je pense que les gens considèrent qu'il y a d'autres façons d'atténuer les abus. Et je pense que de nombreuses choses peuvent être faites du point de vue technique.

La technologie des résolveurs -- il y a plusieurs résolveurs de DNS public. Il y a donc des résolveurs privés aussi qui offrent des couches de sécurité, de mesures sécuritaires. Il y a des vérifications. Et évidemment, il y a les questions de droits de l'homme qui ne doivent pas être ignorées. Mais il existe des solutions. Par exemple, si vous avez une connexion Internet dans une école, vous allez certainement limiter l'accès à tout ce qui est d'ordre pornographique. Donc, évidemment que, si, dans une école, les élèves avaient la possibilité d'accéder à des sites pornographiques plutôt que d'apprendre l'alphabet, eh bien, cela n'irait pas.

En tant que bureau d'enregistrement, nous n'avons qu'une aptitude limitée à faire les choses à certains endroits et non pas partout. Par exemple, je ne peux pas supprimer une image sur un

site Web qui utilise un domaine exploité par notre intermédiaire, sauf si nous l'hébergeons. Il faudrait alors exploiter un service inversé.

Par ailleurs, quand on considère que l'ICANN a toutes les solutions pour traiter les abus de DNS, eh bien, ce n'est pas réaliste. C'est un petit peu comme si on disait, voilà, on leur a demandé de corriger un problème et ils ne l'ont pas fait, ils ont refusé.

Volker a parlé de cela. Pour certains domaines, la seule façon d'y parvenir, c'est par le biais d'une publicité. Donc, ce n'est pas un lien qui est partagé par des amis ou par des gens que l'on connait. Ce sont des liens qui nous viennent par le biais des publicités. Eh bien, donc, les plateformes doivent un petit peu agir.

JUSTINE CHEW Oui, là, on parle de l'univers de l'utilisation malveillante du DNS et pas certainement -- pas seulement de l'utilisation malveillante du DNS sur l'Internet. Bon, il ne nous reste plus de temps. Il est l'heure d'aller déjeuner. Je ne vois pas d'autres questions. Donc, nous allons passer à la prochaine diapositive pour conclure cette session.

Je remercie tous les panélistes qui nous ont rejoints, soit ici, soit en ligne. Nous apprécions vraiment. Et nous espérons que vous allez considérer notre invitation à Séville. Je pense que oui. Nous aurons ce genre de session à Séville. Donc, pour tous les participants qui sont là, dans cette salle et même dans la salle Zoom, eh bien, tous

nos remerciements. Merci de nous avoir écoutés. Merci d'avoir partagé vos commentaires dans le chat et merci d'avoir répondu au Mentimeter. Merci, bien sûr, à tout le personnel qui a été impliqué dans cette séance et surtout le personnel d'At-Large, les interprètes. Nous vous remercions beaucoup pour vos services, et, bien sûr, le personnel technique qui nous aide à avancer. Merci beaucoup à tous.

[FIN DE LA TRANSCRIPTION]