ICANN81 | Réunion générale annuelle – Réunion conjointe : GAC et SSAC
Dimanche 10 novembre 2024 – 16h30 à 17h30 TRT

JULIE CHARVOLEN: Bonjour et bienvenue à la réunion conjointe GAC et SSAC, je suis de l'équipe de soutien du GAC. La séance est enregistrée et est régie par les normes de comportement attendues à l'ICANN et la politique communautaire anti-harcèlement.

Pendant la séance les questions et réponses seront lues à haute voix si elles sont envoyées à travers le chat. L'interprétation pour la séance inclut les 6 langues de l'ONU et le portugais. Si vous souhaitez intervenir, levez la main dans Zoom, indiquez la langue dans laquelle vous allez parler si ce n'est pas l'anglais. Parlez à un rythme raisonnable.

Je cède la parole à Nigel.

NIGEL HICKSON: Bonjour, bonne après-midi. Vous m'avez déjà beaucoup entendu aujourd'hui, j'espère ne pas beaucoup intervenir à cette séance. Et je promets de ne pas parler du tout demain. Nico s'est excusé, il avait une séance du conseil d'administration de l'ICANN à laquelle il devait assister. Mais je n'ai pas beaucoup de travail, comme vous voyez pour cette séance, le rapport entre membres du GAC et SSAC est ce qu'il devrait être. On est à la séance du SSAC et nous sommes ravis d'avoir

l'occasion de les accueillir pour une mise à jour, sachant qu'ils ont énormément travaillé au fil des ans pour contribuer au bon fonctionnement de l'ICANN. Et je suis sûr que vous verrez de vous-même que ce qu'ils ont à dire est très intéressant.

Donc pour l'instant je vais m'en tenir à la modération des questions et des débats plus tard, et je vais céder la parole à Ram.

RAM MOHAN : Merci d'avoir invité SSAC à se réunir au GAC avec vous, c'est toujours un grand plaisir d'être ici avec vous. Je suis le président de SSAC. Avant de me lancer dans notre ordre du jour, je voudrais céder la parole à mes collègues pour leur permettre et leur demander de prendre un petit moment pour se présenter, ils sont membres du SSAC et m'accompagnent ici. Vous aurez l'occasion de voir la diversité de connaissances, d'expériences, d'expertises que nous avons dans la salle.

ROD RASMUSSEN: Rod.

MERIKE KAEO: Merike.

GREG AARON: Greg.

ROBERT GUERRA: Robert.

WARREN KUMARI: Warren.

JOHN LEVINE: John.

STEVE CROKER: Steve.

TARA WHALEN : Tara, vice-présidente du SSAC.

BARRY LEIBA: Barry Leiba. J'ai essayé, mais impossible d'avoir un chapeau plus beau que celui de Robert.

SUZANNE WOOLF: Et parfois je porte trop de chapeaux, je suis Suzanne.

RAM MOHAN : Et vous verrez qu'il y a d'autres membres au fond de la salle et qui lèvent la main, qui sont venus nous accompagner dans la salle pour cette séance.

Nigel, merci de nous avoir invités à venir. Vous devez lever la main, Gabe. Merci de nous accueillir.

Étant donné qu'il y a des délégués qui ne nous avaient jamais vus avant, on s'est dit qu'il valait bien la peine de consacrer quelques minutes à nous présenter, à expliquer qui nous sommes et ce que nous faisons avant d'aborder le vif des sujets.

Diapo suivante.

Lorsque vous regardez quelle est la mission de l'ICANN, il est très clair de quoi il s'agit. Donc la charte du SSAC s'est inscrite directement dans la mission de l'ICANN. Nous sommes un comité consultatif, comme vous, et nous n'avons pas de pouvoir formel au sein de la structure de l'ICANN, ce qui nous convient très bien. Nos avis doivent donc avoir leur propre poids pour être considérés. Il n'est pas question d'avoir un vote pour nous.

Diapo suivante.

Nous avons des membres de partout dans le monde ou moins de presque partout dans le monde. Nous sommes en train d'améliorer la diversité de nos membres. La diversité peut être mesurée de différentes manières, comme vous le savez. Cette année nous avons intégré 9 nouveaux membres dont deux viennent de l'Afrique et d'autres de régions du monde différentes.

Or, la raison pour laquelle sont élus les membres SSAC est en raison de l'expertise profonde et spécifique qu'ils ont dans le domaine dans lequel ils sont spécialisés. La plupart des membres du SSAC sont des experts techniques avec énormément d'expériences dans différents domaines. Nous avons des membres qui ont travaillé dans différents secteurs des identificateurs d'internet. Et c'est à partir de là que nous

obtenons la plupart de l'expertise et des connaissances que nous réunissons au SSAC.

Nous nous concentrons principalement sur les avis techniques que nous fournissons à la communauté que nous desservons. De ce fait, nous essayons d'avoir des membres qui ont une expertise technique.

Diapo suivante.

Voici l'équipe de direction du SSAC. Vous verrez à votre droite, à ma gauche, les membres qui ont été élus pour faire part de l'équipe de direction. Et vous voyez à l'écran également le personnel de soutien aux politiques.

Et je veux prendre un moment pour vous en parler.

À la différence d'autres secteurs de l'ICANN où le personnel de soutien finit par avoir un rôle de soutien à proprement parler, mais au sein du SSAC, ce sont de véritables experts qualifiés en leur propre droit. Donc ce personnel finit par participer et contribuer à nos discussions.

Le rôle n'est pas uniquement d'être des scribes, au contraire, ils ont des orientations utiles, des contributions utiles à apporter lorsque nous travaillons sur les différents sujets qui nous intéressent.

Et regardez les compétences de cette équipe de direction. Et bien au sein du reste du SSAC on en a encore plus. On a des membres du secteur académique, de la société civile, qui ont un parcours dans le secteur commercial, dans le secteur de l'application de la loi. Et, en général, la manière de s'impliquer au SSAC est à travers un processus de candidature. Donc les personnes doivent envoyer leur candidature et

nous avons un comité d'adhésion qui va évaluer les différentes candidatures, qui va mener des entretiens. Et, à la fin du processus, ils vont formuler une recommandation dans laquelle ils suggèrent que les différents experts soient intégrés au SSAC.

Le SSAC a alors la possibilité de donner son avis à propos de tous ces profils et à la fin du processus nous remettons au CA la liste des membres que nous recommandons. Les membres du SSAC sont par la suite désignés par le CA de l'ICANN.

Sur cette diapo qui suit, il y a un autre sujet dont Tara va vous parler, parce que c'est central.

TARA WHALEN : Alors pour ceux qui ne connaissent pas SSAC, nous élaborons énormément de documents techniques et cela depuis des années.

Nous nous concentrons sur différents sujets toujours en lien avec la sécurité et la stabilité des identificateurs de l'internet, mais il y a des sujets qui se répètent et qui sont éternels.

Nous cherchons donc la manière d'aborder ces sujets et d'élaborer des documents qui soient accessibles pour la communauté, surtout lorsqu'il y a des sujets d'intérêts pour vous. Vous pouvez venir nous voir, consulter notre liste de documents et vous informer.

On a ici une liste des principaux sujets. Tout d'abord l'utilisation malveillante du DNS qui est un système d'importance et cela veut dire qu'il y a énormément d'utilisations malveillantes de la part d'acteurs malveillants qui font des attaques de hameçonnage, qui distribuent du

logiciel malveillant. Et donc nous travaillons constamment avec les communautés pour essayer d'atténuer tout ce dommage.

Un deuxième sujet qui est d'intérêt pour les personnes qui s'intéressent à la prochaine série est celui des nouveaux gTLD. À chaque fois que vous voulez enregistrer de nouveaux noms, il y a des implications pour la sécurité et la stabilité du système. On a eu un projet d'analyse par rapport à la collision des noms qui a suscité beaucoup d'intérêts. Et au cours de ce projet, nous nous sommes penchés sur le fait de savoir quels seraient les effets d'un élargissement du système et on a pris des mesures et formulé des recommandations pour éviter des confusions par rapport aux chaines qui pourraient venir s'incorporer.

En troisième, le DNSSEC, l'une des principales technologies consacrées à la sécurité dans le monde du DNS, et comme d'autres nous avons travaillé sur ce sujet pour donner des avis depuis un certain temps, pour faire en sorte que la technologie évolue, qu'elle soit bien mise en œuvre. Nous reconnaissons qu'il s'agit d'une technologie complexe et que très souvent les personnes ont besoin d'aide pour savoir comment travailler dans ce domaine. Et nous essayons de faire en sorte que les personnes aient les bons avis pour se faire.

Donc on travaille sur l'automatisation, par exemple, pour que les personnes puissent mettre en œuvre cette fonctionnalité de sécurité et qu'elle soit accessible facilement.

Quatrièmement, les espaces de noms alternatifs. Vous en avez probablement entendu parler, alors qu'on parlait beaucoup de la chaine de bloc. Bien sûr, ça n'a pas disparu, mais il y avait énormément

d'autres systèmes de noms qui n'étaient pas identiques à ceux proposés par le DNSS. Il y avait des personnes qui travaillaient avec les devises crypto, qui achetaient différents domaines. Et alors il y avait des implications par rapport à la manière dont cela interagissait ou s'intégrait avec le DNS. On se demandait comment prévoir les différents problèmes que pouvait générer la coexistence de ces différents systèmes. Et nous nous penchons sur cela étant donné qu'il s'agit d'un espace en constante évolution.

Et, finalement, un autre sujet qui devrait être de grand intérêt pour les délégués du GAC est celui de la gouvernance de l'internet, mais également la sécurité et la stabilité qui sont les sujets centraux de notre groupe.

Sur internet, il y a beaucoup de sujets dans lesquels on voit une superposition entre les espaces de politique et de sécurité et il y a énormément de questions de part et d'autre. Donc si vous allez prendre des décisions par rapport à ce système, vous aurez besoin d'orientations des experts techniques qui vous aideront à être informés au moment d'élaborer la politique. Et notre objectif est de pouvoir fournir ces informations à partir de notre point de vue technique.

Or, nous savons que la force de notre travail vient de la collaboration avec d'autres groupes qui nous orientent, qui nous font penser aux bonnes questions auxquelles ont doit répondre, qui s'assurent que le niveau de communication soit correct, que l'on fournisse suffisamment de détails.

Et donc nous apprécions énormément nos interactions et nos échanges avec les experts au moment de travailler à l'élaboration de nos avis. Ces personnes nous permettent de penser comment ce travail pourrait être utile pour les participants et pour le public dans l'espace politique. Et c'est cette collaboration qui nous aide à faire en sorte que le produit de nos travaux soit utile pour le public.

En ce moment, nous avons différentes équipes de travail qui élaborent des documents. Et nous avons deux initiatives en cours, d'une part les logiciels à codes ouverts dans l'infrastructure du DNS, parce que vous saurez qu'il y a beaucoup de composantes qui sont mises en place dans l'infrastructure du DNS, par exemple au niveau des résolveurs qui sont des composantes qui viennent des initiatives à codes ouverts qui peuvent être des groupes restreints ou plus élargis avec différents niveaux de financements, avec différents types de responsabilités, d'accords contractuels, des relations avec différentes parties prenantes, et cela fait partie de l'infrastructure fondamentale et essentielle pour l'exploitation du DNS.

Et donc nous nous sommes dit qu'il serait utile de montrer où sont ces interdépendances pour que les personnes puissent voir ces interdépendances avec les logiciels à code ouvert lorsqu'ils utilisent ce type de logiciel et pour remettre en cause certaines des hypothèses que les personnes ont par rapport à ces logiciels, ce qu'elles tiennent pour acquis, ce qu'elles ne peuvent pas faire à partir de ces logiciels, quelle est leur fiabilité et leur force.

Est-ce que Marteen est là ? Non ? Je voulais vérifier qui était là et qui serait là.

Le travail de cette équipe de travail est ce que je viens de dire, mais prévoyez déjà de voir le résultat de leurs délibérations si vous travaillez avec les logiciels à codes ouverts.

Par ailleurs nous travaillons avec le blocage et le filtrage du DNS. Un des mécanismes pour bloquer le contenu en ligne du DNS est utilisé comme une des approches pour administrer le blocage de contenu entre les utilisateurs finaux et les ressources. C'est un travail qui dure depuis un petit moment en tant que technologie et le SSAC se penche sur cela.

Les derniers rapports que nous avons publiés datent d'il y a 10 ans. L'espace technologique a changé et nous avons pensé que le moment était venu de revenir sur cette question, étudier les aspects technologiques des requêtes DNS par exemple, qui sont transportées sur d'autres moyens de transport moins évident qu'avant. Et les informations que les gens reçoivent peuvent être analysées de manière différente. C'est pour cela que nous avons décidé de nous pencher à nouveau sur cette question. Nous avons la chance d'avoir eu la possibilité de parler avec les gens qui s'occupent des politiques de l'ICANN pour savoir quels sont les commentaires qui reçoivent côté politique, pour savoir quelle est la direction que nous devons prendre pour aborder ces questions et ces problématiques.

Donc nous sommes en train de travailler en coopération.

Voilà un aperçu de haut niveau de ce que nous faisons. Nous pouvons rentrer dans le détail et c'est ce que nous allons faire avec la diapo suivante.

RAM MOHAN : Avant de passer à la diapo suivante, Nigel, je me demande si on va répondre aux questions maintenant ou après.

NIGEL HICKSON: J'allais justement intervenir parce que vous nous avez donné pas mal d'informations, c'est très intéressant tout ce que vous avez dit. Y a-t-il des commentaires ou des réactions par rapport à ce qui vient d'être présenté ? S'il y a des personnes en ligne ? Très bien, nos amis lèvent la main. Union Européenne, s'il vous plait ?

GEMMA CAROLILLO: J'ai un commentaire. Tout d'abord, c'est très positif de voir que vous travaillez sur les mêmes problématiques que nous, ce n'est pas toujours le cas, et c'est toujours positif.

Ensuite, j'ai une question par rapport au travail qui est fait en matière de logiciel à codes ouverts, c'est un sujet brulant pour nous et nous voulons savoir si nous pouvons avoir une réunion pour en parler davantage.

BARRY LEIBA: Je suis co-président du groupe de travail qui va produire ce document. Oui, nous serions ravis de vous présenter notre travail de manière périodique, au fur et à mesure de nos progrès. Nous espérons que notre travail sera assez rapide. Et je pense qu'on devrait finir à la fin de nos deux prochaines réunions de l'ICANN. Et, à ce moment-là nous pourrions faire un état des lieux d'où nous en sommes.

GEMMA CAROLILLO: Parfait.

RAM MOHAN : Je voudrais ajouter à ce qui vient d'être dit par Barry, c'est qu'à la discrétion des présidents, les groupes de travail peuvent inviter des experts pour partager des informations ou pour faire des points sur le travail effectué. Donc nous avons la possibilité de faire cela entre les réunions de l'ICANN.

NIGEL HICKSON: Il y aura donc des occasions de revenir sur cette question dans d'autres séances.

RAM MOHAN : Maintenant nous allons passer à la prochaine diapo. Jeff Beds devait présenter cette partie, mais il ne se sent pas bien, et je vais donc faire la présentation à sa place.

Nous avons pensé que ce serait peut-être utile pour vous de connaitre les avis de nos membres par rapport à l'IA et l'utilisation malveillante du DNS. On n'a pas demandé au SSAC de travailler sur cette question et de donner un avis. Donc ce que vous allez voir ici ce sont des informations tirées de l'expertise de nos propres membres. Nous ne parlons pas ici au nom du SSAC, mais il s'agit plutôt une présentation de l'expertise de nos propres membres.

Diapo suivante.

Juste pour jeter les bases de cette présentation, nous savons qu'il y a l'apprentissage automatique et l'IA. L'apprentissage automatique est une sous-partie de l'IA, ce sont des algorithmes qui permettent de faire des prévisions de décision. Alors que l'IA comprend d'autres technologies qui permettent aux machines d'imiter l'intelligence humaine. Donc l'apprentissage automatique est un aspect dans le cadre de l'IA.

L'utilisation malveillante du DNS peut être une bonne application de l'IA, c'est le type de technologie que les malfaiteurs peuvent vouloir utiliser parce que l'IA, et notamment l'IA générative, peut créer des textes, des vidéos et d'autres types d'images, par exemple des logos très précis qui imitent les logos de certaines organisations commerciales. Et ils peuvent faire cela avec les différentes technologies de l'IA comme, par exemple, le filtrage par motif. Et cela permet de créer des images, des messages de courrier électronique, des emails qui semblent être créés par des humains.

Et donc plus vous arrivez à les rendre semblables à ceux qui sont faits par des humains, plus la victime tombera dans le piège.

Donc l'IA générative a plusieurs utilisations. Dans le passé, quand vous receviez un email de hameçonnage, vous saviez qu'il y allait avoir des fautes d'orthographe ou de grammaire, mais maintenant tout cela est bien fait, dans la langue de création du message. Mais aussi, cela peut être dans d'autres langues.

Cela veut dire que l'échelle et la portée du problème s'accroissent de manière dramatique.

Diapo suivante s'il vous plait.

La lutte contre l'utilisation malveillante du DNS a utilisé jusqu'à maintenant la technique du filtrage par image pour essayer de trouver les utilisations malveillantes. On essaie de trouver des informations qui sont sous-jacentes à un nom de domaine ou à un niveau de fraude que l'on peut voir apparaitre, par exemple des adresses IP qui sont associées à une ressource enregistrée et on trouve donc des tendances ou bien on analyse un fichier HTML et on voit qu'il y a certains modèles qui sont réutilisés, on analyse les valeurs H, parce que c'était les humains qui étaient derrière toutes ces actions et il y avait des modèles qui se répétaient. Avec l'IA générative, chaque domaine spécifique ou URL peut être randomisé, complètement. Et chaque message de hameçonnage qui sort, et on parle de centaines de milliers de ces messages qui peuvent être générés dans l'espace de quelques heures et qui peuvent arriver au fichier de zone, avant on avait un message de hameçonnage qui était envoyé à 100 personnes, maintenant on peut avoir des centaines de milliers de messages envoyés et chaque message a l'air authentique et a l'air de venir d'une personne.

Donc il y a des moyens plus efficaces pour tromper les humains.

Quelles sont d'autres utilisations de l'IA pour l'utilisation malveillante du DNS ?

Nous voyons que l'IA commence à être utilisée pour créer des fausses identités, de faux comptes, des faux avis, révisions, et cela est utilisé pour l'enregistrement de noms de domaines et de comptes d'hébergement. Cela est également utilisé pour les images intimes non

consensuelles et pour le matériel pédopornographique. Cela est aussi utilisé pour la falsification de documents, d'images.

On peut créer ces documents d'identités par exemple. Dans certaines juridictions par exemple, vous avez des codes de pays qui disent : vous devez nous fournir une identité pour obtenir un nom de domaine. Maintenant, cette identité peut être générée par l'IA sans aucun problème.

Donc ce mécanisme de sécurité peut être trompé très facilement maintenant. Il y a des images qui sont générées par IA et accompagnent toutes ces activités et elles sont liées aux différents contenus. Vous allez trouver que certaines de ces images sont très réalistes, d'autres le sont moins, mais la technique s'améliore, les mêmes qu'il y a 6 mois produisent des images plus réalistes aujourd'hui.

Diapo suivante.

C'est difficile de lire les informations sur cette diapo, il s'agit des informations qui viennent d'un rapport de recherches et qui nous montrent la fréquence des tactiques pour l'utilisation malveillante à l'aide de l'IA. Vous voyez que la fréquence la plus importante est l'usurpation d'identité, mais elle est utilisée pour amplifier les attaques, pour la falsification, etc.

Cette diapo vous montre les statistiques par rapport à tous ces types d'utilisation malveillante et vous voyez que cette utilisation malveillante est assez importante.

Diapo suivante.

Les images générées par l'IA semblent créer des images de plus en plus sombres et, même si les capacités ne conduisent pas à des attaques plus sophistiquées, nous pensons que l'IA générative a le potentiel d'augmenter l'échelle et la portée de ces attaques. Nous disons ici que les cybercriminels vont progressivement intégrer ce type de techniques. Et je dirais : ils ont déjà intégré les techniques de l'IA et utilisent déjà des systèmes IA dans leur plan. C'est ce que l'on voit de plus en plus.

Prochaine diapo.

Mais alors dans tout cela il y a quand même de bonnes nouvelles. Vous voyez sur cette image des visages mal formés. Et c'est ce que nous avons demandé de l'IA. Encore une fois, nous avons demandé aux moteurs qu'à partir de tout ce qui a été montré jusqu'à maintenant ils nous donnent un résultat. Et voilà ce qu'on a eu.

Diapo suivante.

Même si l'apprentissage automatique et l'IA peuvent être utilisés pour faire augmenter la fréquence de ce type d'attaque, l'IA peut être également utilisée pour identifier les attaques de hameçonnage par email. Les emails qui contiennent des attaques de hameçonnage dans leur génération actuelle et habituelle sont différents des emails générés par les personnes et diffèrent également des emails escrocs qui sont générés manuellement. Donc si l'on combine l'apprentissage automatique et le traitement de la longueur naturelle du texte, l'IA générative, avec ses outils, peut mieux comprendre les processus et générer un texte qui puisse se lire et avoir l'air authentique et généré

par un humain. Et sachant que ces technologies existent nous pouvons utiliser l'IA pour identifier un message généré par l'IA.

Vous voyez ce qui vient. Les vecteurs et stratégies d'attaques qui utilisent l'IA à des fins malveillantes sont déjà à peu près connus de tous, il y a la désinformation politique qu'il est facile de générer par l'IA, pas besoin d'humain qui intervient. Bien sûr, l'utilisation malveillante orientée au profit et l'échelle et l'augmentation de la vitesse des entreprises délinquantes. Mais, bien sûr, l'IA est très en lien avec l'argent que génère le cyber délit pour les attaquants.

Donc les personnes vont changer de stratégie si elles voient qu'il n'y a plus de profit à tirer de tout cela. Donc même si l'IA était utilisée pour pouvoir identifier tous ces types de problèmes, on verrait une évolution qui suivrait. L'IA elle-même évolue très rapidement. Mais, en termes globaux, nous sommes d'avis qu'il s'agit d'une continuité du même monde, des menaces qui existent depuis l'apparition de la technologie.

Il existe des acteurs qui décident d'utiliser la technologie pour tirer un profit, un avantage. Et notre fonction est d'être sûrs d'être toujours à jour par rapport à ce qu'il se passe et déployer des mesures pour atténuer et arrêter ce type de menaces.

Diapo suivante.

Je viens de parler de l'IA et du DNS et je ne vais consacrer beaucoup de temps aux rapports entre le DNS et la chaine de blocs. On en a déjà longuement discuté à d'autres forums et ici nous avons publié un rapport le SAC123 qui est disponible. Nous avons également tenu un panel lors de l'atelier SAC 2024 à Washington en septembre de cette

année. Tout cela est public, ça a été enregistré, vous pouvez y accéder. Et dans ce panel nous avons inclus des experts de l'espace de blockchain actuel ainsi qu'un représentant de l'OCTO de l'ICANN.

Donc il y a beaucoup de collaborations entre le SSAC et le bureau du responsable de la technologie, OCTO, de l'ICANN, afin de veiller à ce que nous soyons d'accord sur les domaines de recherche. Nous ne coordonnons pas par rapport aux résultats exacts de nos initiatives, mais nous essayons de veiller à ne pas redoubler les travaux.

Diapo suivante.

Et pour moi, cette diapo est la plus importante, c'est ce que nous avons à vous demander en tant que membres du GAC.

Au fil du temps, nous avons vu que les décideurs de politique ont besoin de se former, d'avoir un renforcement de compétences sur des sujets clefs et ce de personnes qui savent de quoi elles parlent. Mais que tout cela leur soit présenté d'une manière qui leur soit compréhensible, et non pas en jargon technique.

Nous avons l'occasion et la possibilité de faire cela, nous avons les compétences nécessaires et nous élaborons des rapports. Certes, ces rapports en général s'étalent sur des dizaines de pages, mais nous essayons en ce moment de synthétiser tout cela en documents d'entre 500 et 1000 mots, donc d'une page ou deux.

Mais pour nous, le plus utile serait si vous, en tant que décideurs politiques, quels sont les sujets d'intérêts pour vous, ce qui vous intéresse le plus.

Nous avons 126 documents qui ont été élaborés et il ne nous semble pas efficient d'essayer de tout synthétiser. Dites-nous ceux qui auraient une valeur pour vous et nous allons travailler avec vous pour vous fournir des documents d'information que vous pourriez utiliser avec vos propres publics.

Finalement, nous souhaiterions travailler avec vous et vos gouvernements parce qu'il se pourrait que vous ayez des réunions au cours desquelles vous allez aborder la sécurité, la stabilité et la résilience. Et, sans doute, quand vous irez à ces réunions, vous verrez qu'il y a d'autres collègues ou d'autres décideurs de politique qui sont là, mais sans avoir les bonnes informations, sans connaitre les faits, mais qui, cependant, vont essayer de donner leur avis par rapport à ce qui devrait être fait dans un domaine particulier ou à propos d'un sujet particulier. Et alors on voit qu'il y a un manque de correspondance entre les solutions de politique et la viabilité de ces propositions.

Il nous semble qu'étant donné que vous aidez à élaborer les politiques, il serait mieux que ces politiques soient fondées sur des faits et sur des données concrètes qui pourraient vous aider à être mieux informé, vous et vos gouvernements, au moment d'élaborer ces politiques.

Nous voudrions vraiment pouvoir ouvrir cette voie de communication avec vous et mettre à votre disposition toute l'ampleur d'expertise technique que nous avons, au-delà de nos documents.

Merci.

NIGEL HICKSON: Merci pour cette présentation détaillée. Et si je reprends ce que vous disiez à la fin, il est clair qu'en tant que décideurs de politiques nous utilisons énormément et nous tirons énormément de profits de la communauté technique et des autres secteurs de l'ICANN.

Je me souviens qu'il y a quelques années, lorsque nous discutions de l'utilisation malveillante du DNS par rapport à la série de nouveaux gTLD et à la lumière des rapports du SSAC, je ne sais plus quel numéro de document, mais je me souviens d'avoir lu dans le détail les recommandations que vous formuliez par rapport au sujet et qui ont été fondamentales et ont énormément influencé les recommandations et avis formulés par nous au cours des réunions.

Donc je suis d'accord avec vous, il y a énormément de marches pour que nous puissions mieux travailler ensemble.

Je vois qu'il y a énormément d'intérêts par rapport à la chaine de blocs, en particulier à l'utilisation malveillante du DNS. Et je sens qu'on pourrait travailler ensemble là-dessus. Je suis sûr que c'est une question sur laquelle nous reviendrons sans arrêt. Et donc nous vous remercions d'avoir présenté tous ces sujets et d'avoir attiré notre attention là-dessus.

Voyons s'il y a des commentaires ou des questions dans la salle. Les Pays-Bas ?

ALISA HEAVER: Merci pour cette présentation et pour tout le travail que vous faites. Je devrais probablement savoir cela, mais je ne sais pas s'il y a un agent de

liaison du GAC auprès du SSAC ou l'inverse. Si ce n'est pas le cas, je pense que ça pourrait être très utile.

RAM MOHAN : Merci. Non, je ne crois pas que l'on ait un rôle formel de liaison entre nos deux groupes. Ce serait très intéressant d'envisager de désigner quelqu'un. Au sein du SSAC, ce que nous faisons est ce qui suit : s'il quelqu'un souhaite agir comme liaison, on leur permet de suivre tout le processus d'adhésion pour devenir des membres de plein droit et leur permettre de participer. Parce que vous avez aussi beaucoup d'experts. Donc je pense que ce serait utile, si cela vous intéresse.

Geb, juste devant vous, est membre du SSAC et parfois il agit comme un point de transfert d'information de manière informel. Mais on n'a pas de rôle formel.

NIGEL HICKSON: Merci d'avoir soulevé cette question. Je crois que la réponse est que ce n'est pas un rôle qui existe actuellement, mais c'est à considérer.

Comme vous avez raison, vous êtes un comité consultatif très transparent et votre travail est public, mais il serait intéressant peut-être d'avoir un peu plus de connaissances à propos du travail que vous faites.

Je ne vois rien, avec ou sans lunettes. Quelqu'un d'autre ? L'Australie ?

IAN SHELDON: Il y a une liste d'intervenants qui commence à se former en ligne, mais vous regardez dans la salle.

NIGEL HICKSON: Merci. Allez-y.

IAN SHELDON: Merci de nous proposer de nous aider. Je vois que vous avez énormément d'expertise et des connaissances profondes. Mais comme vous le savez, les membres du GAC en général ont énormément de fichiers à lire et énormément d'informations à digérer au sein de l'ICANN et en dehors. Donc je voudrais savoir ce que vous pensez par rapport à cette proposition d'expertise et de soutien, quelle serait l'ampleur de cette mission ? Est-ce juste à propos du DNS ou pouvons-nous vous demander autre chose en tant qu'experts ?

RAM MOHAN : Pour ce qui est du SSAC, on est limité à une mission, un mandat. Mais vous pourriez également accéder à nos membres, vous pouvez les contacter, s'ils sont prêts à vous aider par rapport à des sujets qui ne sont pas dans la portée du travail de l'ICANN, tant mieux pour vous.

NIGEL HICKSON: Merci. Les États-Unis et puis je passerai à la liste sur Zoom.

LÉONARD HAUSE : Je suis du département d'Etats des États-Unis. Vous parliez de la combinaison entre IA générative et utilisation malveillante du DNS, êtes-vous au courant des meilleurs pratiques utilisées, est-ce que cela se ferait à travers le processus d'enregistrement ou à un autre moment de la chaine ? Est-ce que cela arriverait jusque la racine même ? Donc comment faire en sorte que l'IA générative puisse être arrêtée avant que cela n'arrive à ce niveau de profondeur ? Quelles seraient les meilleures pratiques ? Et merci pour votre excellent travail.

RAM MOHAN : Alors, je n'ai pas de réponse à votre question. Mais on peut demander aux experts du SSAC qui se sont penchés sur la question et on reviendra vers vous.

Au sein de l'espace de l'ICANN, il faut au moins considérer la question de savoir que si, avec l'IA générative en l'espace de quelques heures on peut avoir un nom de domaine qui s'ajoute à la résolution, à ce moment-là on sait qu'il y a énormément de messages malveillants qui seraient envoyés, quelles seraient les mesures qui pourraient être entreprises au sein de l'espace de l'ICANN afin d'atténuer ce risque rapidement. S'il y a des cas d'abus en l'espace de quelques heures, serait-il possible d'atténuer cela à travers l'identification en quelques minutes ?

NIGEL HICKSON: Merci beaucoup et merci pour cette réponse. Nous avons deux ou trois personnes en ligne. Commission Européenne d'abord.

GEMMA CAROLILLO: Merci beaucoup. Puisque vous avez demandé quels seraient nos sujets d'intérêts, je pensais qu'ici, au GAC, quand on a discuté de l'utilisation malveillante du DNS, nous avons évoqué l'utilisation d'outils de prédiction. À la Commission Européenne nous avons une certaine expérience par rapport à cela, mais ce serait intéressant de savoir si vous avez du matériel par rapport à cela ou si vous avez travaillé avec ces outils de prédiction pour prévenir l'abus du DNS avant d'arriver à la phase d'atténuation.

Ensuite, si j'ai bien compris, avec l'utilisation de l'IA et de l'IA générative, nous ne sommes pas en train d'élargir l'espace de risques technologiques, il n'y a pas plus de menaces ou des menaces plus sophistiquées ?

RAM MOHAN : Pour la deuxième question c'est vrai, nous ne pensons pas que le paysage des menaces soit plus important, mais plutôt le nombre de menaces.

Pour la première question, est-ce que nos collègues souhaitent y répondre ?

GABRIEL ANDREWS: Je vais vous donner la perspective des forces de l'ordre. Ce que nous constatons rejoint ce qui vient d'être dit, les gens qui faisaient ce type de délits de manière manuelle adoptent maintenant ces technologies de l'IA. Donc on n'observe pas de nouvelles activités, ce sont les mêmes

tromperies, mais en utilisant des outils plus sophistiqués. C'est le constat que nous faisons.

RAM MOHAN : Merci. Je pense que vous devriez reformuler votre première question pour que les autres membres du GAC fassent plus attention cette fois-ci et puissent vous répondre.

GEMMA CAROLILLO: C'est très gentil de votre part, je vais reformuler ma première question. Vous avez parlé de sujets potentiels qui pourraient être d'intérêt pour le GAC, je disais que dans le GAC, lorsqu'on parle de l'utilisation malveillante du DNS, nous avons évoqué à plusieurs reprises l'existence d'outils de prédiction pour éviter les abus du DNS avant d'arriver à l'étape d'atténuation. Donc je me demande si vous avez travaillé là-dessus, si vous avez du matériel à partager ou s'il y a un travail en commun que l'on pourrait entreprendre en la matière.

RAM MOHAN : Bénédict, vous souhaitez répondre ? Et ensuite, Steve.

BÉNÉDICT ADDIS : Je suis mis sur la sellette. Il existe des outils de prédiction, notamment pour l'utilisation de réseaux zombie parce qu'il y a des algorithmes très prévisibles pour la création de ce type d'attaques, nous pouvons donc prédire de manière assez précise ce type d'attaques. Mais les outils qui

se disent un peu magiques pour pouvoir prédire l'utilisation malveillante, je serais prudent là-dessus.

RAM MOHAN : Steve, vous souhaitez répondre ?

STEVE CROCKER: Pour pouvoir utiliser les processus prédictifs et avoir accès de manière rapide et graduelle aux données d'enregistrement et aux enregistrements eux-mêmes, nous sommes dans une période un peu de transition où nous mettons l'accent sur la vie privée, ce qui est très bien pour se protéger et se prémunir contre des attaques à la vie privée. Mais, en même temps, cela rend très difficile, voire impossible, d'avoir accès à des données en ayant des motifs légitimes, comme cela peut être le cas de faire des analyses prédictives à travers les différents noms de domaine.

Donc c'est un peu difficile. C'est très complexe, le fait de pouvoir accéder aux informations devient difficile pour faire un bon travail au niveau de la prévision. Donc il y a un équilibre entre ces deux éléments.

NIGEL HICKSON: Merci beaucoup et merci pour cette question qui a suscité d'excellentes réponses. Monsieur Santosh, de l'Inde, vous avez la parole.

T. SANTOSH : Merci, Ram, pour cette excellente présentation sur l'IA et l'abus du DNS. Commençons par les bases, comment l'IA peut nous aider avec

l'exactitude du WHOIS ? Parce que c'est vraiment une question fondamentale lorsqu'on parle d'utilisations malveillantes, parce la plupart des informations du WHOIS ne sont pas exactes. Alors, pouvons-nous avoir un outil de l'IA qui puisse identifier des informations du WHOIS qui ne sont pas exactes ?

RAM MOHAN : La réponse spécifique à votre question est la suivante : vous pouvez prendre des algorithmes de l'apprentissage automatique, vous pouvez prendre l'IA et comparer à des adresses réelles et arriver à tirer certaines conclusions.

Mais, comme on l'a dit, une grande partie de ces données ne sont pas disponibles. Donc même si la technologie nous permettait de faire cela, les jeux de données qui pourraient nous servir pour utiliser ces outils ne sont pas disponibles.

BARRY LEIBA: Je voudrais ajouter un élément à ce que vous venez de dire, Ram. Les données qu'il faut vérifier ne sont pas disponibles, mais aussi les données dont vous avez besoin pour entrainer votre machine ne sont pas disponibles non plus.

GREG AARON: Les données de contact des noms de domaine ne sont pas disponibles pour nous, en général, dans le WHOIS par exemple. Cependant, il y a des parties qui peuvent accéder à ces données ou qui les détiennent. Ce sont les opérateurs de registre et les bureaux d'enregistrement. Ces

parties, opérateurs de registre et bureaux d'enregistrement, mettent en place des tests de vérification de données par le biais par exemple de différents outils, comme ça peut être le cas de .NL ou .UK qui le font.

Donc il y a certaines parties qui peuvent vérifier l'exactitude des données et potentiellement l'utilisation malveillante. Nous avons les données d'achat, par exemple, les outils financiers qu'on utilise pour enregistrer un nom de domaine, les adresses IP. Et donc le potentiel pour l'utilisation de l'IA est là, mais se trouve dans les mains de ces parties qui détiennent les informations.

NIGEL HICKSON: Merci beaucoup pour cette réponse. Nous avons deux ou trois autres questions dans le chat. On va passer à ces questions. Et ensuite nous allons devoir clore cette séance. Je ne sais pas dans quel ordre je dois les lire. Marco, vous avez la parole.

MARCO HOGEWONING : Je vais être bref et nous apprécions la proposition de travailler ensemble que vous avez faite. Nous avons beaucoup de domaines sur lesquels nous pourrions travailler ensemble et j'apprécie les explications que vous avez données par rapport à l'impact de ces nouvelles technologies et la stabilité du système DNS.

D'un côté, j'aimerais savoir quelle est la perspective du SSAC par rapport aux dialogues mondiaux qui sont en cours, par exemple le pacte numérique mondial. Qu'en pensez-vous et comment pensez-

vous que cela pourrait nous aider et quelle serait la possibilité pour le SSAC de contribuer à ce type de discussions mondiales ?

RAM MOHAN : Merci beaucoup. La gouvernance de l'internet et la sécurité, stabilité et la résilience du système font partie des 5 piliers sur lesquels reposent notre travail. Nous n'avons pas une structure qui nous permette d'envoyer des agents de liaison dans ces plateformes globales. Or, nous avons des membres qui sont impliqués dans ces discussions dans leur travail quotidien. Et c'est une partie de cela qui nous a amenés à créer le groupe de travail qui se penche sur les logiciels à codes ouverts puisque nous avons constaté qu'il y a un intérêt de la part des gouvernements par rapport à ces sujets.

BARRY LEIBA: Il y a trois façons de décider de travailler sur une problématique en particulier au sein du SSAC. D'un côté, si le conseil d'administration nous demande de le faire. D'un autre côté c'est si la communauté nous demande de le faire. Ou bien parce que nous décidons nous-mêmes de le faire. Donc si vous nous dites qu'il y a une problématique qui est très importante pour vous, nous pouvons entamer un travail là-dessus.

NIGEL HICKSON: Merci pour ces questions. Les États-Unis.

OWEN FLETCHER: Non, je pense qu'il y avait quelqu'un avant moi, ce n'était pas moi qui ai levé la main.

WANG LANG: Je remercie Ram pour cette excellente présentation. Vous avez mentionné qu'il y a des noms de domaine alternatifs. On a parlé des unstoppable domain, à un moment donné. Donc qu'en pensez-vous pour l'avenir ?

RAM MOHAN : Le SSAC n'a pas produit un rapport sur la blockchain, mais nous avons développé un rapport sur l'évolution du DNS. La technologie évolue et nous devons essayer d'intégrer ces nouveaux espaces de nom au lieu d'essayer de protéger notre espace de nom. Hors, le plus important est de se demander si ces autres espaces de domaine doivent s'intégrer dans notre espace de domaine, cela doit être fait de manière responsable, en pensant toujours à veiller à la sécurité, la stabilité et la résilience ; c'est la façon dont nous envisageons le travail là-dessus.

Si nous faisions un rapport sur la blockchain, d'autres aspects ne seraient pas couverts par ce rapport.

NIGEL HICKSON: Merci, Ram.

OWEN FLETCHER: Je suis représentant des États-Unis. Je pense que cela a été une séance fantastique, l'IA et les abus du DNS, ce sont des exemples parfaits de

types de thématiques qui intéressent les gouvernements pour pouvoir prendre des décisions fondées sur certains problèmes. Ce serait excellent d'avoir davantage de sessions comme celles-ci. Et j'ai fait un commentaire sur le chat par rapport à cela.

La présentation décrit un certain nombre d'abus qui ne sont pas strictement des abus du DNS parce que les domaines peuvent être utilisés pour commettre d'autres délits.

Donc la question est la suivante : si j'ai bien compris la présentation, nous constatons une accélération dans la création de ce type de domaines, donc anticipez-vous une augmentation du signalement de cas d'abus dans l'avenir ?

RAM MOHAN : Je vais parler à titre personnel parce que le SSAC n'a pas de position par rapport à cela, mais je pense que ce serait une prochaine étape logique. Quand la technologie permettra de simplifier quelque chose qui est maintenant très complexe et que ce sera moins cher à faire, alors la valeur d'un email de hameçonnage c'est 20 000 USD, si cela coûtait 1000 USD d'enregistrer un nom de domaine, ça ne vaudrait pas la peine. Donc si on pense de manière logique, on peut envisager une augmentation dans ce type d'abus.

C'est mon point de vue personnel, je ne sais pas pour le reste.

MERIKE KAEO: Oui, personnellement, je vois cela au quotidien et je ne fais confiance à rien du tout. Mais, pour moi, l'intéressant est de regarder les

campagnes de spam et ce qu'il se passe, je n'ai pas de filtre à ce niveau-là. Mais, en fait, le type d'emails qui comporte des attaques de hameçonnage sont de plus en plus réels. C'est incroyable. Et même, je crois qu'ils doivent analyser ce que vous publiez sur Facebook ou LinkedIn et vous ciblent spécifiquement pour que l'intelligence qu'ils ont puisse être utilisés pour être plus crédibles. Donc il faut que l'on soit plus rapide pour agir plus rapidement et dissuader tout cela.

NIGEL HICKSON: Merci, merci à tous. Il va falloir qu'on s'arrête là, même si la discussion est extrêmement intéressante. Mais on n'a plus de temps. Ça montre le niveau d'intérêts qu'il y a dans votre excellent travail. C'est formidable de voir qu'on a tant d'experts qui sont venus nous accompagner. Je suis fier de vous avoir parmi nous et de vous avoir.

Je suis émerveillé par le travail technique, le travail des experts, les connaissances que vous apportez, non seulement au travail de l'ICANN, mais au travail de la communauté technique également. Nous espérons que ce ne sera pas la dernière fois qu'on vous verra, on espère pouvoir continuer à échanger avec vous et à vous interroger à propos des différentes thématiques.

Avant de lever la séance, je vais demander à ce qu'on nous rappelle à quelle heure nous commençons demain.

JULIA CHARVOLEN: Nous commençons à 13 h 15, il y a la cérémonie d'ouverture dans la matinée, mais les séances du GAC reprennent à 13 h 15 pour discuter des questions d'enregistrements associés avec les données WHOIS.

NIGEL HICSKON: On a énormément de temps.

RAM MOHAN : Merci, Nigel, de nous avoir accueillis, je parle au nom du SSAC, nous espérons également que ce ne sera pas la dernière fois et nous espérons continuer de collaborer avec vous.

[FIN DE LA TRANSCRIPTION]