ICANN72 | Réunion générale annuelle virtuelle – Présentations de NextGen
Lundi 25 octobre 2021 – 10h30 à 12h00 PDT

DÉBORAH ESCALERA: Nous allons maintenant lancer l'enregistrement.

Bonjour à toutes et à tous, bienvenue à cette séance des présentations NextGen. Je m'appelle Déborah Escalera et je suis responsable de ce programme. Je suis responsable de la participation à distance.

Veuillez noter que cette séance est enregistrée et qu'elle suit les normes de comportement attendues par l'ICANN.

Les questions et commentaires soumis dans le chat ne seront lus à haute voix que s'ils sont soumis dans la fenêtre questions/réponses, je les lirai à haute voix pendant le temps alloué par le président ou modérateur de cette séance.

Le service d'interprétation simultanée sera disponible en anglais, français et espagnol. Cliquez sur l'icône d'interprétation sur Zoom et sélectionnez la langue dans laquelle vous souhaitez écouter la séance. Si vous souhaitez prendre la parole, veuillez lever la main dans la salle Zoom et lorsque le modérateur de la séance dira votre nom, notre équipe technique vous permettra d'activer votre micro.

Avant de prendre la parole, assurez-vous d'avoir sélectionné la langue dans laquelle vous allez parler dans le menu d'interprétation. Veuillez

indiquer votre nom pour l'enregistrement et la langue dans laquelle vous allez parler si ce n'est pas l'anglais.

Au moment de prendre la parole, veillez à mettre en sourdine tous les autres dispositifs et notifications. Veuillez parler clairement et à un rythme raisonnable pour permettre une interprétation exacte de vos propos. Tous les participants à cette séance peuvent faire des commentaires dans le chat. Veuillez utiliser le menu déroulant dans le chat et sélectionner « répondre à tous les panélistes et participants », cela permettra à tout le monde de voir votre commentaire.

Veuillez noter que les discussions privées ne sont possibles qu'entre les panélistes dans le format Zoom Webinaire. Tout message envoyé par un panéliste ou un participant ou à un autre participant sera également vu par les hôtes de la séance, les co-hôtes et les autres panélistes.

J'aimerais vous souhaiter la bienvenue et également à tous nos participants de la nouvelle génération. Et j'aimerais remercier mon mentor, Aris Ignacio, qui a parlé, qui a travaillé avec acharnement pour préparer tout cela et aider les jeunes à préparer leur présentation.

J'aimerais également remercier Siranush Vardanyan qui va gérer les diapos et présentations. Merci beaucoup, Siranush. Ceci dit, étant donné que nous n'avons que 90 minutes et 6 présentations, nous allons présenter tout de suite et j'aimerais donner la parole à notre première présentatrice, Sarah Alsamman. Nous allons mettre à l'écran sa présentation. Sarah, vous avez la parole, et on pourra ensuite vous poser des questions. Merci, Siranush, Sarah vous avez la parole.

SARAH ALSAMMAN: Bonjour, merci beaucoup, merci Déborah, merci de m'avoir invitée. Aujourd'hui nous allons parler du DNS et de l'utilisation malveillante du contenu, de la désinformation.

Si vous n'êtes pas déjà au courant, le système des noms de domaine est un système crucial qui permet de se connecter à l'internet avec des dispositifs, et il y a beaucoup d'abus à ce niveau. Tel que l'a indiqué le GAC dans sa déclaration, ceux qui gèrent l'infrastructure du DNS doivent prendre des mesures pour s'assurer que cette ressource publique est sûre et sécurisée.

Cela nous permettra de nous baser sur l'internet pour la communication, pour les transactions.

Mon objectif aujourd'hui est d'encourager un dialogue dans la communauté des parties prenantes pour parler de ces questions de politique et pour encourager également la communauté de l'ICANN à continuer à limiter l'utilisation malveillante du DNS.

Mais avant que nous puissions gérer cela, les bureaux d'enregistrement et les registres doivent bien comprendre ce dont on parle et définir cette utilisation malveillante du DNS.

C'est ce que nous allons voir à la prochaine diapo.

Donc, par rapport au cadre de référence sur l'utilisation malveillante du DNS, il y a 5 essentiellement formes d'abus : les logiciels malveillants,

les réseaux zombies, le hameçonnage, le dévoiement et les courriers indésirables.

Au niveau non technique, également, utilisation malveillante au niveau des contenus.

Pour protéger la liberté d'expression, les registres et bureaux d'enregistrement ne font rien sur le contenu. Néanmoins, dans notre cadre de référence, nous présentons des cas où des registres et bureaux d'enregistrement doivent agir au niveau des contenus, en cas d'abus sexuel des enfants, de trafic d'être humain, de distribution illégale concernant des médicaments dangereux ou bien d'incitation à la violence qui soit spécifique et crédible.

Donc nous avons défini ce qu'est l'utilisation malveillante, les abus au niveau du contenu. J'aimerais maintenant parler des réseaux zombies que nous observons parfois, avec des algorithmes qui sont des instruments de plus en plus influents de perception de notre réalité.

Nous avons beaucoup de réseaux zombies qui permettent de manipuler l'opinion publique, par rapport à des applications de réseautage social, que nous utilisons au quotidien. Il y a donc un travail qui est fait sur les problèmes publics, sur la perception que nous avons des réalités politiques et sociales. On le voit souvent lorsqu'il y a une propagande computationnelle et lorsque les réseaux zombie sont durant une situation de crise ils distordent la réalité et créent beaucoup de dégâts en cas de crise. Parce que ces moments de crise génèrent une incertitude au niveau collectif, le public et les publics sont très influençables à ce moment-là.

Diapo suivante.

Donc il y a eu une étude faite dans le journal britannique de sociologie avec ce qu'on a appelé le bombardement de Manchester, c'est un cas où sur Face Book une femme a indiqué qu'il y avait 60 enfants perdus chez elle et elle indiquait également son numéro de téléphone et on l'a retrouvé sur Twitter et Face Book. On l'a appelé l'Ange de Manchester, le Daily Mail, ce journal l'a appelé ainsi. Mais le problème est que rien n'était vrai, ça ne s'est pas passé, c'était un événement fantôme. La femme a indiqué qu'elle n'avait jamais fait ce poste sur Face Book et n'avait jamais donné son numéro de téléphone.

Il y a eu 28 incidents et évènements fantômes de ce type durant la même nuit. Donc beaucoup de chaos a été créé de cette manière.

Un autre incident en ligne, un poste Face Book indiquant qu'il y avait un tireur avec une arme dans un hôpital, l'hôpital de [inaudible], cela a été partagé par 368 comptes Twitter, l'hôpital a nié cette rumeur, mais elle a continué à circuler durant de longues heures à la suite de l'attaque terroriste. Et il y a eu des ambulances qui ont dû rester sur place pour gérer la situation.

Donc ce sont des situations dangereuses qui ont un impact sur la sécurité des communautés lorsque les réseaux sociaux sont utilisés de cette manière, les services d'urgence, parfois, sont concernés et impactés.

Alors, quelles sont les conclusions et solutions ?

Il y a une véritable menace irréversible sur la sécurité civile, sur la vie des citoyens, il faut parler de politique pour l'avenir et donc avoir l'adoption de mesures proactives anti-abus et qu'il y ait des clauses dans les contrats régissant les bureaux d'enregistrement et les registres.

Merci beaucoup de votre attention.

DÉBORAH ESCALERA: Merci beaucoup, Sarah, très, très bien. Est-ce qu'il y a des questions pour Sarah ? Je ne vois pas de question, il n'y a pas de main levée.

Très bien, donc vous pouvez toujours poser des questions en fin de séance. Ceci dit, nous allons passer à Meri Baghdasaryan, avec sa présentation que nous allons mettre à l'écran.

MERI BAGHDASARYAN: Merci beaucoup Déborah et Siranush. Bonjour ou bonsoir. Je m'appelle Mery Baghdasaryan, je suis de l'université de Pennsylvanie, département de droit, je vais donc parler de l'accréditation et l'anonymisation et l'enregistrement fiduciaire à l'ICANN.

En 2013, dans le contrat d'accréditation des bureaux d'enregistrement, le RAA a indiqué qu'il y avait des rapports qui existent avec les bureaux d'enregistrement et on y parle donc de services d'anonymisation. Et il y a eu des négociations pour ce contrat d'accréditation avec l'ICANN. Ça a commencé en octobre 2011 et on a demandé un rapport de la GNSO et il y a eu une conclusion des négociations. La GNSO a eu un processus de développement pour gérer des points qui n'avaient pas été abordés

durant les contrats d'accréditation, il s'agissait des services d'anonymisation et d'enregistrement fiduciaire.

Il y a une spécification temporaire qui existe au sujet de cela, la date limite a été étendue plusieurs fois et elle doit expirer le 31 juillet 2022 ou bien lorsqu'il y aura un autre contrat d'accréditation des bureaux d'enregistrement.

Donc que voulons-nous dire par l'anonymisation et l'enregistrement fiduciaire ? C'est défini de cette manière : c'est un service qui permet d'avoir des détails de contact qui soient disponibles différemment avec des services d'anonymisation et pas par le titulaire de nom de domaine.

Dans le cas de l'enregistrement fiduciaire, là le titulaire peut donner à une autre personne la possibilité d'enregistrer les informations de contact du titulaire de nom de domaine qui n'apparaissent pas. Ce sont les informations et coordonnées.

NON IDENTIFIÉ : Je vais vous demander de ralentir un peu le débit, on vous entend bien, mais ralentissez un peu s'il vous plait.

MERI BAGHDASARYAN: Donc, dans le cadre de ces spécifications, celle qui est en vigueur actuellement, nous avons un minimum de critères qui doivent être requis et observés, il y en a 4 : la divulgation des termes de service clef, la publication du point de contact et la publication des informations sur le contact commercial, ainsi que l'entiercement des données du client.

Diapo suivante.

Pourquoi parlons-nous de ce sujet ? Pourquoi est-ce important ?

Si l'on revient en 2013, alors que le conseil d'administration avait demandé à la GNSO de travailler là-dessus, et travailler sur ces services d'anonymisation et d'enregistrement fiduciaires pour plus protéger les titulaires de nom de domaine et limiter l'utilisation malveillante du DNS également. Depuis, c'est devenu plus persistant et ça s'est passé beaucoup durant la Pandémie. À l'ICANN 68 on a dit que 65 % des noms de domaine étaient utilisés pour des fraudes et avec des problèmes au niveau de l'anonymisation et l'enregistrement fiduciaire. Il y avait également le RGPD qui a montré qu'il y avait de plus en plus de plaintes concernant l'utilisation malveillante du DNS, avec peu de conformité par rapport aux coordonnées, aux points de contact des services d'anonymisation et d'enregistrement fiduciaire. C'est pour ça qu'il y a eu cette politique de règlement uniforme de litiges relatifs aux noms de domaine pour la réception des coordonnées. Cela a été rendu très clair et a soulevé beaucoup de préoccupations et d'inquiétudes. Et donc cela montre qu'il faut plus de temps pour véritablement développer des procédures solides concernant les coordonnées des titulaires de nom de domaine et la gestion des plaintes. Il faut mieux protéger les titulaires de nom de domaine.

Passons donc maintenant aux demandes du conseil d'administration de l'ICANN auprès de la GNSO, avec la diapo suivante.

Le développement de politique, ce PDP de la GNSO date de 2013. Il y a donc le groupe de travail qui a fonctionné, il y a eu des délibérations du

conseil de la GNSO en janvier 2016, adopté par le conseil d'administration en 2016, et ensuite il y a eu une mise à jour de ces recommandations.

Nouveau programme d'accréditation, comme vous pouvez le voir à l'écran, qui contient des conditions plus nuancées par rapport aux spécifications dont on a déjà parlé. Et à la lumière de ce que vous voyez à l'écran, il est clair qu'un nouveau programme vise à régler le problème dont on vient de parler qui est lié aux services d'anonymisation et d'enregistrement fiduciaire.

Par exemple, cela fournit un cadre clair par rapport aux sollicitudes des forces de l'ordre ou titulaires de droits de propriétés intellectuelles ou fournisseurs par rapport à une communication avec des tiers, vis-à-vis des clients de services d'anonymisation et d'enregistrement fiduciaire, donne également des entiercements de données et rétentions de données.

DÉBORAH ESCALERA: Je vous redemande de bien vouloir ralentir un petit peu s'il vous plait.

MERI BAGHDASARYAN: Merci. Alors, comme vous le voyez, le programme vise à régler le problème lié aux spécifications actuelles pour fournir un cadre plus efficace concernant l'accréditation.

Diapo suivante s'il vous plait.

Donc, comme je vous l'ai dit, après que le conseil de la GNSO ait adopté les recommandations du groupe de travail le conseil d'administration de l'ICANN les a approuvées et envoyées au conseil d'administration pour application. Et il a été entendu que ce nouveau programme d'accréditation allait remplacer le programme précédent.

Toutefois, à l'heure actuelle, la mise en œuvre de ce programme est en attente. La raison en est que l'ICANN s'efforce d'amener les pratiques actuelles de protection des données de telle sorte qu'elles soient conformes avec le RGPD.

Et, pour revenir en arrière, en juillet 2018, après l'annonce de l'ICANN d'adopter les spécifications temporaires, le conseil de la GNSO a lancé un processus d'EPDP, il s'agit du premier EPDP dans l'histoire de l'ICANN. Puis, en mars 2019, le premier rapport sur la première phase de l'EPDP a été adopté, 27 des 49 recommandations contenues dans ce rapport ont été ensuite approuvées par le conseil d'administration de l'ICANN.

Toutefois, conformément à la recommandation 27 de la phase 1, il est apparu clairement qu'à la lumière de ces nouveaux développements, par rapport au fait que l'ICANN souhaitait être plus conforme au RGDP, il fallait réviser les pratiques pertinentes qui sont aussi liées aux données d'enregistrement non publiques. C'est pourquoi ce programme est actuellement en suspens, en attente de sa révision. Et il est clair que les spécifications temporaires et ce nouveau programme tendent dans la même direction, à savoir toutes les données qui ne sont pas publiques.

Après la reprise de cette mise en œuvre, on s'attend à ce que la communauté réagisse sur ce document.

Pouvons-nous passer à la diapo suivante s'il vous plait ? Merci.

Donc les retours d'information de la communauté vont avoir avec une demande vis-à-vis du fournisseur de service d'anonymisation et d'enregistrement fiduciaire, également des procédures. On voit que l'accréditation des services d'anonymisation et d'enregistrement fiduciaire est un aspect important du processus d'élaboration de politique de l'ICANN, mais il s'agit d'un puzzle plus large à l'ICANN en vue d'être conforme au RGPD, c'est pourquoi ce programme est pour l'instant suspendu dans son application. Une fois harmonisé, ce programme, avec les autres programmes en cours, et en tout état de cause, ce programme d'accréditation a une approche plus nuancée que le programme actuel.

Toutefois, les questions sous-jacentes par rapport aux services d'enregistrement fiduciaire et d'anonymisation n'ont pas été réglées, loin de là puisque ça s'est exacerbé durant la pandémie. Et j'espère que la mise en œuvre va avoir lieu suffisamment vite pour régler toutes ces questions sous-jacentes.

Merci de votre attention et j'attends avec impatience d'en apprendre plus sur toutes ces questions lors de l'ICANN 72.

DÉBORAH ESCALERA : Merci Meri. Je crois qu'il y a une question sur le chat : pourriez-vous expliquer ce que veut dire entiercement des données, par rapport à la question que vous nous avez présentée.

MERI BAGHDASARYAN: Oui, alors écoutez, c'est un peu long de répondre à cette question, donc je vais rapidement taper la réponse sur le chat. Mais, en quelques mots, il s'agit de la manière dont les services d'anonymisation et d'enregistrement fiduciaires gèrent une requête de la part des forces de l'ordre ou fournisseurs IP et comment ces données sont retenues par ces services. Voilà, ce serait une réponse rapide. Mais je vais taper sur le chat une réponse un peu plus longue.

DÉBORAH ESCALERA: Très bien, merci beaucoup. D'autres questions pour Meri ? Très bien, alors on va garder un œil sur le chat, merci encore Meri, très bon travail. Et on va passer à notre prochain présentateur, Sai Chandrasekaran et excusez-moi si j'ai écorché un petit peu votre nom de famille. Sai, c'est à vous.

SAI CHANDRASEKARAN: Merci, Déborah et Siranush. Est-ce que mon écran est en train d'être partagé par Siranush ?

DÉBORAH ESCALERA : Oui, dans un instant, attendez un petit peu s'il vous plait. Je crois qu'on a un petit problème technique, attendez. C'est bon, c'est à l'écran.

SAI CHANDRASEKARAN : Très bien, merci Siranush et Déborah. Je vais vous parler aujourd'hui d'une question qui m'intéresse beaucoup dans le cadre de ma recherche : la modération de contenu. Donc la question que je vais couvrir a à voir avec les défis que pose la modération de contenu, la liste en termes de confidentialité et comment aborder une question aussi complexe.

DÉBORAH ESCALERA : Sai, veuillez parler lentement et clairement s'il vous plait.

SAI CHANDRASEKARAN : Alors, quelques informations personnelles. Je suis diplômé de cybersécurité de l'Université d'Indiana et au cours de ces derniers mois j'ai travaillé et fait de la recherche sur certaines questions liées à la gouvernance de l'internet, y compris modération de contenu. Donc je suis très impatient de partager mes connaissances avec vous sur cette question.

Diapo suivante s'il vous plait.

Alors, pour la plupart d'entre vous qui avez suivi les nouvelles, vous aurez certainement entendu parler de cette modération de contenu. De quoi s'agit-il ? Les gouvernements qui détiennent des informations, notamment en période de pandémie, des entreprises sur les réseaux sociaux qui posent certaines menaces par rapport à la modération de contenu, par rapport à la confidentialité, droits humains, et des

individus qui posent certaines menaces par rapport à la modération de contenu, notamment par rapport à la liberté d'expression.

Alors, j'ai créé une brève ligne du temps pour vous présenter cette modération de contenu. J'aimerais vous mentionner les principaux évènements pour vous expliquer pourquoi cette question est importante et pourquoi il s'agit d'une question complexe.

Par exemple, en 2021, il y a quelques mois, nous avons eu un débat aux États-Unis par rapport à une menace importante sur les plateformes des réseaux sociaux par rapport à la mésinformation. Et ce qu'il faut bien comprendre, c'est que la modération de contenu ça n'est pas quelque chose de local qui est lié uniquement aux États-Unis, c'est quelque chose de mondial. En Inde, on a adopté une série de lois numériques en vue de modérer le contenu, pour assurer un suivi. Ça, ça s'est appliqué à Whatsapp qui a d'ailleurs porté plainte par rapport à cette nouvelle réglementation. Et, récemment, il y a quelques semaines, on a d'anciens employés de Face Book qui ont fait un témoignage devant le Sénat par rapport aux pratiques de modération de contenu à Face Book et leurs effets sur la société.

Alors, si vous allez demander à une personne qui travaille dans le domaine de la sécurité, on vous dira que la meilleure manière de procéder c'est de faire une évaluation de risque. Donc c'est ce que j'ai fait par rapport à la modération de contenu et ça se fonde sur la taxonomie développée par Daniel Solove.

Donc imaginez que vous partagez des informations sous forme de message chiffré, dans ce cas, en tant qu'utilisateur, j'ai certaines

attentes de base en termes de confidentialité et je ne veux pas que ce message soit échangé. Mais partons du principe qu'en tant que fournisseur de service j'utilise un algorithme pour détecter si ces messages sont préjudiciables ou pas et expose ces messages.

Dans ce cas-là, d'une certaine manière, je suis en train de violer la confidentialité des consommateurs. Donc ce qu'il faut voir dans l'histoire c'est qu'à chaque fois qu'une nouvelle capacité est développée, il ne faut pas penser à la manière dont on l'utilise, mais aussi comment l'utiliser à mauvais escient.

Donc prenons en considération le fait qu'avec les nouvelles technologies, les nouvelles capacités peuvent être utilisées par les gouvernements, les acteurs malicieux, qui promeuvent la surveillance et peuvent perturber aussi notre société, notamment violer la liberté d'expression. On voit toutes les conséquences importantes.

DÉBORAH ESCALERA : Je vous rappelle de ralentir s'il vous plait.

SAI CHANDRASEKARAN : Il y a d'autres choses aussi dont j'aimerais vous parler, à savoir que parfois l'exposition des informations peut être contreproductive.

Alors, moi je suis utilisateur et mes détails personnels, comme mon orientation sexuelle est exposée au grand jour. Dans ce cas-là je n'ai aucun moyen de me protéger par rapport et à cet effet délétère de cette exposition.

Et voyons des informations financières qui sont divulguées, là c'est un cas différent, vous pouvez bloquer votre carte de crédit comme mesure pour éviter toute fraude. Mais dans ce cas-là, étant donné que vos données de santé sont exposées, vous n'avez aucun moyen de remédier à cela.

DÉBORAH ESCALERA : Sai, vous devez absolument ralentir, vous n'avez absolument par ralenti, s'il vous plait. Donc respirez bien et essayer de ralentir s'il vous plait, Sai.

SAI CHANDRASEKARAN : Oui, je suis désolé Déborah.

Comme je le disais auparavant, je parlais du respect de la vie privée et de la modération du contenu, mais il y a des arguments valides également qui sont présentés de l'autre côté. Par exemple des personnes disent que la modération du contenu peut être utilisée pour arrêter la violence ou pour éviter même [Coupure son].

Adopter une approche avec 3 piliers pour le respect de la vie privée, au niveau technique, une collaboration avec des organisations techniques et des institutions éducationnelles pour collaborer et avoir des techniques cryptographiques qui assurent que l'on détecte les fausses informations et que la confidentialité et le respect de la vie privée soient observés. Par exemple, on peut utiliser au niveau sécurité des techniques cryptographiques qui peuvent utiliser des images comme étant vraie et donc là c'est à parier ou faux, pas d'appariement. Donc on

peut travailler avec les prestataires de service pour effectuer cela avec un programme pilote.

Au niveau du processus également, un modèle où l'on contrôle donc le contenu par rapport aux fake news et aux fausses informations et qu'il y ait un modèle de confiance basé sur la confiance contre la désinformation.

CHRISTINA RODRIGUEZ (Services linguistiques) : c'est très difficile pour les interprètes de vous suivre, donc s'il vous plait, ralentissez le débit, on comprend que vous êtes très enthousiaste, mais merci de ralentir le débit.

SAI CHANDRASEKARAN : Désolé Christina.

Donc le dernier point c'est le principe. Établir donc la confiance entre les parties prenantes. Un exemple ici, un prestataire de service modère le contenu, il faut qu'il y ait une transparence au niveau des algorithmes pour s'assurer que la confiance soit présente.

Diapo suivante.

Donc, ça c'est ma dernière diapo, je pense que la modération de contenu et très similaire aux changements climatiques par exemple, il y a différents pays qui veulent gérer le problème mais les pays ont des compréhensions différentes de la question. Et il y a peu d'homogénéisation.

Donc je pense qu'il faudrait qu'il y ait une approche multipartite à la modération du contenu et pour la limiter. Donc il faut limiter les fausses informations, il faut améliorer les connaissances, la compréhension au niveau des institutions éducatives et des éducateurs, les plateformes techniques doivent avoir moins de déficit d'information, prioriser la détection des personnes qui posent problème et qui ne respectent pas la vie privée. Et les gouvernements doivent avoir au niveau fédéral, au niveau local, au niveau des organisations non lucratives, un bien commun, un élément commun qui doit être dégagé pour des mesures de réglementations et juridiques qui soient appropriées.

Merci beaucoup de votre attention, je suis prêt à répondre à vos questions.

DÉBORAH ESCALERA: Merci beaucoup Sai. Y a-t-il des questions pour Sai ? Je n'en vois pas dans le chat. Très bien.

Donc j'aimerais rappeler à tout le monde que cette séance est enregistrée et que vous serez en mesure d'y accéder dans environ une semaine, vous pourrez écouter l'enregistrement.

Donc nous allons passer… Quelqu'un a levé la main. Enoch, vous avez une question ? Allez-y.

ENOCH NIKINGBOUNG DUUT : Merci beaucoup, une question très rapide. Sur la modération du contenu, il y a deux côtés sur cette problématique, on ne veut pas limiter

la liberté d'expression, mais d'un autre côté, on veut prévenir les contenus qui pourraient être dangereux. Donc est-ce que l'on pourrait trouver une solution médiane qui permette de limiter les risques et, au même moment, ne limite pas la liberté d'expression ? Donc nous posons la question en Afrique notamment.

SAI CHANDRASEKARAN: Merci Enoch de votre question. Pour le moment nous n'avons pas de solution médiane, équilibrée, par rapport à la désinformation et la liberté d'expression, mais vous avez entendu parler de certains points. Lorsque nous avons, par exemple, l'utilisation, les abus sexuels sur les enfants, la pédophilie, tout cela est un problème qui est géré et ce contenu est donc interdit.

Je crois qu'il faut qu'il y ait au niveau de la cryptographie, au niveau multipartite nous pourrions trouver des méthodes pour limiter cela et un travail plus étroit avec les prestataires de service pourrait également être très utile. J'espère avoir répondu à votre question.

ENOCH NIKINGBOUNG DUUT : Merci beaucoup, vous pourrez indiquer cela dans le chat.

SAI CHANDRASEKARAN: Oui, absolument.

DÉBORAH ESCALERA: Merci beaucoup de votre question, est-ce qu'il y a d'autres questions pour Sai ? Très bien. Donc nous allons passer à la prochaine présentation avec Kady Hammer.

KADY HAMMER: Oui, bonjour. J'espère que vous m'entendez bien. Je ne me vois pas, donc je ne sais pas ce qu'il se passait.

Très bien, donc je m'appelle Kady Hammer, je suis étudiante en droit à American Université à Washington, capitale des États-Unis, et je vais parler de ces questions de passerelle et de protocoles passerelles, mécanismes de sécurité que l'on appelle des protocoles passerelle, si l'on veut frontière, Border Gateway Protocole, BGP.

Donc, comment sommes-nous arrivés à ce point ? Je ne suis pas un spécialiste de la technologie, je suis juriste, j'étudie le droit, et donc, comme vous le savez, l'internet a été créé pour la communication principalement. Et la sécurité n'était pas la première préoccupation lorsqu'on a mis en place l'infrastructure de l'internet. Mais aujourd'hui, il y a de plus en plus de menaces cybernétiques et de mauvais acteurs et d'attaques.

En 1989, il y a eu donc ce développement de protocole de passerelle, le BGP, je vais parler donc maintenant en parler.

Le BGP, ce protocole passerelle, se base sur des réseaux individuels qui partagent les informations sur des liens de données disponibles qui permettent à l'internet de continuer sa croissance en tant que réseau mondial, tel qu'il est aujourd'hui.

Ce qu'il faut savoir c'est qu'il n'y a pas besoin d'authentification pour le BGP, c'est un système de routage qui se base sur un cadre de référence de confiance, un système d'honneur si vous voulez. On fait confiance à l'autre réseau, on indique que ce sont de bons acteurs. Donc c'est une solution simple pour des protocoles de routage, et assez versatile pour durer des dizaines d'années.

Vous avez donc ce protocole de routage, avec un diagramme, à l'écran. Comme je l'ai indiqué, c'est pour le trafic de l'internet, c'est son objectif principal, entre les différents réseaux, dispositifs, appareils. Et, comme je l'ai dit auparavant, son intention n'est pas d'assurer la sécurité du trafic ou de la livraison du trafic. Et comme vous pouvez le voir, il y a différents types de protocoles internet. La liste longue, vous l'avez à l'écran, je ne vais pas tout lire, mais vous avez tous ces sigles qui sont indiqués sur la droite de l'écran qui vous montrent comment le BGP et d'autres protocoles permettent le routage et comment les réseaux se parlent entre eux et communiquent. Je vais l'expliquer un peu plus d'ici peu.

Diapo suivante s'il vous plait.

Donc pour rentrer plus dans les détails, la manière dont il fonctionne, c'est un protocole qui choisit une voie pour aller d'un système autonome à un autre sur internet. Il y une carte qui se dessine et les routeurs du BGP reçoivent des informations des routeurs qui sont voisins et choisissent la route, la voie la plus rapide, la plus courte. Et donc cela permet de communiquer avec les routeurs voisins. Et il y a donc cet échange d'information qui se déroule.

Lorsque l'on parle de systèmes autonomes ou de réseaux qui sont utilisés, mais un système autonome parfois, c'est plusieurs routeurs. On peut le décrire en tant qu'un domaine administratif simple et il y a parfois des systèmes autonomes qui incluent aussi plus d'une seule organisation.

Donc il y a des chiffres qui sont assignés par les prestataires, les protocoles de service internet et les utilisateurs finaux s'y connectent, ou bien ce sont les registres qui affectent ces numéros pour les systèmes autonomes de l'internet. Donc cela permet de choisir le chemin le plus court pour les réseaux et il y a donc des routes et des voies tout à fait populaires qui permettent d'avoir un trafic internet très rapide en trouvant les voies où il y a le moins de circulation, on va plus rapidement à un site par exemple.

Donc cela est important parce que les systèmes groupés ensemble peuvent être ciblés ensemble et ils peuvent être également attaqués ensemble par de mauvais acteurs. Et on peut attaquer donc ainsi une organisation, une entreprise dans son entièreté. Donc cela pose des problèmes de sécurité.

Et c'est ce dont je voudrais parler aujourd'hui.

Nous avons des explications qui arrivent dans le chat, nous y reviendrons.

Mais les problèmes de sécurité ce n'est pas seulement avec le BGP, c'est avec d'autres protocoles de routage, et il peut y avoir des erreurs

humaines, il peut y avoir un problème de configuration, une mauvaise configuration accidentelle.

Excusez-moi, je regarde le chat également en même temps.

Donc ce n'est pas exactement un exemple. Mais l'erreur humaine peut poser des problèmes de configuration et peut interrompre la connectivité de l'internet et créer de véritables problèmes.

Mais ce dont je voudrais parler, ce sont les interférences abusives, nuisibles, qui existent et donc des protocoles qui peuvent être des cibles d'attaque ou il peut y avoir des dévoiements, détournements, déni de service, avec une inondation de paquets de mauvaises informations et cela pourrait donc introduire des informations incorrectes dans les tables du BGP. Et, étant donné qu'on a des réseaux voisins, on peut avoir un réseau voisin qui est un mauvais acteur et qui, donc, pose problème et qui vous envoie vers un site web qui est nuisible et qui pose problème.

Donc il n'y a pas de mécanisme d'authentification authentique qui soit intégré au BGP, il n'y a pas de signature numérique du BGP et il n'y a pas d'authentification cryptographique, ce n'est pas une obligation. Si c'est crédible c'est validé puisque, comme je l'ai dit, ça se basait sur la confiance.

Je vais rentrer plus dans les détails.

Donc pour être plus concrète, j'aimerais vous donner une étude de cas sur ce à quoi ressemble un piratage BGP qui a eu lieu via le DNS Amazone. En 2018 un acteur malveillant a utilisé l'attaque BGP qui s'appelle l'attaque de l'homme du milieu pour rediriger le trafic vers la

route Amazone, vers le centre de données, Chicago et IBX. Et la cible était une plateforme de blockchain. Et donc ont redirigé leurs propres trafics de clientèle vers cette autre plateforme qui a piraté les informations des clients.

De quelle manière ont-ils procédé ? Ce trafic de l'internet a été redirigé vers un serveur hébergé en Russie qui a utilisé un certificat et a volé les cryptomonnaies des clients. Cette attaque a requis qu'il y ait un accès au routeur BGP du prestataire de service internet qui a dû faire face à un trafic énorme sur leur serveur.

Pourquoi c'est important ? Cette attaque a mis en exergue les préoccupations existantes par rapport à la sécurité, au niveau du BGP et du DNS et d'une manière plus large par rapport au protocole internet. Et cette attaque à haute échelle montre bien la fragilité du BGP et du DNS qui ont été présentés par les autres présentateurs.

Et le graphe que vous voyez en bas, c'est une vision assez simple de cette attaque.

Alors, comment nous protéger de cela ? D'une manière générale il y a un certain nombre de choses qu'il faut prendre en considération pour faire en sorte que les protocoles soient plus sûrs et surtout que les protocoles BGP soient plus sûrs.

D'une manière générale, il faut mettre en œuvre le IPSec, il s'agit de la sécurité IP, vous pouvez le mettre en place par des infrastructures publiques clefs [PKI]. On doit également établir les responsabilités des personnes qui sont responsables par rapport à l'identité des routeurs

BGP et la personne qui en est responsable. Il faut également renforcer l'infrastructure de l'internet, ce qui implique des investissements conséquents au niveau des prestataires de service et des clients pour déterminer le rôle des IP dans la certification des informations. Bien entendu, la mise à jour de ces softwares physiques, ça implique un coût conséquent. Et il faut maintenir une approche fondée sur la sécurité en essayant d'être aussi proactifs que possible plutôt que d'être réactifs et en fonction d'un certain nombre de critères. Comment déterminer qu'un réseau, un routeur, une personne ou une entité est considérée comme digne de confiance ou mérite d'être authentifié et quand est-ce que vous pouvez permettre à ces routeurs d'être échangés.

Les trois solutions que je propose à l'écran, aucune de ces solutions n'est nouvelle, elles remontent toutes à la création du BGP dans les années 80, ou au début des années 90. Donc il y a un certain nombre de solutions pour protéger les protocoles spécifiquement.

Une option consiste à mettre en place un BGP, protocole de passerelle frontière, avec trois mécanismes. D'abord l'infrastructure qui va être utilisée pour authentifier le propriétaire de l'adresse IP. Autre option à cette première solution, créer un attribut de passerelle utilisé pour signer de manière numérique les informations authentifiées pour que les informations puissent voyager et montrer d'autres informations. Ou, comme je l'ai dit auparavant, vous pouvez utiliser IPSec qui est utilisé pour fournir des données qui permettent d'authentifier les informations avant que les informations ne soient échangées par l'intermédiaire du BGP.

Autre solution, c'est de sécuriser l'origine du BGP, donc ça revient au troisième point de la première solution. Donc avant que les informations ne soient échangées, chaque entité doit certifier ou être certifiée, donc il faut vérifier leurs informations, leurs informations doivent être validées, chaque certificat d'autorisation doit être validé, et ça, ça renvoie au rôle des fournisseurs de service internet.

Il faut voir également où seront hébergés ces certificats et ce que les opérateurs de registre ou parties prenantes de l'internet seront amenés à faire par rapport à cette base de données, et là encore ça nous renvoie à la sécurité de cette base de données.

Autre solution, le transport échelonnable BGP, un autre protocole, il s'agit d'un protocole de transport de propriété. Cette solution n'est pas forcément la plus viable étant donné que cela consiste à rendre privé ce mécanisme. Donc envoyer des messages de connexion à ses voisins plutôt que de se connecter à tous les réseaux.

Bien entendu, il y a un certain nombre de défis qui se posent par rapport à ce protocole, c'est pourquoi les solutions qui existent actuellement n'ont pas été totalement satisfaisantes ou pourquoi nous avons cette discussion aujourd'hui, donc les principales préoccupations ont toujours à voir avec les coûts que ces solutions impliqueraient en termes d'infrastructures, de personnel, de coordination, de responsabilités à définir.

Voilà les principaux défis qui se posent par rapport à ces solutions. Et j'ai d'ores et déjà évoqué la dernière solution, mais celle-ci implique une modification complète du protocole, ça implique beaucoup de travail.

Et, autre élément, ce serait quelque chose de privé, il y aurait un propriétaire, donc ça ne serait pas quelque chose de gratuit. Donc, là encore, on en revient à la propriété privée.

Et, d'une manière générale, le principal défi c'est qu'il semblerait qu'il y ait un manque de sentiment d'urgence par rapport à ces défis, ces difficultés, je vous en ai déjà parlé. La plupart des parties prenantes, y compris moi, ne prennent pas vraiment au sérieux la question de la sécurité. Et, étant donné l'importance de l'internet et le nombre d'années depuis lesquelles l'internet existe, il est important d'être proactif. Et très souvent aussi le problème est vu comme mineur étant les incidents de petite échelle qui se sont produits. Et je sais que ce vol de cryptomonnaie a été réduit et n'a touché qu'une entreprise, mais imaginez à quelle échelle ce genre d'attaque pourrait se produire et les coûts que cela impliquerait.

Donc vous voyez bien, le BGP est l'une des principales cibles maintenant des acteurs malveillants.

DÉBORAH ESCALERA: Excusez-moi, je vous interromps parce que vous avez dépassé de loin vos 10 minutes. On est dans les temps, je vous ai laissé parler, mais il faudrait conclure.

KADI HAMMER : Excusez-moi, j'ai essayé de parler lentement.

DÉBORAH ESCALERA : Oui, vous faites un excellent travail, mais il y a encore deux présentations derrière vous.

KADI HAMMER : Alors j'ai déjà parlé de la plupart des points évoqués à l'écran, pourquoi c'est important, mais l'une des choses sur lesquelles je souhaite insister c'est que même s'il s'agit d'une préoccupation importante, on peut voir les modèles qui existent pour certifier et changer notre approche à la sécurité du BGP et voir comment passer du HTTP au HTTPS pour résoudre ce problème.

Voilà, merci de votre temps et excusez-moi si j'ai dépassé mon temps de parole, parce que normalement je parle beaucoup plus vite.

DÉBORAH ESCALERA: Excellente présentation, très intéressante d'ailleurs. Fascinante. Alors, il y a eu de bons échanges sur le chat pendant votre présentation. C'est un sujet qui intéresse beaucoup.

Y a-t-il des questions pour Kady ? Excellent travail, Kady, bien présenté et bien organisé. Alors, il n'y a pas de question, et sachez que, de toute façon, vous pouvez envoyer vos questions après cette séance.

Donc on va passer maintenant à notre présentateur suivant, Scott Kim. Scott, c'est à vous.

SCOTT KIM: Bonjour à tous. Je suis actuellement étudiant dans le domaine de la sécurité, mon rôle est de collecter les informations, les diffuser aux parties prenantes pertinentes.

Aujourd'hui je vais vous parler de la recherche ICANN pour trouver des IOC, donc indicateurs de compromission. De quoi je vais vous parler ? Le résumé de l'APT41, certaines études de cas, et, enfin, je vais conclure avec certaines recommandations.

Alors, l'APT41, qui n'est pas forcément bien connu ici à la communauté, mais bien connu des praticiens de la sécurité, l'APT41 également connu sous un autre nom, on peut l'appeler donc APT, en français c'est « menaces persistantes avancées ». L'APT41 c'est une menace persistante avancée chinoise qui est liée à une campagne d'espionnage qui remonte à 2012. Et donc cette campagne est liée au parti communiste chinois et la cible était le secteur académique, plusieurs entreprises de jeux vidéo. Et il y a eu plusieurs opérateurs de cette campagne qui ont récemment été pointés du doigt par l'administration américaine.

Récemment, la Blackberry research and intelligence team a découvert une campagne malveillante conduite par des acteurs malveillants et l'APT41 utilise également différents logiciels malveillants, tels que le ShadowPad et on a mis à jour l'infrastructure APT41 en dévoilant le chevauchement entre l'APT41 et d'autres menaces dans le domaine de la sécurité.

Et, comme vous le voyez sur les domaines, ils ont essayé d'utiliser des domaines légitimes dans le cas des 3…

[Inaudible : chevauchement parole, paroles anglaises].

Donc l'outil de recherche de données d'enregistrement de l'ICANN vous permet de trouver des données sur les numéros de domaine sur l'internet. Il faut pour se faire aller sur WHOIS.ICANN.ORG, rentrer le nom de domaine. En particulier, dans le cas de celui-ci, j'ai choisi le nom de domaine qui figure ici, à l'écran et lorsque j'ai tapé le nom de domaine, voilà l'information que j'ai obtenue. Vous voyez des dépositaires de renseignements, et pas d'autres informations.

Donc le domaine qui est mentionné ici appartient à l'adresse IP qui figure à l'écran, qui apparait sur la campagne de logiciels malveillants.

Donc, on veut utiliser ces sources ouvertes et utiliser ces adresses IP et les utiliser pour avoir accès à différentes infrastructures.

Et, comme vous le voyez ici, les dates de certificat ont une validité d'un an, donc ça, ça nous met en garde, nous spécialistes de la sécurité, parce qu'en général on utilise ce genre de nom de domaine fake ou faux à des fins d'activités illicites. Donc toutes ces informations nous mettent en garde.

Donc, pour ma conclusion, depuis l'étude qui a été faite par Blackberry, nous avons appris beaucoup sur cela, c'est par corrélation avec différentes compagnies de sécurité qui étaient déjà au courant, donc ce type de scénario va encourager le partage d'informations pour créer une image beaucoup plus vase sur cette menace. Avec des efforts collectifs, nous pouvons véritablement avoir des activités cybercriminelles limitées.

Si vous avez des questions, faites-le-moi savoir. Merci beaucoup.

DÉBORAH ESCALERA: Est-ce qu'il y a des questions pour Scott ? Très bien, merci. Parfait.

Et bien, nous avons un peu de temps et nous allons avoir notre dernière présentation avec James. James Paek vous avez la parole, une fois que tout cela est à l'écran.

JAMES PAEK: Oui, merci beaucoup Déborah. Je vais parler de l'autoritarisme numérique, comment le contrer.

Vous allez peut-être vous poser la question : qu'est-ce que cet autoritarisme numérique ? Il y a une définition qui existe c'est l'utilisation de l'internet et des technologies numériques en rapport avec cela par des leaders avec des tendances autoritaires pour limiter la confiance dans les institutions publiques, accroitre le contrôle politique et social et saper les libertés civiles. Tout ce qui peut, potentiellement, limiter le respect de la vie privée, la liberté d'expression et tout ce que nous prenons pour acquis. Mais tout le contrôle qu'un gouvernement peut effectuer sur tous les aspects de votre vie.

Donc qu'est-ce qui cause cela ? Et bien c'est comme les gouvernements autoritaires, ça peut être un problème d'instabilité économique, sociétal, politique, une érosion de la confiance publique dans les institutions, un accroissement de la légitimité et de l'autonomie, le

contrôle et la manipulation de l'opinion publique, tout simplement le mécontentement.

Nous observons beaucoup plus de peurs dans nos sociétés, le manque de certitudes avec la pandémie, notamment. Et c'est une des raisons pour laquelle nous avons de plus de manque de confiance dans les autorités. Nous pensons que nous devons obtenir beaucoup plus et c'est très commun également, le nationalisme et le populisme sont en croissance.

C'est pour cela que nous avons de plus en plus d'autoritarisme numérique dans de nombreux pays.

Donc, je crois que nous avons diverses tendances, prenons l'exemple de la Chine, dont on parle beaucoup, beaucoup plus de surveillances, caméra de surveillances, ccTLV en circuit fermé dans toutes les villes, partout où vous allez vous allez être observé par des circuits fermés de caméra de surveillance, dont tous vos comportements seront scrutés, quel que soit votre comportement, s'il ne convient pas, votre comportement social peut être vu comme étant quelque chose de craint par les autorités. Et nous l'avons vu à Hong Kong, pour les citoyens de Hong Kong, depuis 2019 et avec le passage également de la loi sur la sécurité nationale. Je ne vais pas entrer dans les détails, mais je peux vous dire que récemment cette révolution du contrôle est tout à fait similaire à la révolution culturelle qui existait dans les années 50 en Chine.

Cela peut se dérouler dans d'autres pays également. Et nous le voyons, nous l'observons.

Donc quel est le système de crédit social ? Et bien, ça, c'est votre comportement social qui est noté, on vous donne des notes correspondant à la manière dont vous vous comportez socialement, c'est quelque chose qu'on observe en Chine, être un bon citoyen, on peut être puni pour ne pas l'être, et vous êtes donc noté et vous perdez des privilèges, vous ne pourrez pas voyager librement, vous serez puni d'une manière ou d'une autre si vous ne vous conformez pas socialement.

On l'a vu également en Corée du Sud, les célébrités de Corée sont parfois blacklistées, mis sur des listes noires en raison de leur point de vue trop gauchiste éventuellement. Il y a une guerre psychologique qui provient du ministère de l'information pour intimider les utilisateurs de l'internet. Et les activités qui peuvent être vues comme étant en opposition à l'État peuvent être censurées à la suite d'une surveillance.

Sur la diapo suivante nous voyons qu'en Russie, en Belarus, nous voyons qu'il y a beaucoup de surveillance et de limitation de l'internet. Alexandre Lukashenko, le président, a truqué les élections. En Russie également, la Russie a interféré avec les élections présidentielles américaines, avec l'utilisation des réseaux sociaux. Ça c'est une grande inquiétude pour la crédibilité des élections. Et ça donne des doutes sur le système de vote et cela peut influencer beaucoup de ces comportements en disséminant beaucoup de propagande.

En France, nous avons observé une loi sur la sécurité nationale qui donne beaucoup de pouvoir de surveillance au gouvernement français

pour contrôler le harcèlement contre les forces de l'ordre et donc poursuivre en justice les citoyens ayant violé ces lois.

Diapo suivante.

Il y a diverses méthodes pour l'autoritarisme numérique, différents outils sont utilisés, la censure, la surveillance, la manipulation électorale, la brutalité policière, la désinformation, les fausses informations.

Et sur la diapo suivante nous allons voir encore plus de méthodes comme la reconnaissance faciale, les attaques cybernétiques. Tout cela c'est de l'autoritarisme. Et cela inclut également l'espionnage et les fake news, les fausses informations pour la manipulation, notamment des photos, des images prenant divers formats. Cela devient de plus en plus commun. Et beaucoup de citoyens et d'utilisateurs de l'internet ne peuvent pas identifier une source de confiance et une source malfaisante, de propagande.

Donc quelles sont les menaces de cet autoritarisme numérique ?

Et bien, je crois que cela sape la démocratie ainsi que les institutions gouvernementales, les agences gouvernementales, l'engagement civique. Et il y a une violation des droits de l'homme et cela est tout à fait nocif pour l'humanité, cela peut aller jusqu'à plus de harcèlement sexuel et d'autres formes de violences.

Tout cela est en rapport avec l'autoritarisme digital et numérique. Donc les conséquences sont nombreuses à l'avenir et vous pouvez les voir à l'écran.

Là, vous voyez c'est un texte démocratique provenant du magasine The Economist, donc le niveau des démocraties de 167 pays, et bien avec la pandémie nous voyons que beaucoup de gouvernements utilisent de plus en plus d'outils et d'excuses pour en fait être de plus en plus autoritaires et il faut donc se poser la question : comment peut-on restaurer les institutions démocratiques ?

Aux États-Unis, c'est pratiquement un régime hybride, une démocratie faillit parfois, pas complète, pas totale en tout cas. Il y a une détérioration de ces régimes démocratiques qui le deviennent de moins en moins. Si vous regardez de l'autre côté du monde, beaucoup de pays ont connu une détérioration au niveau de leur démocratie et il faut vraiment contrer cette tendance à l'autoritarisme et avoir des approches pratiques pour limiter cela.

Donc utiliser des outils pour limiter les problèmes que l'on pourrait rencontrer dans notre vie quotidienne. Le totalitarisme, on le connait en Corée du Nord, en Chine, mais cet aspect de surveillance peut exister dans de nombreux endroits, donc il faut vraiment réagir.

Et, nous allons le voir avec la diapo suivante, quelles sont ces solutions possibles pour contrer cet autoritarisme numérique.

Moi, je dirais que ce que nous devons absolument faire, c'est de promouvoir la démocratie et les droits de l'homme chez nous et à l'étranger. Première priorité, chez nous, nous voulons notamment que les États-Unis dirigent par l'exemple, et il faut commencer chez nous, dans notre pays, et cela va forcer d'autres pays à devenir plus

démocratique et à promouvoir les droits de l'homme et la démocratie, la liberté et l'égalité.

Hélas, si les États-Unis ne font pas cela, s'ils ne veulent pas et ne désirent pas s'attaquer à ces problèmes, ils ne pourront pas diriger par l'exemple et ne seront pas suivis par d'autres pays. C'est une analogie que je fais, si vous êtes dans une mission diplomatique et que vous représentez les États-Unis, et bien vous allez avoir une perception qui va exister du pays et de la personne que vous êtes.

Donc il faut qu'il y ait plus de confiance dans les institutions publiques, y compris dans les gouvernements. Il faut renforcer la civilité pour limiter les problèmes sociaux et politiques, les divisions notamment dans les pays, la haine, les manifestations violentes, nous devons limiter cela et promouvoir l'unité. Je sais que c'est extrêmement difficile, mais il faut qu'on arrive à plus de civilité, à plus de caractère sociable pour promouvoir et renforcer la liberté de l'internet, l'inclusivité numérique notamment.

Cela inclut l'accroissement de coalitions multilatérales, on l'a vu avec ce qu'on appelle les FIVE EYES, les dialogues au niveau de la sécurité, multipartites, multilatérales, des coalitions et possiblement un OTAN de l'Asie à l'avenir. Cela peut nous permettre d'avancer et il faut qu'il y ait des investissements publics en capital humain.

Je sais que la Chine, véritablement, investit beaucoup en capital humain, avec beaucoup de professionnels de la cybersécurité, mais ils veulent continuer à faire plus. Mais aux États-Unis, je crois que nous avons des pénuries de talents au niveau de la cybersécurité et nous

devons véritablement investir en capital humain, en ingénieurs, en mathématiciens, informaticiens, sinon nous allons avoir des conséquences néfastes au niveau de la recherche et du développement. Et on va se mettre en retard, les États-Unis vont prendre du retard par rapport à la Chine.

Nous devons faire plus au niveau du chiffrement, au niveau de la protection informatique, et se préparer avec les meilleurs talents et limiter les crises nationales, comme nous l'avons vu avec cette pandémie. Nous devons absolument nous assurer que nous sommes les leaders technologiques du monde.

Voilà, à l'écran, mes références et les citations que j'ai empruntées. J'ai fini cette présentation, merci de l'avoir écoutée, sur cette tendance mondiale et merci donc d'avoir pris le temps de m'écouter. Si vous avez des questions, n'hésitez pas à me les poser maintenant.

DÉBORAH ESCALERA: Merci beaucoup. Il y a une question de Brian sur le chat, qui s'adresse à tous d'ailleurs, mais étant donné que vous venez d'intervenir, je vais vous la poser : que pensez-vous de la liberté d'expression sur internet pendant la pandémie de Covid 19 ?

JAMES PAEK: Brian, merci de cette question. Je ne suis pas bien sûr d'avoir compris la question. Est-ce que vous pourriez peut-être me l'expliquer un peu mieux ?

DÉBORAH ESCALERA: Est-ce que vous avez des précisions Brian à apporter par rapport à cette question ?

JAMES PAEK: Écoutez, je ne sais pas quoi faire, est-ce que j'attends ou est-ce que je réponds en fonction de ce que j'ai compris de la question ?

DÉBORAH ESCALERA: Vous pouvez répondre tel que vous avez compris la question. Il nous reste encore 10 minutes.

JAMES PAEK: Écoutez, Brian, oui, ça peut vouloir dire beaucoup de choses cette question posée. Mais si on pense à la liberté d'expression des gens sur l'internet pendant la Covid 19, comme je l'ai dit dans la présentation, il y a beaucoup de cas dont je vous ai parlé, en Chine, en Belarus, en Russie montrent bien qu'aux États-Unis il y a encore beaucoup de travail à faire au niveau de la liberté d'expression. Et on l'a vu dans un cas récent, en 2014, c'est un exemple où les gouvernements ont mis en danger énormément d'informations et de données. Et, pour l'heure, comme je l'ai dit, on voit des comportements autoritaristes émerger de plus en plus, une détérioration des principes mêmes de la démocratie.

On l'a vu dans la région Afrique avec un rapport qui a été fait sur plusieurs régions en Afrique et il faut s'assurer que le gouvernement n'ait pas la possibilité de contrôler quel que type que ce soit

d'informations sur internet, parce que ce qui va se produire c'est qu'il va y avoir des conséquences néfastes, c'est-à-dire que le gouvernement va commencer à vous contrôler en fonction de vos comportements, des données dont il dispose. Et donc c'est quelque chose qui me préoccupe et le gouvernement ne devrait pas avoir le droit de vous contrôler ou de vous censurer en fonction des risques que vous pouvez présenter. Il faut s'assurer que vous avez votre liberté d'expression intacte, indemne, et il faut s'assurer que le gouvernement ne puisse pas intervenir, s'immiscer dans votre vie privée.

Et, ce qu'on a vu au cours de ces dernières années, y compris ce qu'on a vu en Corée du Nord et en Chine, c'est bien ça. Est-ce qu'on veut voir cela se produire dans d'autres pays du monde ? Je ne le pense pas. Parce que c'est une intrusion de la vie privée.

La liberté d'expression, les libertés civiles en seraient toutes bafouées.

Je vois beaucoup de pays qui ont des tendances autoritaires et je crois qu'il faut s'en préoccuper et il faut préserver la liberté d'expression et tous les droits civils qui sont les nôtres, parce que si on ne le fait pas, on a tendance à partir du principe que c'est quelque chose d'acquis et, tout d'un coup, on le perd et on ne s'en rend pas compte.

Donc il faut s'assurer qu'on renforce l'éducation, qu'on renforce la confiance du public vis-à-vis des institutions. C'est ce qui se passe actuellement et c'est particulièrement important aux États-Unis et partout dans le monde, il faut s'assurer que nous écoutons de manière active les autres, les points de vue différents, c'est pourquoi je parlais de l'importance d'accroitre la civilité, parce que ça, ça va au-delà de

l'autoritarisme numérique. Il s'agit simplement d'être respectueux, tolérant vis-à-vis des autres et de respecter les opinions différentes de la sienne.

DÉBORAH ESCALERA: Merci James. Je crois que Brian a précisé sa question sur le chat. Il ne nous reste plus que quelques minutes, donc je vais vous la lire, mais je vais vous demander d'être très bref pour répondre à sa question. Il dit : vous avez dit que les gouvernements contrôlent la liberté d'expression des gens sur internet de manière plus grave qu'auparavant. Pensez-vous que c'est une bonne évolution du monde démocratique ?

Et vous avez deux minutes pour répondre à cette précision de Brian.

JAMES PAEK: Oui, comme je vous l'ai dit, il faut investir dans le capital. Il faut investir donc dans l'être humain pour nous assurer que nous avons les capacités nécessaires pour répondre à cela. Si ce n'est pas le cas, on va devoir faire face aux conséquences néfastes de cela.

Il faut promouvoir les démocraties et ça, ça commence d'abord par le fait que les États-Unis montrent l'exemple pour que les autres pays suivent.

Ne pensez pas, évidemment, que la démocratie ce soit la meilleure chose au monde, je ne dis pas que ça n'est pas une bonne chose, mais je dis qu'il faut l'améliorer, la démocratie.

Et il faut, à n'en pas douter, accroitre le niveau de confiance du public vis-à-vis des institutions pour nous assurer aussi qu'on augmente le niveau de civilité chez nous, pour montrer l'exemple encore une fois.

DÉBORAH ESCALERA: Merci, je crois qu'il y a une autre question, je vais vous donner une minute pour y répondre et je vais vous rappeler de parler lentement. Enoch, quelle est votre question ?

ENOCH NIKINGBOUNG DUUT : ça n'est pas une question, c'est un commentaire. Je pense qu'il est très important de prendre note du fait qu'un certain nombre de gouvernements ont tiré parti de la situation de la Covid 19. Certains ont confisqué certains droits ou ont volé des informations et ont profité de ces informations pour retirer des droits aux gens.

Et certaines de ces lois n'ont pas fait avancer les choses, parce qu'il y avait énormément de mésinformation et désinformations pendant la Covid 19.

Mais ces lois ne vont pas prendre fin avec la fin de la Covid 19. Donc, on l'a vu pendant la Covid 19, les gouvernements ont profité de cette situation pour retirer des droits et des libertés aux gens. Et ça, c'est quelque chose qu'il ne faut pas perdre de vue.

Merci.

DÉBORAH ESCALERA: Merci de votre commentaire. Sur ce, nous allons clore cette séance d'aujourd'hui. Je vous remercie tous d'avoir participé aujourd'hui à cette réunion, merci à Siranush d'avoir projeté les présentations, merci aux présentateurs de votre excellent travail aujourd'hui. Excellentes thématiques, excellent travail de présentation.

Merci à l'équipe de réunion, merci aux interprètes et merci à tous ceux qui ont participé à notre réunion de NextGen. Nous sommes très heureux que vous nous accompagniez.

Et, à l'attention des NextGen, profitez bien de l'ICANN 72, on a plein d'activités intéressantes cette semaine, je sais que ça peut être un petit peu impressionnant d'écouter autant d'acronymes, c'est beaucoup pour une première fois, mais vous allez passer un bon moment.

L'enregistrement est terminé.

[FIN DE LA TRANSCRIPTION]