FR

ICANN85 Mumbai | Forum de la communauté – De la stabilité à la survie : rôle de l’ICANN dans l’avenir de la résilience de l’Internet
Lundi 9 mars 2026 – 10h45 à 12h00 IST

KATHY SCHNITT

Je suis chargée de la participation à cette séance. Cette séance est régie par les normes de comportement attendues de l'ICANN et les politiques anti-harcèlement de la communauté de l'ICANN.

L'interprétariat est fourni en anglais, français, chinois, arabe, russe et hindi. Veuillez suivre les lignes de conduite prescrites pour cette séance. Je les afficherais aussi dans le chat.

Il y a trois façons de poser des questions. Si vous êtes en personne, veuillez vous rendre au microphone. Si vous êtes à distance, veuillez soumettre vos questions en ligne. Je lirai les questions ou vous pouvez donc lever la main. S'il vous plaît, levez la main virtuelle en bas de votre écran et attendez d'être appelé à prendre part à la parole.

Que vous soyez sur place ou à distance, lorsque vous prendrez la parole, indiquez votre nom, la langue dans laquelle vous parlerez si ce n'est pas l'anglais et exprimez-vous à un débit raisonnable. Je donne maintenant la parole à Ram Mohan.

RAM MOHAN

Merci. Bonjour à cette séance plénière. Je m'appelle Ram Mohan et je suis donc le président du comité consultatif Stabilité et sécurité. Dans les rues de Mumbai, vous voyez donc l'illustration de ce qu'est la résilience ici. Donc nous ne sommes pas une ville verte, mais nous avons une capacité incroyable à surmonter les obstacles. L'Internet n'est pas très différent aujourd'hui. La résilience consiste à savoir si les paquets atteignent leur destination. Il faut savoir si le système de confiance qui achemine ces paquets peut survivre.

Il ne s'agit pas simplement d'une histoire de technologie, il s'agit de l'histoire des dépendances cachées, le cloud, les règlements mondiaux sur lesquels nous nous appuyons. Donc, à travers le monde, nous avons cette connectivité accrue. Il est important donc de comprendre les vulnérabilités qui peuvent avoir un impact.

La résilience, c'est la capacité de maintenir une source de vérité unique, même quand le monde semble fragmenté. Aujourd'hui, nous ne sommes pas ici pour parler de politique. Nous sommes ici pour parler des questions techniques, des protocoles, de la stabilité, de l'infrastructure et opérationnel.

Nous souhaitons parler du fait que les systèmes sur lesquels s'appuie la population mondiale pour les communications, le commerce, les services publics, la sécurité, si ces systèmes peuvent continuer de fonctionner en cas de défaillance, en cas de crise géopolitique ou en cas d'attaques sophistiquées.

J'ai avec moi un panel d'éminents intervenants et avant de procéder, je voudrais dire que nous allons utiliser le Mentimeter

tout au long de cette séance. Et ce que vous voyez à l'écran est un QR code. Quand vous verrez le QR code, veuillez prendre votre téléphone. Veuillez le flasher, flashez le QR code et vous verrez des questions.

Nous souhaitons avoir votre point de vue sur ces questions. Et donc vos retours seront partagés avec vous au fur et à mesure. Fiona et moi sommes rejoints par cinq panélistes, Danny McPherson, qui dirige l'organisation de sécurité et de technologie à VeriSign, et il a participé activement à une recherche et une standardisation de l'Internet depuis les années 90. Il a occupé différentes fonctions dans le domaine de l'ingénierie de l'Internet. Il a rédigé plusieurs ouvrages sur les protocoles internet notamment.

Nous sommes rejoints aussi par Bruce Tonkin qui est le responsable de l'administration de .au, AUDA. Donc avant d'occuper ces fonctions, il a occupé des fonctions pendant 18 ans dans le domaine de l'administration. Il a aussi été au conseil d'administration de l'ICANN et il a été responsable donc de DNSO.

Donc nous sommes aussi rejoints par M. Singh, M.A.K.P. Singh. Il est responsable au sein de CyberPeace et ancien membre d'une équipe gouvernementale sur la sécurité de l'information en Inde. Donc, il a été jusqu'à sa retraite, responsable de la transition énergétique et de la cybersécurité, et il a dirigé la transition vers les énergies non fossiles.

Nous sommes aussi rejoints par Dan York. Il est responsable à l'ISOC. Il dirige le développement du noyau sécuritaire de l'Internet

et il est à l'IETF un membre de L'équipe qui s'occupe de la sécurité. Il est en ligne depuis les années 80. Il est auteur de nombreux ouvrages sur les réseaux, la sécurité et Linux. Donc, en tant que membre de l'ISOC depuis 2011, il a travaillé à diverses initiatives, notamment la résilience de l'Internet, les défaillances de l'Internet IPv6.

Nous avons aussi Paul Vixie. Il a conçu, mis en œuvre et déployé plusieurs extensions et les applications qui sont utilisées sur Internet actuellement, les mises à jour dynamiques, les réputations et aussi les logiciels code source ouvert. Il est ancien membre du SSAC et il est actuellement membre du RSSAC. Fiona, veuillez vous présenter, s'il vous plaît.

FIONA ALEXANDER Bonjour. Donc j'ai occupé plusieurs fonctions et je suis heureuse de me joindre à vous de Washington DC.

RAM MOHAN Merci. Donc le DNS, IPv4, BGP occupent une grande place. Il y a de grandes transformations; cependant, nous observons donc des perturbations de l'Internet causées par des pannes de systèmes externes tels que les réseaux électriques, les chaînes d'approvisionnement de logiciels.

Le problème n'est pas la fragilité de l'Internet. Le problème semble une fragilité environnementale. Nous sommes à un tournant. L'axe de concentration aujourd'hui n'est pas de vous donner un tutoriel

sur le fonctionnement de l'Internet. Nous n'allons pas débattre des statuts constitutifs ou des mandats de l'ICANN, mais nous allons parler de ce qui se passe lorsqu'il y a une défaillance des systèmes fondamentaux de l'Internet et que faire dans ces cas. Fiona.

FIONA ALEXANDER

Merci. Je voudrais vous donner un contexte avant de poursuivre cette conversation. Un bon nombre d'entre nous, y compris Ram et Danny, sont impliqués dans les travaux qui sont signalés dans le rapport de la société Marconi.

Il y a eu donc énormément d'ateliers qui ont été aussi proposés pour savoir ce que nous pouvons faire pour faire de la résilience un sujet majeur.

En novembre, il y a eu le point culminant d'un travail de longue haleine, en novembre 2025. Donc, nous nous sommes appuyés sur le travail qui avait été fait par une équipe de l'Académie des sciences de Washington, et nous avons donc utilisé les travaux dans lesquels Ram avait été impliqué sur la résilience de l'Internet. Et nous savons que les dirigeants s'inspirent de nos travaux.

La résilience doit être traitée comme étant un problème majeur et non pas donc quelque chose que l'on envisage après coup. Il y a plusieurs thèmes qui ont été dégagés par le SAC132, qui a été publié en septembre 2025. Nous avons quatre thèmes que nous allons aborder.

Tout d'abord donc les pannes des réseaux électriques et ce que cela veut dire pour l'Internet. Donc la cascade des pannes du nuage et les pannes, les défaillances des API et aussi ce que cela implique pour le DNS.

Nous allons donc donner la parole aux différents panélistes, et nous allons demander à chacun de s'exprimer pendant trois minutes au maximum.

DANNY MCPHERSON Bonjour, nous allons parler de l'infrastructure fondamentale de l'Internet, les protocoles fondamentaux qui permettent donc à l'Internet de fonctionner, notamment le DNS, qui permettent la navigation à travers le monde, ils sont particulièrement robustes, même face à l'instabilité. Ils n'ont pas été conçus avec à l'esprit les questions sécuritaires, mais ils ont été conçus en s'appuyant sur la confiance qui règne.

L'Internet a énormément évolué et ces protocoles continuent d'être évolutifs, avec comme optique la question sécuritaire et les protections relatives à l'intégrité. Il s'agit aussi d'élargir les domaines de services qui doivent être fiables. Il y a davantage de complexité et quand il y a davantage de complexité, il y a davantage de risques.

Il y a donc des mécanismes qui sont parfois des paradoxes. Ces renforcements sécuritaires doivent pouvoir protéger contre des défaillances et des problèmes majeurs.

Les protocoles fondamentaux ont pour but de minimiser les risques liés aux dépendances. Il y a des dépendances systémiques et elles sont critiques. Il faut des gardes fous, des zones tampons afin que le système puisse absorber des chocs plutôt que de se comporter en cascade.

Quand on parle de stabilité, on se demande : Qu'est-ce qui compte? Où est-ce que l'on trouve cela? Comment est-ce que cela peut fonctionner. Qu'est-ce que cela? Qu'est-ce qu'il faut pour pouvoir contrôler, pour atténuer?

KATHY SCHNITT S'il vous plaît Danny, veuillez ralentir un peu pour les interprètes.

DANNY MCPHERSON Alors on se demande ce que l'on peut faire soi-même. Donc les opérations DNS doivent souligner les transports, les substrats de transport. Cela inclut les RPKI. Cela comprend tout ce qui est équipement informatique, les services, les universités, la résilience des systèmes. Et donc il s'agit là des systèmes de contrôle, encore une fois. Il faut soutenir ces systèmes de contrôle pour avoir accès au réseau et avoir contrôle sur la sécurité.

Pour avoir une bonne pratique pour les hyperscalers, les CDN, c'est qu'il faut avoir une bonne dépendance, il faut faire confiance aux logiciels, aux protocoles, etc. Cela a un impact, bien sûr sur le côté robuste du contrôle. Il faut comprendre les services technologiques, il faut comprendre aussi les impacts et les

responsabilités. Il faut considérer tous ces éléments pour pouvoir atténuer les problèmes de manière appropriée. Voilà, c'est tout pour moi.

FIONA ALEXANDER Paul Vixie, allez-y. Vous avez trois minutes. Paul, vous êtes là en ligne.

PAUL VIXIE Vous m'entendez bien?

RAM MOHAN On ne vous entend pas très bien. Rapprochez-vous de votre micro.

PAUL VIXIE Très bien, je vais faire ce que je peux. Alors je voulais parler un peu de la chaîne d'approvisionnement des logiciels. L'Internet n'avait pu être créée que grâce à des dépendances. Pour résumer, des logiciels, des protocoles qui ont été créés un peu partout par beaucoup de personnes, toutes ces personnes qui étaient intéressées et qui voulaient savoir comment les choses fonctionnaient.

Ils n'avaient pas à considérer tous les éléments quand on construisait ou qu'on développait des logiciels ou des choses qui pouvaient être téléchargées, on s'attendait à ce que ça fonctionnait. On n'était pas motivés par les mêmes choses. Ce que cela voulait dire, c'est que cette affaire de dépendances de parties

non contractantes, ça reste en place aujourd'hui. C'est encore une question.

Il y a des bugs dans les logiciels, il y a toujours des bugs, mais on s'attend toujours à ce que ces logiciels auront toujours des bugs. Donc quand vous téléchargez un logiciel open source, vous téléchargez quelque chose sur votre téléphone. Vous savez très bien qu'il y aura des bugs et on ne les connaît pas tous, mais les patchs arrivent.

Chacun et chacune d'entre nous a un smartphone et on s'attend tous de voir du trajet de milliers de gigabytes par semaine. Et on espère que ces logiciels recevront des patchs pour réparer les problèmes. On n'aurait pas pu arriver à cette étape, enfin du moins pour expliquer à tout le monde, enfin je veux dire pour que toutes les personnes comme nous qui sommes intéressés par ces problèmes, on doit se dire qu'on doit trouver une manière de régler les choses qui soit meilleure. Il faut que les créateurs de logiciels comprennent les nouveaux défauts de leur travail et apprennent à les réparer.

Donc on se demande si c'est lié à la sécurité. On se dit par exemple est-ce que ces choses vont endommager? Est-ce que ça va nuire? Est-ce que toutes ces choses-là vont nuire à d'autres personnes, etc. Donc il faut pouvoir passer ces logiciels avant que les attaquants ne mettent mainmise sur cela. Il faut demander à ces personnes qui développent des logiciels de publier leurs travaux et donc il faut qu'ils soient motivés par la sécurité.

Donc, il nous faut trouver des solutions créatives, mais on ne le fait pas parce qu'il y a ce côté non contractant. On n'a pas une liste de qui utilise les logiciels. Donc ces logiciels peuvent propager d'une manière indirecte des problèmes d'autres applications ou d'autres créateurs d'applications, etc. Ça inclut beaucoup d'éléments. Donc en attendant, on ne sait pas qui ils sont, mais on connaît, on sait quels sont les clients. Non, on ne sait même pas quels sont les clients en aval.

Donc, si vous dépendez de logiciels open source, je ne parle même pas d'applications sur les smartphones. Je ne parle même pas des choses que l'on met sur nos ordinateurs portables. Mais donc, lorsqu'on compte sur ces logiciels, on a besoin de pouvoir compter sur l'entreprise qui a développé le logiciel.

RAM MOHAN

Pour les personnes qui sont dans cette salle, veuillez utiliser votre téléphone. Scannez le code QR qui est à l'écran pour répondre au sondage. Donc, c'est ce qu'on appelle le Mentimeter. Donc, nous allons passer la parole à M. Singh qui est notre troisième intervenant.

SHRI M. A. K. P. SINGH

Bonjour, je suis M. Singh. Je viens du secteur de l'électricité. Je vais me concentrer sur les infrastructures nationales. Nous avons besoin de générateurs pour gérer le réseau de l'électricité.

Chez nous, le réseau d'électricité, c'est très important. Nous avons sept secteurs en Inde. Aux États-Unis, il y en a 16. Si les secteurs électriques échouent, cela pose des problèmes à tout le monde. Il y aura des black-out qui surviendront très rapidement.

Je vous donne l'exemple du black-out en 2003, aux États-Unis et au Canada. C'était un black-out qui a été gérable, mais ça cascadait sur toute la région nord-est des États-Unis. Ça posait un problème à toutes les tours, à tous les systèmes, et il y a eu beaucoup de coupures.

Alors, c'est ce qui se passe bien sûr, quand il n'y a pas d'électricité. On a vu beaucoup d'exemples comme celui-ci. Alors, il y a un impact sur le réseau. Et donc il y a un problème d'infrastructure, il y a un problème sur les tours. Ces tours ont des batteries qui comportent 2 ou 3 heures d'énergie.

Alors si cela dure plus longtemps, si l'électricité ou l'énergie ne revient pas de suite, cela ne dure pas longtemps. Il n'y a pas aussi de refroidissement. Donc, il y a des coupures d'urgence qui rentrent en jeu. Et donc cela représente des coupures d'Internet, des coupures de cloud. Et donc quand il y a un collapse comme ça, un échec logistique, tout échoue. Il y a des coupures.

KATHY SCHNITT Veuillez ralentir, M. Singh, pour les interprètes.

SHRI M. A. K. P. SINGH

Comme vous le savez, en Ukraine, quand il y a une attaque cyber, les attaquants ont créé un DDoS sur les lignes fixes. Donc ce genre d'impact peut apporter des problèmes physiques sur les réseaux. En 2012, il y a eu un black-out dans notre pays en Inde. Donc on a demandé à ce que toutes les installations soient atteintes, toutes les installations du secteur de l'énergie. Les satellites nous ont permis de restaurer ou de coordonner la restauration du réseau. D'un autre côté, quand il y a des coupures, en général, il y a des coupures d'énergie, d'électricité et on se rend compte vraiment sur les modes de communication pour contrôler et pour communiquer, bien sûr.

Lorsqu'Il y a des coupures comme ça, cela nuit à tout le réseau.

Donc, dans ce sens, nous avons beaucoup d'équipements qui fonctionnent grâce à l'Internet, même si ce n'est pas l'Internet public, mais cela peut être toutes sortes d'équipements qui sont gérés par l'Internet des objets, etc. Il y a plein de choses qui dépendent de l'Internet public. Et alors les opérateurs du réseau énergie aussi comptent sur l'Internet.

Nous faisons un suivi très, très détaillé de tous ces équipements, ces installations, mais nous ne pouvons pas opérer à distance au niveau du réseau. Et ça, c'est vraiment un problème. Cela, c'est la cause la plus importante de coupure d'énergie lorsqu'il y a une coupure de réseau, un échec de réseau. Alors par exemple, en 2003, pour le black-out, il y a eu une coupure au niveau régional qui a créé une crise, qui s'est élargie à 50 millions de personnes.

Alors, cela, il faut bien sûr mettre en œuvre des systèmes de résilience pour tout ce qui est communication d'Internet, pour que l'énergie, pour qu'il y ait de l'électricité, que lorsqu'il y a d'électricité, toutes les autres installations qui dépendent de cette électricité vont continuer à fonctionner.

Donc, aujourd'hui, dans le secteur de l'énergie, où on sait que tous les équipements sont déjà legacy, et donc elles ont été conçues il y a 35 ans. Cela pose un problème de cybersécurité, car nous avons beaucoup de ces systèmes qui sont anciens et qui n'adoptent pas la nouvelle technologie. Donc, tout cela est lié.

On ne peut pas opérer ce réseau à l'aveugle. Donc il nous faut nous concentrer sur la sécurité pour qu'il y ait de la sécurité sur le réseau. Il nous faut de l'énergie, il faut que l'électricité fonctionne. Voilà.

FIONA ALEXANDER

Merci M. Singh. Je pense que nous avons notre prochain intervenant, Bruce Tonkin. Bruce.

BRUCE TONKIN

Oui. Je travaille pour .au en Australie. Alors, quand on parle du DNS, quand on parle de ça, c'est un petit peu comme parler d'une compagnie aérienne nationale. Ça a un impact sur l'économie nationale et sur le marché, sur le commerce international. Bien sûr, quand on parle de cela, c'est exactement comme les ressources critiques telles que l'eau, l'électricité, etc. Il y avait une tendance dans certains pays comme l'Australie, pour créer des lois, pour

gouverner ces systèmes de la même manière que les lois qui avaient été créées pour protéger les réseaux électriques, etc. Donc à .au, on nous demande une approche complète.

Alors, cela comprend quatre domaines. La sécurité de l'information, on en parle beaucoup durant ces réunions de l'ICANN, mais aussi on parle. Il y a les risques au niveau du personnel. Alors cela peut être un acteur malveillant qui attaque les infrastructures, cela peut être une erreur humaine aussi. Donc la chaîne d'approvisionnement comporte des risques aussi, voire des risques. Et des risques sont parfois physiques, ce sont parfois des désastres naturels. Alors que ces désastres soient naturels tels que des incendies, des tremblements de terre, des ouragans, des choses comme ça ou des pandémies ou bien sûr, ils peuvent être le résultat d'actes d'humains comme des guerres, des attaques d'organisations criminelles, etc. Donc, toutes ces choses ont un effet sur toutes ces infrastructures critiques.

Donc, il ne s'agit pas seulement de problèmes d'électricité ou du DNS. Ça a un impact sur les deux en même temps. Donc, il y a une prise de conscience de ces dépendances entre ces industries des ressources critiques et du DNS. Donc, quand il s'agit de l'énergie ou du secteur de l'énergie, elles dépendent aussi des services web. Quand il y a un échec d'un côté, et bien voilà les deux échouent. Il y a des coupures des deux côtés. Nous, nous utilisons des logiciels communs et nous avons fait des recherches là-dessus il y a très peu de temps sur cela.

On a vu que ces infrastructures critiques avaient été impactées en même temps, en général. Donc, nous avons examiné la chaîne de la chaîne d'approvisionnement en général pour étudier justement ces dépendances, pour nous assurer que nous ayons une infrastructure qui soit résiliente et qui soit diversifiée. Donc, en attendant, on ne peut vraiment pas prédire ce qui va se produire. Donc, il faut deviner un petit peu, il faut s'entraîner, si vous voulez, il faut faire des essais et il faut faire des essais avec tous les éléments qui sont les composantes de la chaîne d'approvisionnement. La parole est à vous, Fiona.

FIONA ALEXANDER Merci Bruce.

DAN YORK Bonjour. Donc, il est important pour nous de parler de la résilience. Je dirais dans un sens un peu différent. Donc pensez à un camion qui traverse un pays où il pourra fournir une formation sur l'utilisation de l'Internet.

Mais imaginez une femme qui a une petite entreprise, et après avoir suivi une formation a pu augmenter son revenu. La présence en ligne de ces acteurs a pu avoir un impact positif sur leur situation économique.

Il y a des témoignages à travers le monde qui peuvent être témoin de ces réussites. Il y a donc ces possibilités de changer des vies. Les

revenus augmentent. Voilà la raison pour laquelle nous devons parler de résilience ici, à l'ICANN.

L'ICANN joue un rôle critique pour assurer la résilience et la continuité de l'activité de l'écosystème. Donc, quand on regarde l'écosystème des DNS et les autres identificateurs dans les différentes régions, y compris en Afrique, les scores sont de 30 à 40.

Quand l'Internet est défaillant dans un pays, il n'y a pas seulement les services qui sont perturbés. Il y a aussi le fait que cela a un impact sur la subsistance de nombreuses personnes. Et donc, quand les infrastructures publiques sont numérisées de façon accrue, la dépendance sur Internet est accrue.

Aussi, il faut appréhender la résilience humaine, les interdépendances. Il y a donc des lieux dans le monde entier où nous pouvons tirer des enseignements. Nous devons tirer des enseignements auprès des économies émergentes. Lorsqu'il y a des pannes Internet, nous devons étudier ce qui se passe.

Il y a quelques années, j'ai vu donc ce qui s'est passé à Porto Rico. 90 % de l'infrastructure a été touchée, 95 % de l'infrastructure. Donc, j'ai demandé pourquoi. J'ai demandé ce qui a maintenu le fonctionnement. Eh bien, ce qu'on m'a dit, c'est que les gens ne dépendent pas du réseau électrique, car ils savent qu'il y aura des pannes et ils ont recours à leurs propres dispositifs, notamment des panneaux solaires ou leur propre batterie, pour faire en sorte que leur routeur continue de fonctionner en cas de perturbation.

Il y a énormément de choses auxquelles nous devons réfléchir. Il y a 2,2 milliards de personnes qui ne sont pas en ligne. Et donc parfois, cela veut dire qu'il n'est pas facile de convaincre nos interlocuteurs de se concentrer sur la continuité de la continuité de la connectivité en cas de perturbation. Donc j'ai hâte de poursuivre la discussion.

FIONA ALEXANDER Merci Dan. La parole est à Ram.

RAM MOHAN Merci Fiona. Nous avons donc trois thèmes pour nos exports. Démontrer que la complexité du système est importante. Les dépendances circulaires et les risques pour la chaîne d'approvisionnement. Et enfin, le rôle de l'ICANN dans la résilience de l'Internet. Pour entamer notre discussion, voyons un peu l'échelle de notre système.

L'Internet n'est pas simplement une collection de routeurs et de câbles. C'est un réseau massif d'API, de services de nuages et d'autres fournisseurs de services. Que se passe-t-il lorsque cette complexité rend difficile la gestion de tout cela? Donc, les applications modernes dépendent de 30 à 40 API. À quel stade la complexité elle-même devient une menace? Et qui est responsable de la gérer? Qui souhaite prendre cette question?

SHRI M. A. K. P. SINGH

Je répondrai à cette question. M. Ram, lorsque nous parlons donc de cette quantité d'API et de fournisseurs tiers, il y a donc un problème qui se profile pour trouver des solutions. Il faut parfois naviguer à vue. Il y a énormément d'API qui intègrent nos systèmes et cela a un impact sur la chaîne d'approvisionnement. Nous ne sommes pas forcément en mesure de régler tous les problèmes qui surviennent.

Donc, en 2024, il y a eu un crash majeur au niveau de Windows lorsque les correctifs n'ont pas pu être déployés et les services n'ont pas pu être dans le cas de la compagnie aérienne qui a été impactée. Donc, les cartes d'embarquement n'ont pas pu être émises. Il nous faut moins de dépendance sur les API et sur les fournisseurs tiers.

RAM MOHAN

Merci. Paul, est-ce que vous êtes d'accord ou en désaccord avec ce que M. Singh vient de dire? Si vous êtes en train de parler, nous ne vous entendons pas. Nous vous entendons maintenant.

PAUL VIXIE

Je voudrais ajouter que la complexité a un rôle dans les systèmes numériques. Et donc c'est la même chose que la chaleur dans les systèmes physiques. Plus on monte en échelle, plus nous devons suivre la règle du grand nombre. Nous devons faire des suppositions.

RAM MOHAN

Merci. Bruce, est-ce que vous avez un avis à ce sujet? Pas à ce stade. Très bien.

Eh bien, maintenant, je vais poser la question suivante. Les hyperscalers ont les ressources et les opérations pour effectuer des tests dans les cas de scénarios de défaillance. Que se passe-t-il dans le contexte d'un écosystème lorsque les petits opérateurs n'ont pas ces capacités?

DANNY MCPHERSON

Ce que j'ai vu donc avec CrowdStrike est quelque chose qui ne me convainc pas forcément. Je ne suis pas convaincu que les capacités soient réelles pour régler les problèmes qui peuvent se poser en cas de panne.

Je pense qu'avec les petites structures qui ont moins de ressources, les capacités manquent. Mais il appartient à chacun d'élaborer des pratiques qui peuvent les aider à apporter des solutions, le cas échéant.

RAM MOHAN

Merci Danny. Dan, vous avez été observateur et vous avez mesuré la résilience de l'Internet. Vous avez un point de vue. Donc, ces scénarios de panne, quels sont les scénarios de panne qui vous inquiètent le plus? Donc vous allez dans une direction différente, d'ailleurs.

DAN YORK

Donc au sein de l'Internet, il y a toujours le maillon faible qui aura un impact sur les capacités de résilience. Ce qui me tient éveillé la nuit, c'est la capacité des organisations au niveau local de reprendre l'activité. Il y a toutes ces dépendances et ce que vous avez dit au début, Ram, il faut avoir une approche holistique sur toutes les interconnexions. Quelle est la chaîne d'approvisionnement? Quel est l'approvisionnement en électricité? Quelle est la chaîne d'approvisionnement? Quel est le routage? Quels sont les systèmes de paiement?

Comment faire évoluer l'expertise au niveau local? Comment avoir une meilleure expertise au niveau local et la développer? Comment avoir une infrastructure de pair à pair? Donc, le renforcement des capacités, c'est aussi important que les protocoles. Il faut donc voir que les communautés qui sont bien formées ont la capacité de reprendre leurs activités beaucoup plus rapidement.

C'est comme disait Danny, il faut identifier et partager les meilleures pratiques et il faut faire en sorte que sur le terrain, il y ait des gens qui sachent comment bâtir, réparer, corriger les structures qui doivent être réparées.

RAM MOHAN

Merci Dan. Carlos, y a-t-il des résultats du premier sondage Mentimeter. Le Mentimeter demandait quelle est sera la prochaine cause d'une perturbation majeure, de la prochaine perturbation mondiale majeure? On attend donc la réponse de Carlos.

Et en attendant, je voudrais poser une question supplémentaire à cet éminent panel. Nous parlons de résilience et nous disons que la résilience est un problème de prévention et que la prévention n'attire pas l'argent. Donc Bruce, qui, dans cet écosystème sur la résilience, contrôle les budgets. Que faudrait-il faire pour changer ce calcul? Donc, comment nous allons allouer le budget à la prévention et ne pas allouer le budget à l'atténuation?

BRUCE TONKIN Oui, en fait, c'est quelque chose dont il faut parler. Il nous faut parler des risques. Nous savons qu'il y a de l'argent qui est disponible, des fonds sont disponibles. Donc, quand il s'agit de résilience, il faut vraiment, vraiment articuler et expliquer les risques. Qu'est-ce qui va se passer et pourquoi? Et puis il faut allouer des fonds additionnels pour cela.

RAM MOHAN Merci Bruce.

SHRI M. A. K. P. SINGH Est-ce que je peux rajouter quelque chose? La plupart du temps, lorsqu'on demande des fonds pour la sécurité cyber et pour la résilience, le conseil m'en pose toujours beaucoup de questions. Le département des finances pose beaucoup de questions aussi.

Donc lorsqu'il y a des incidents, par exemple lorsqu'il y a eu des problèmes avec Jaguar Land Rover, cette entreprise Jaguar Land Rover a demandé l'aide du gouvernement. Souvent, ces

entreprises ont besoin de se rendre compte à ce moment-là qu'ils ont besoin de faire ce qui est nécessaire pour être résilient. Donc, avant d'être réactif, il faut être proactif. Il faut s'assurer d'avoir des mécanismes en place pour justement prévenir les risques, les problèmes.

RAM MOHAN

Carlos, je pense que vous afficherez les résultats lorsque vous serez prêt. Donc, si nous acceptons que la complexité dépasse nos budgets de prévention, nous devons examiner où se trouve réellement cette complexité. Et de plus en plus, les maillons faibles sont les systèmes invisibles qui se trouvent entièrement en dehors de nos propres réseaux. Donc, il nous faut examiner notre prochain thème. Il s'agit des dépendances circulaires et les risques liés à la chaîne d'approvisionnement.

FIONA ALEXA

Merci Ram. Alors, comme vous l'avez dit, il faut parler de ces dépendances circulaires qui sont réelles. Il faut travailler dans cet environnement. Il faut voir comment les réseaux électriques sont gérés et qui sont, bien sûr, dépendants des réseaux Internet. Donc, il faut étudier les risques posés par les logiciels.

Donc, vous savez, lorsque nous avons eu la panne d'électricité qui a touché la péninsule ibérique en 2025, cela nous a montré que les pannes d'électricité entraînent des pannes d'Internet qui, à leur tour, entraînent des pannes d'électricité. Quelle est votre question

là-dessus? Le secteur de l'énergie est conscient qu'il y a un problème avec Internet.

SHRI M. A. K. P. SINGH

Oui, en fait, il y a eu des millions de personnes qui ont été impactés par cette panne d'électricité de la péninsule ibérique en 2025. Le problème venait de l'énergie renouvelable parce que tout le monde est relié au réseau principal. Lorsqu'il y a des coupures, on ne peut pas stabiliser. Quand on parle de mettre en place des capacités d'énergies renouvelables, on sait qu'il va y avoir des échecs tel que celui-ci. Donc, il va nous falloir mettre en œuvre, nous assurer que notre infrastructure numérique soit plus sécurisée et dans ce cas, ces systèmes autonomes ont posé des problèmes dès qu'il y a eu des coupures d'électricité. Mais dans des cas comme ce problème qui a touché la péninsule ibérique, au Portugal, il y a eu 90 % de coupures et en Espagne, un peu moins car ils avaient plus de capacité. Donc, ces coupures d'électricité demandent des approvisionnements de back-up.

Si vous avez le backup, les infrastructures continuent à fonctionner et dans ce cas-là, si vos infrastructures fonctionnent, vous allez pouvoir restaurer l'électricité, les systèmes d'électricité et ce sont les leçons apprises de ce problème. Nous avons déjà vu que beaucoup d'instruments, beaucoup d'équipements, beaucoup de systèmes demandent un montant minimum d'énergie. Donc les batteries, les niveaux de batterie doivent toujours être à 75 % pour que les réseaux s'arrêtent et reprennent et repartent pour restaurer

donc la chaîne d'approvisionnement. Voilà. Donc c'est pour cela que l'on met en place des infrastructures adéquates.

FIONA ALEXANDER

Alors merci. Pour les ccTLD, des opérateurs de ccTLD, comment est-ce que ces opérateurs ccTLD se trouvent à un carrefour critique entre la politique de l'ICANN et les infrastructures nationales? Dans quelle mesure les opérateurs de registre sont-ils exposés à des risques liés à la chaîne d'approvisionnement qu'ils ne peuvent même pas voir alors?

BRUCE TONKIN

Oui, donc il faut avoir un réseau qui serait conçu et qu'on travaille avec les vendeurs clés, ces vendeurs qui fournissent ce genre de système. Alors une des questions de laquelle on parlait tout à l'heure, c'est ce côté complexe.

Ce que j'ai observé, moi, c'est que dans toutes les organisations, il y a toujours une ou deux personnes qui comprennent vraiment ces éléments complexes. Si l'on parle à une de ces personnes, ou alors si elles ne sont pas disponibles parce que parfois elles ne sont pas disponibles, si vous ne pouvez pas vous rentrer en contact avec ces personnes, c'est un problème. Et donc il n'y a pas de back-up de capacité dans ce sens.

Donc, le point clé pour les infrastructures ou les chaînes d'approvisionnement, ces systèmes doivent avoir les bonnes personnes et ils doivent vraiment mettre en place un plan de

gestion de risques. Ces organisations devraient vous fournir des copies des audits qui sont faits par des services externes, des parties tierces. Et donc ces personnes doivent travailler avec vous, mettre en œuvre des exercices de cybersécurité pour bien comprendre ce qu'il y a au sein de leur chaîne d'approvisionnement.

FIONA ALEXANDER

Merci Bruce. Alors on voit très bien qu'on est vulnérable dans tous les secteurs, même si tout est bien configuré dans nos réseaux. On est là aujourd'hui à cette réunion de l'ICANN. Donc on doit se demander ce que l'ICANN, l'ICANN Communauté peut faire. Et voilà, ça va amener notre prochaine thématique.

RAM MOHAN

Avant de faire cela, est-ce que l'on pourrait avoir les résultats de la troisième question du sondage? Nous avons donc affiché une nouvelle question. Donc, encore une fois, les gens qui peuvent scanner ce code QR devraient le faire et répondre à cette question. La question que vous voyez à l'écran, c'est que si votre vendeur régional ou votre réseau électrique échouait pendant 72 h, comment avez-vous confiance au service de base?

Alors, on va revenir vers l'ICANN. On sait qu'on ne peut pas résoudre les problèmes du réseau électrique du monde. On ne peut pas résoudre tous les problèmes géopolitiques mondiaux non plus. Mais nous, ensemble, nous sommes les superviseurs de l'Internet

et le système d'identifiants uniques. Alors, quelle est l'intersection entre le mandat ou la mission de l'ICANN avec la fragilité environnementale que l'on observe très clairement dans le monde autour de nous? Que doit-on faire pour que les systèmes tels que les API ou le DNSSEC, pour qu'ils soient élargis, pour qu'il y ait moins de perturbations?

DANNY MCPHERSON Alors je pense que le DNS est assez robuste d'un côté, opérationnel. Je pense que c'est encore plus robuste du côté cache, du côté des échecs. Il y a plein d'éléments dans les infrastructures qui permettent d'opérer ces systèmes de façon adéquate.

Vous savez, quand on regarde les opérations des bureaux d'enregistrement, que ces systèmes sont inférieurs à ceux qui fonctionnent très bien. Il y a eu bien sûr des échecs du DNSSEC.

Mais il y a aussi des cas où il y a des échecs RKPI et qui ont un impact sur le DNS. Parce que bien sûr, cela dépend du routage. Donc, on ne peut pas toujours réparer le RKPI quand il y a un problème de DNS, parce que le RKPI dépend du DNS. Donc, c'est la raison pour laquelle les opérateurs ont mis en œuvre des systèmes de contrôle pour mettre en place des barrières ou des sauvegardes ou d'autres systèmes de contrôle. Et donc ça leur permet d'atténuer les risques et d'atténuer les attaques sécuritaires.

Donc, je pense que, en général, qu'on voit bien sûr que les RKPI dépendent du DNS et du routage. Les dépendances circulaires

posent des problèmes. Quand on essaie de concevoir des plans de reprise ou de résistance à ces échecs, cela pose beaucoup de problèmes, et donc il faut fournir quand même un certain niveau de service, pouvoir faire faire un suivi et mettre en place un bon contrôle sur ces opérations.

RAM MOHAN

Donc les économies en voie de développement sont les plus exposées quand il y a des échecs au niveau du système. Donc je vais poser la question à Dan : Quels sont les coûts humains dont on ne parle pas? On n'en parle pas suffisamment.

DAN YORK

Les coûts humains. Mais nous, on ne va pas changer le monde. Quand on observe la société civile, le secteur des organisations à but non lucratif, on voit que ces gens-là sont focalisés sur les missions, mais pas forcément sur d'autres éléments tels que le côté technique, informatique, les infrastructures, etc. Alors, que ce soit une école, une bibliothèque, une organisation telles que celles-ci, ils pensent aux changements qu'ils peuvent apporter au niveau mondial.

C'est leur priorité. Alors tous ces gens-là, ces organisations sont dépendantes des systèmes qui sont fournis par des parties tierces. Donc, il faut vraiment pouvoir aider ces gens-là pour qu'ils puissent avoir une reprise, pour qu'ils puissent être résilients au niveau humain et pour qu'ils puissent résoudre leurs problèmes.

Alors dans ce sens, on se dit que peut faire l'ICANN. Je pense que l'ICANN, la communauté ICANN joue un rôle important ici. En partageant cet écosystème résilient, cela peut aider. Nous avons une communauté résiliente du DNS qui peut aider. Je pense que l'on peut faire des choses à partir de l'ICANN. On pourrait étudier ces dépendances, ces meilleures pratiques. Où est-ce que la communauté pourrait peut-être aider à l'identification d'un certain point d'échec, pour pouvoir justement identifier les meilleures pratiques à tous les niveaux, que ce soit à tous les niveaux des services, les opérateurs, etc. Et donc, si on pouvait développer ce genre de système au sein de la communauté ICANN et pouvoir faire la promotion de ces meilleures pratiques pour pouvoir partager ces informations à travers toutes les parties prenantes.

Donc il faudrait communiquer avec les ISP, avec le groupe de parties non commerciales, parler avec les organisations à but non lucratif. On pourrait donc ainsi partager ce message de nouvelles meilleures pratiques et donc communiquer avec toutes ces parties de la communauté pour construire, pour élaborer la résilience, pour continuer à opérer le DNS.

Donc, je pense qu'il y a des tas de choses que l'ICANN peut faire dans ce sens, parce que le coût humain, c'est ne pas livrer sur cette mission, ne pas faire ce qui est nécessaire pour cette mission. On parlait des économies en voie d'émergence, eh bien souvent ils sont dépendants de ces systèmes. Il nous faut élaborer une expertise au niveau national, régional, cette capacité humaine. Et

c'est comme ça que l'on rendra les choses beaucoup plus résilientes.

RAM MOHAN M. Singh, vous voulez parler rapidement, répondre rapidement sur cette question qui est liée au coût humain de la résilience?

SHRI M. A. K. P. SINGH Je vais vous donner un exemple classique à savoir quand le réseau électrique a été impacté. J'étais ce matin ici durant la cérémonie d'ouverture. On a parlé de la chaîne d'approvisionnement d'énergie à Bombay. Nous avons eu un problème dans les centres de données en Inde, à Mumbai, à Bombay. Et vous savez, en 2020, on a eu ce problème. On a eu une coupure de six heures à Bombay, et on a perdu beaucoup de données. Et je pense que ce sera la même chose à travers le monde.

Lorsqu'Il y a des perturbations telles que celles-ci, la plupart des infrastructures ne sont pas disponibles. Comme l'a dit Fiona tout à l'heure, on a parlé de la péninsule ibérique. Les personnes dans ce cas-là ne pouvaient même pas acheter des choses en ligne parce que tout était lié. Il n'y avait pas d'internet, donc il n'y avait pas de transactions bancaires, etc. Par exemple, lorsque nous voulons donner de l'aide humanitaire, on ne peut pas fournir cette aide dans ces dans ces circonstances.

Quand nos systèmes ne sont pas gérés à la bonne cadence, lorsqu'il y a des coupures telles que celle-ci, les acteurs malveillants sont

encore plus actifs. Donc, si on veut envoyer des financements, de l'aide humanitaire au Myanmar, dans ce cas-là, je me souviens, il y avait eu du spoofing et des attaques cyber lorsque les opérations avaient été faites de manière manuelle parce qu'il y avait une coupure. Donc cela peut vraiment nuire à toutes sortes de situations.

RAM MOHAN

Merci beaucoup. Nous avons le quatrième Mentimeter. Et donc, quand on regarde le paysage de la résilience de l'Internet, quel est vraiment l'angle mort pour la communauté de l'ICANN actuellement? Si vous avez des questions, veuillez vous orienter vers le microphone et pour les participants en ligne. Utilisez donc la fenêtre Questions-réponses. Il ne nous reste que peu de temps. Donc, s'il vous plaît, limitez-vous à 90 secondes. Y a-t-il des questions dans la salle?

KATHY SCHNITT

Oui. Michael Palage, veuillez activer votre micro.

MICHAEL PALAGE

Michael Palage. Merci. Vous m'entendez bien? Merci. Merci Ram. Nous avons entendu l'APNIC sur ce rôle. Donc pourquoi est-ce que le rôle critique de l'ICANN a été donc survolé? Deuxièmement, l'ICANN a un protocole d'accord avec NRO. Est-ce que du point de vue de la chaîne d'approvisionnement, cela constitue une vulnérabilité? Et enfin, quelles sont les questions liées à la

confiance entre l'ICANN et les opérateurs concernant les identificateurs uniques? Est-ce qu'un des intervenants souhaite se prononcer sur ce sujet?

RAM MOHAN

Alors Danny, est-ce que vous voulez répondre à l'une de ces trois questions?

DANNY MCPHERSON

Oui, je serai heureux de le faire. Nous avons donc passé beaucoup de temps à travailler avec trois des RIR. Nous suivons leur développement et donc les RPKI ont beaucoup d'impact sur l'infrastructure. Pour ce qui nous concerne, nous souhaitons que l'infrastructure soit robuste et sécurisée. Il est important de faire des investissements. Il faut que les personnes qui gèrent ces infrastructures soient au niveau et cela s'applique à tous les fournisseurs. Nous passons beaucoup de temps pour assurer que tout cela soit donc à un niveau optimal. Donc, nous devons faire en sorte que la capacité des RIR soit au niveau. Il faut qu'ils aient des plans en cas de défaillance.

Dans l'un des commentaires, j'ai dit qu'il y a des systèmes qui ont des relâchements et il faut que les tampons, les protections soient en place en cas de défaillance. Je pense que les RIR améliorent les capacités.

	L'état de la chaîne d'approvisionnement pour les logiciels a un impact positif sur les RPKI et il faut continuer de renforcer les capacités afin qu'elle puisse demeurer sécurisée et robuste.
RAM MOHAN	Merci Danny. Nous avons une question dans la salle. Veuillez bien vous exprimer dans le micro.
ANAND RAJE	Donc, les systèmes de services sur Internet dépendent d'infrastructures centralisées. Donc ma question porte sur l'impact de cette centralisation sur la confiance.
PAUL VIXIE	Veuillez répéter la question.
RAM MOHAN	Donc, quel est l'impact de cette architecture centralisée de confiance sur la résilience Internet régionale?
PAUL VIXIE	C'est par défaut assez préoccupant. Nous avons constaté qu'il y avait une résilience inadéquate entre certaines régions et le reste du monde, et il y avait des situations où un système ne pouvait pas entrer en connectivité avec un autre système. Ou alors il y avait aussi des questions de confiance qui se posaient.

Cela se produit par défaut. Chaque concepteur doit envisager cette problématique. Et il faut que soit effectué des tests dans des contextes où l'on simule l'hostilité.

RAM MOHAN Merci. Y a-t-il des questions en ligne?

KATHY SCHNITT Oui, il y a une question en ligne de la part de Bruce. Donc, en Australie, la cybersécurité est traitée au niveau ministériel. Est-ce que cela renforce le rôle du gouvernement dans la sécurité du DNS? Ou y a-t-il toujours cette difficulté de mise en œuvre entre les agences gouvernementales et le secteur?

BRUCE TONKIN C'est une question difficile. En Australie, du point de vue de la gouvernance, il y a des corrélations entre les différentes agences et il y a donc un département qui s'occupe des infrastructures critiques qui font l'objet de législation. Le ministère de la Cybersécurité déploie son action sur l'ensemble du secteur et non pas simplement sur les fournisseurs de services Internet. Et il s'agit de renforcer la sensibilisation auprès des petites entreprises, sensibiliser ces petites entreprises à l'importance de la cybersécurité. Et nos interactions se situent au niveau des opérateurs de registre.

RAM MOHAN Prenons une question dans le public.

IDIL KULA Je suis boursière de l'ICANN. Donc vous parlez de la résilience, de la robustesse et de la continuité des opérations de l'Internet, donc de ces infrastructures dans leur ensemble. Il s'agit donc d'un réseau d'infrastructure, d'API, de divers services et fournisseurs tiers de services de nuages.

Donc, il y a des risques liés à la chaîne d'approvisionnement à nos secteurs. Il y a le risque énergétique et il y a donc la question écologique et environnementale qui entre en jeu.

Comment est-ce que l'ICANN peut encourager toutes les parties prenantes afin qu'elles s'orientent vers des pratiques qui soient davantage pérennes et responsables? Si un acteur peut encourager les autres à adopter des pratiques davantage pérennes et responsable, cela peut être optimal.

Comment agir tous ensemble? Car si nous attendons que les gouvernements imposent les meilleures pratiques, nous serons toujours en retard et nous n'aurons pas de continuité de l'Internet.

RAM MOHAN Merci. Je vais donc poser cette question à Dan. Que peut faire l'ICANN pour aider à la résilience environnementale et écologique?

DAN YORK Combien de temps nous reste-t-il, Ram? Je crois que la question n'a pas vraiment été entendue, si vous voulez bien la répéter.

RAM MOHAN Je l'ai résumée. Que peut faire l'ICANN pour aider à la résilience écologique dans le contexte du changement climatique?

DAN YORK Merci. Je crois qu'il y a beaucoup de travail qui est fait au sein de l'écosystème. Certains des travaux portent sur la façon de gérer de façon plus verte les data center, et il y a toute une palette de choses qui sont faites pour avoir une meilleure empreinte carbone. Donc, quand on envisage l'ensemble de l'écosystème Internet, chaque acteur a la possibilité de déterminer quel est son impact sur l'empreinte écologique. Comment chacun peut agir à son propre niveau, qu'il s'agisse des registres, des bureaux d'enregistrement, des fournisseurs de services internet individuels. Il y a donc beaucoup de choses qui peuvent être faites à tous ces niveaux-là. Et donc il y a aussi peut-être ce que peut faire l'ICANN.

RAM MOHAN Carlos, est-ce que vous pouvez partager avec nous et l'auditoire le résultat du Mentimeter? Voici ce que vous pouvez dire sur la cause de la prochaine perturbation mondiale. Et voilà la prochaine question. Veuillez attendre quelques instants. Nous examinons les réponses du sondage Mentimeter. Passez à la question suivante. Donc ici, on dit que la coordination intersectorielle, c'est l'angle

mort principal de l'ICANN. C'est ce que nous indique la réponse à cette question du Mentimeter. Merci beaucoup.

Je vais maintenant passer à nos panélistes maintenant. Et je vais commencer par Bruce. Je vais donc poser mes questions aux panélistes. Si vous aviez un peu de temps pour parler au leadership de l'ICANN et cela directement, que voudriez-vous faire en premier?

BRUCE TONKIN Je pense qu'il faut faire des efforts au niveau de la chaîne d'approvisionnement pour tout ce qui est des registres des fournisseurs de DNS, pour qu'il y ait des dépendances qui soient mises en place et qu'il y ait des essais qui soient mis en œuvre pour exactement savoir quelles sont les dépendances et ce qui se passerait au cas où il y aurait des problèmes. Donc, mettre en œuvre certains scénarios de risque.

RAM MOHAN Alors, Ram, Paul, qu'en pensez-vous? Qu'est-ce qu'il faudrait que le leadership fasse après cette séance?

PAUL VIXIE Nous n'avons pas parlé des pressions au niveau réglementaires, mais je pense qu'il y a des éléments qui peuvent ressortir à n'importe quel moment. Si on va en Californie pour leur dire voilà, on a besoin de clarifications sur tel ou tel sujet, sur des choses qui

ne fonctionnent pas, y a-t-il d'autres choses qui vous intéressent comme ça on peut en parler?

Donc de toute façon, dans tout cela, il nous faut avoir beaucoup plus de partage, de communication à travers le monde et poser des questions aux personnes au niveau mondial, à tout le monde, à toutes les parties prenantes pour savoir ce qu'ils recherchent, ce qu'ils demandent de l'internet. Sinon, ce n'est pas réaliste.

SHRI M. A. K. P. SINGH — Oui, nous avons besoin de mieux comprendre comment les entités communiquent, comment elles collaborent pour apporter du soutien aux fonctions critiques, aux infrastructures critiques.

RAM MOHAN — Quelles questions poseriez-vous aux leaders de l'ICANN?

DAN YORK — Je dirais trois choses. Il faut que l'ICANN commence à penser à la résilience au niveau de sa propre infrastructure. Il faut parler de résilience technique. Comme le disait Bruce, il faut parler de la carte, il faut cartographier. Il faut donc observer toutes les dépendances cachées du DNS, du système d'identificateurs, de parler des meilleures pratiques. Comme on l'a dit plus tôt, il y a beaucoup d'organisations qui travaillent dans cet espace et l'ICANN peut collaborer avec ces genres d'organisation. Si l'ICANN

fait cela, nous allons pouvoir avoir accès à un Internet beaucoup plus résilient.

RAM MOHAN Merci Dan. Danny, allez-y.

DANNY MCPHERSON Oui. Plusieurs des éléments dont on a parlé auparavant sont déjà incorporés dans le plan stratégique de l'ICANN. Les systèmes techniques, le mandat technique de l'ICANN représentent un exemple lorsqu'il s'agit de la gestion des infrastructures, et cela se fait depuis longtemps. Je pense qu'il y a des opportunités plus larges pour que l'on puisse se concentrer sur le côté fonctionnel des systèmes. Et donc ce que l'on n'a pas dans tout cela, c'est que les entités responsables, ce sont les parties prenantes au sein de la communauté de l'ICANN ne se focalisent pas forcément sur cela, et elles ne travaillent pas avec des partenaires pour justement mettre en œuvre des exercices pour prévenir justement tous ces risques.

Je ne sais pas si l'ICANN a besoin de faire ça directement, mais encourager, cela serait une bonne chose. Et donc mettre en œuvre des prévisions, enfin apporter des informations, faire des prévisions, parler des perturbations géopolitiques qui pourraient de toute façon à déstabiliser l'ICANN en général.

Je pense qu'il y a des forces externes qu'il faut comprendre, et il faut essayer de comprendre cela au sein de la communauté de l'ICANN.

RAM MOHAN Laissez-moi poser la question aux personnes qui sont dans cette salle. Levez la main si, après cette heure que vous avez passé avec nous, est-ce que vous pensez que la résilience devrait devenir une stratégie importante ou priorisée de la part de l'ICANN? Est-ce que l'ICANN devrait prioriser cette question de la résilience? Donc, Fiona, je vous passe la parole à savoir s'il y a des commentaires, si vous avez des commentaires finaux.

FIONA ALEXANDER Je voudrais remercier toutes les personnes qui nous ont fait leur présentation, surtout pour ces personnes qui étaient en ligne. Nous avons donc pu voir que tout le monde avait un rôle. Toutes les parties avaient un rôle quand il s'agit de la résilience.

RAM MOHAN Merci à tous. Merci aux panélistes. Cette session est donc terminée. Merci.

[FIN DE LA TRANSCRIPTION]