ICANN68 | Forum de politiques virtuel – Séance plénière : le DNS et l'Internet des objets : opportunités, risques et défis
Mardi 23 juin 2020 – 13h00 à 14h30 MYT

RIA OTANES : Bienvenue à cette séance plénière sur le DNS et l'internet des objets, opportunités, risques et défis. Je suis Ria Otanes, je vais m'occuper de cette séance. Cette réunion va être enregistrée et va respecter les normes de conduite d'ICANN.

Pendant la séance les questions et les commentaires seront lus s'ils sont posés en anglais dans le secteur des questions et réponses. Vous pouvez y accéder dans les outils de Zoom.

Je lirai les questions et commentaires à haute voix lorsque le président me dira de le faire. Si vous voulez poser une question ou faire un commentaire à haute voix, levez la main, on vous donnera la parole, vous donnerez votre nom et vous direz dans quelle langue vous allez parler si vous ne parlez pas en anglais.

Cette séance inclut un service de transcription et d'interprétation. Pour la transcription, cliquez sur « close caption » dans les outils de Zoom. Pour aider les interprètes nous vous demandons de parler clairement et à une vitesse raisonnable.

Pour entendre l'interprétation vous devez télécharger l'application de l'interprétation, et vous avez davantage d'informations sur ce point dans le site.

Je vous rappelle que vous pouvez utiliser le menu déroulant dans le chat pour choisir si vous voulez que tout le monde lise votre commentaire, ou seulement un panéliste. Et vous avez cette option dans le chat.

Je vais donner maintenant la parole à Alejandra Reynoso.

ALEJANDRA REYNOSO : Merci beaucoup, merci Ria. Je suis Alejandra Reynoso, je travaille pour le ccTLD, et je suis heureuse de présider cette plénière. J'appartiens à .GT.

Donc les ccTLD essayent de rendre notre vie plus durable, plus facile, en connectant les objets entre eux dans un environnement physique. Cela rend les choses différentes si on compare aux applications internet comme l'email et autre chose. Et beaucoup utilisent le système de noms de domaine pour utiliser le service à distance dont ils ont besoin.

Le Comité de sécurité et de stabilité, le SSAC, a publié récemment un document, SAC105 qui parle des différents défis qui existent dans cette connexion. Et, aujourd'hui, au cours de cette plénière, nous allons parler davantage, notamment nous allons permettre aux

membres de la communauté, des différentes unités constitutives, de parler de ces thèmes avec les experts et d'en discuter entre eux.

Cette plénière est un suivi de la séance de ccNSO sur le SAC105 qui a eu lieu à Montréal et qui s'est focalisée sur les ccTLD.

L'objectif de cette plénière est de mieux comprendre comment l'internet des objets diffère des différentes applications d'internet interactives et traditionnelles. De mieux comprendre comment le DNS et les acteurs de l'IoT comprennent cette interaction entre leurs écosystèmes, en termes d'opportunité de risques et de défis et pour avancer dans la réflexion sur le rôle de la communauté d'ICANN.

Prochaine diapo.

Aujourd'hui, voilà notre ordre du jour. On va d'abord parler et présenter le document SAC105, ensuite nous aurons un panel d'experts qui partageront les perspectives sur ce thème. Ensuite il y aura une révision par des pairs avec des présentations d'experts. Et puis nous conclurons sur des questions et des réponses de la part du public.

Prochaine diapo.

Je vais d'abord vous présenter Cristian Hesselman qui va nous donner un petit peu une idée de ce qu'est le SAC105. Il est directeur d'un laboratoire, qui est l'équipe de recherche. Et il travaille pour .NL, aux Pays-Bas. Et il va nous parler de la sécurité et de la résilience des communications internet, des mesures qui ont été faites, des

recherches dans ce domaine, et de l'évaluation des nouveaux systèmes d'internet et des outils. Cristian est aussi membre de SSAC et il appartient au groupe de travail qui a présenté des rapports sur l'internet des objets, les opportunités, les risques, les défis et SAC105. Il est aussi professeur d'université aux Pays-Bas, et il est président de NETLAB.

Cristian vous avez la parole.

CRISTIAN HESSELMAN : Merci beaucoup Alejandra. J'ai l'honneur aujourd'hui de vous faire une petite présentation sur SAC105. Et donc c'est le rapport qui a été présenté par SSAC le 19 juin, et c'est un résumé de ce document qui porte sur l'internet des objets, le DNS et qui se focalise un petit peu sur les différentes discussions qui peuvent avoir lieu au sein de la communauté de l'ICANN.

Ce rapport va aussi apparaitre comme un document de revue de pairs, dans une revue, et cela sera publié dans quelque temps.

Donc l'internet des objets, ce que nous utilisons comme définition dans notre rapport est la définition de l'IoT qui a été présentée par ISOC aussi en 2015. Il s'agit d'une application qui permet d'étendre la connectivité des réseaux et les capacités pour les objets, les appareils, les senseurs et les objets, qui permettent donc d'être connecté à un réseau.

Les différences avec les applications traditionnelles, comme l'email ou le navigateur, voilà ces différences sont les suivantes. L'IoT a des senseurs qui interagissent avec un espace physique, c'est la différence qui existe, et puis il interprète les informations qu'il reçoit de différents senseurs pour agir sur cet espace. En général, cela se fait sans que l'utilisateur le sache. Et cela a lieu à l'intérieur de différents types d'objets qui interagissent entre eux sans qu'on le sache et sans qu'ils le sachent. C'est pour ça qu'on appelle cela une interaction passive. Ce n'est pas une interaction interactive qu'on pourrait avoir avec le navigateur, l'email, etc.

Donc il va y avoir une série d'appareils, d'IoT, qui vont surgir avec le temps. On a 20, 30 milliards d'appareils qui fonctionnent dans notre vie quotidienne sans qu'on s'en rendre compte, sans qu'on interagisse avec eux. Ils sont là.

Et aussi, la différence c'est que ces outils, ces éléments, ces appareils IoT sont beaucoup plus hétérogènes, ce ne sont pas des ordinateurs, ce sont différents types de systèmes. On parle par exemple d'appareils, on parle de différents types de connexion de réseaux, ce n'est pas seulement le Wifi, c'est aussi d'autres types de réseaux.

Et, finalement, l'IoT diffère parce que les appareils de l'IoT ont une durée de vie plus longue, parce qu'ils sont inclus dans des structures physiques et ils se caractérisent par une opération dont on n'a pas besoin de s'occuper. Ils sont là, ils travaillent, ils connectent, ils se connectent avec le réseau sans qu'on le sache ou qu'on s'en rendre compte.

Par conséquent, l'IoT est considéré comme la prochaine étape importante. C'est quelque chose qui existe depuis les années 1990 dans le domaine de l'informatique. On a donné différents noms à ce concept, mais maintenant on en est à un stade où il est possible de déployer ce type d'appareil et le résultat est que les gens pensent, ils sont convaincus même, que l'IoT va permettre d'avoir une société plus soutenable, plus durable dans le transport par exemple, dans les transports en commun, ça va nous permettre de fournir d'autres possibilités, d'avoir des maisons qui fonctionneront de manière plus intelligente, un système énergétique qui soit aussi plus intelligent avec des réseaux énergétiques différemment utilisés et qui fonctionneront différemment.

Donc il y a beaucoup de promesses dans le domaine des IoT, mais quand on parle de cela, il faut parler aussi de sécurité de l'IoT.

Donc ici, vous voyez un exemple, c'est le modèle que nous utilisons à SSAC quand on pense à l'internet des objets. Donc ici, ce que vous voyez, c'est un plan avec un espace physique sur la gauche, vous avez ces espaces physiques avec des personnes qui sont chez elles, et qui interagissent avec ce que l'on appelle le déploiement de l'Iot, c'est-à-dire ce que vous voyez en gris au milieu de l'écran. Et ce déploiement de l'IoT est constitué de différentes choses, les appareils IoT, la connectivité des réseaux et le service back-end. Voilà ici vous avez un exemple. Vous avez quelqu'un qui s'approche de la porte, quand il est près de la porte, il y a des informations qui vont être collectées concernant la proximité de cette personne, à travers sa montre, donc

il va y avoir des empreintes digitales, ces informations vont être transférées à d'autres services par internet, et on va prendre une décision pour voir si on laisse entrer cette personne ou pas, avec une politique d'utilisateurs bien sûr.

Donc ce que vous voyez ici, c'est un exemple simple, qui montre que les informations sont analysées par ce système, par la montre, par exemple, elles sont partagées sur internet, elles sont envoyées dans un service, et elles sont envoyées à la porte, à l'ouverture de porte. Donc on a ici un système qui permet d'agir sur l'environnement de l'utilisateur et cela a lieu de manière automatique, sans que l'utilisateur doive intervenir. L'utilisateur voit les appareils, il voit qu'il y a une montre intelligente, qu'il y a une porte, mais il ne voit pas toutes les machines qui sont derrière cela.

Et une partie importante de ces machines c'est le DNS, parce que l'on sait qu'il y a toute une série d'appareils qui vont interagir avec des services sur l'internet pour offrir certaines fonctions, cela est différent du navigateur traditionnel pour lequel vous allez interagir, vous allez choisir des informations, vous allez voir ce que vous voulez utiliser comme service, où est ce service. Donc cela permet à ces appareils d'offrir, de fonctionner. Ici, ça va être différent, l'appareil va prendre une décision, va décider d'ouvrir la porte ou pas à cette personne.

Donc on a ici le DNS qui joue un rôle important. Je ne vais pas parler du détail ici, parce que les autres intervenants en parleront après ma présentation.

Donc voilà, je crois que pour le moment j'en ai terminé avec cette diapo. Passons à la diapo suivante s'il vous plait.

Alors, ce rapport s'appelle donc les opportunités et les risques de l'augmentation de l'IoT. Donc je vais vous parler des opportunités sur cette diapo, et sur une autre diapo, je vous parlerai des autres aspects.

Donc à SSAC nous nous focalisons principalement sur les risques, mais dans ce cas-là nous avons pensé qu'il était intéressant aussi, et que c'était une bonne occasion de parler du DNS. Parce que c'est une structure qui demande une confiance au niveau mondial. Il va falloir augmenter la transparence, la sécurité et la protection de la vie privée sur le DNS, c'est important.

Et donc j'ai présenté ces trois points ici, et je vais vous donner davantage de détails là-dessus.

Le premier point, c'est que le DNS doit permettre à l'utilisateur d'avoir moins de risques. Parce que ces appareils dont nous venons de parler vont interagir avec le DNS, et donc les requêtes du DNS, il y a un observateur entre le passage de cet appareil IoT et le service à distance utilisé. On va voir qu'il y a une interaction entre le DNS et la personne qui est chez elle, quel type d'appareil utilise cette personne, ou peut-être si cette personne utilise un appareil et quelles sont les interactions avec le DNS.

Autre possibilité, si vous savez quel type de dispositif IoT est utilisé en regardant le nom de domaine, vous pouvez même, en tant qu'attaquant, essayer de voir quel est ce dispositif IoT qui est en train

de créer cela. Donc voilà les éléments qui montrent que beaucoup de dispositifs IoT utilisent ces noms de domaine pour faire les requêtes, comme on l'a vu sur la diapo précédente, et parfois les requêtes DNS ou les noms de domaine qui sont utilisés utilisent également des informations par rapport au dispositif utilisé. Donc voilà ce qui se cache un peu derrière ce qu'on a intitulé ici réduction des risques.

Ensuite, le chiffrement. La requête DNS génère ce genre de chose. Donc vous pouvez le voir par exemple par le DoH ou DoT dont on a beaucoup parlé.

Autre opportunité que nous avons identifiée pour atténuer les risques que les dispositifs IoT soient redirigés vers d'autres plateformes à distance, il y a ce qu'on appelle les « routes hijacks » c'est-à-dire un trafic redirigé vers un réseau malicieux. Et ça, ça pourrait avoir une incidence néfaste sur l'IoT, parce l'IoT n'est plus connecté au service auquel il est censé être connecté, mais peut être connecté à un service malicieux. Donc ça oblige à partager les données internet avec des services à distance qui, à leur tour, peuvent agir sur leur environnement à distance. Donc on pense que l'IoT et le DNS peuvent aider ici parce que grâce au DNSSEC on peut valider l'intégrité des messages qui proviennent du DNS. Et, s'il y a piratage du routage, comme je vous le disais, alors le DNS va pouvoir le détecter parce qu'ils vont voir qu'il n'y a pas de validation des messages reçus.

Autre opportunité qu'on voit ici pour les bureaux d'enregistrement de donner des authentifications à plusieurs niveaux. Par exemple, ils

peuvent protéger les noms de domaine qui sont utilisés par les dispositifs IoT de manière plus importante.

Voilà donc certaines des opportunités que l'on voit pour réduire les risques des dispositifs IoT qui soient redirigés vers des services malicieux.

Et enfin, en termes d'opportunités, pour donner un meilleur aperçu des services et des résolveurs qui sont utilisés par les dispositifs IoT, la plupart du temps les gens utilisent de dispositifs IoT, or ils ne savent pas le genre d'information qu'ils sont en train de partager avec les services de l'internet. Donc, en utilisant les requêtes DNS que les dispositifs de l'utilisateur génèrent et en les rendant visibles aux utilisateurs finaux, ça va aider à avoir un meilleur aperçu de ces interactions.

Donc dans les exemples que je vous ai donnés, vous allez voir que vous pouvez voir et partager des informations sur les services à distance de l'internet.

Diapo suivante s'il vous plait.

Donc voilà un site web, risques. Peut-être qu'il faudrait, je n'ai plus beaucoup de temps, donc je vais passer rapidement sur cette diapo. Le principal risque que l'on voit, c'est que l'IoT donne lieu à de nombreuses attaques des DDOS, donc attaques de déni de service distribué. C'est ce qu'il s'est passé en 2016 sur un opérateur DNS. Et on voit qu'il y a d'autres réseaux zombies des DDOS qui sont créés, il faut agir rapidement, et qui pourraient aussi commencer à utiliser des

résolveurs ouverts qui auraient une incidence sur le trafic DDOS et donc créer encore plus d'afflux de trafic.

Et l'autre risque c'est ce qu'on appelle les programmes non amicaux, c'est-à-dire par exemple il y a eu quelques années un exemple, une appli pour iPhone qui demandait au résolveur de supprimer leurs caches et donc des informations sensibles étaient révélées.

Diapo suivante s'il vous plait.

Donc vous voyez, on a parlé du modèle d'IoT qu'on a analysé au SSAC, les opportunités et risques identifiés. Question suivante : que devons-nous faire pour saisir ces opportunités et réduire les risques ?

Alors nous avons élaboré une série de défis pour le DNS et les industries IoT, pour faire face à cela, qui vont au-delà du champ du SSAC, donc il y a ici un rôle pour la communauté IoT d'agir.

Donc développer une bibliothèque de sécurité du DNS, pour développer les fonctions dont je viens de vous parler sur la diapo opportunités. Donc ça passe par la validation DNSSEC et soutien DoH/DoT. Également faire en sorte que les requêtes DNS soient visibles pour les utilisateurs finaux et soient attrayantes d'une certaine manière.

Ensuite, défis en termes de formation. Formation pour les experts IoT, comprendre bien quelles sont les fonctionnalités en termes de sécurité, savoir les utiliser et même chose pour les experts DNS pour qu'ils comprennent bien comment fonctionne l'IoT et peut-être se

rendre compte aussi que l'IoT va modifier la manière dont les domaines sont utilisés. Ce qui implique peut-être d'autres types de fonctions pour les opérateurs de registre de noms de domaine dans le domaine de l'IoT.

Ensuite, le principal défi serait le suivant : coopérer avec un groupe d'opérateurs DNS pour partager ce qu'on appelle les empreintes des DDOS, c'est-à-dire les attaques DDOS qui ont lieu au sein des opérateurs DDOS. Donc ils vont partager ces informations. Et les opérateurs DNS peuvent également partager leurs capacités en termes d'atténuation de risque et de menace. Et on voit un rôle également pour les réseaux périphériques, pour protéger ces réseaux vis-à-vis des attaques.

Enfin, si on est un peu idéal, ce serait une très bonne chose d'avoir un système en place évolué de l'internet des objets.

Et sur ce, j'en ai fini avec cette présentation.

ALEJANDRA REYNOSO : Merci beaucoup Cristian.

Nous allons maintenant passer la parole à nos experts. D'abord Eliot Lear, Lise Fuhr, puis Cristian.

Je vais vous présenter brièvement Eliot Lear et Lise Furh. Eliot travaille en tant qu'ingénieur à Cisco dans le domaine de la sécurité IoT en se concentrant sur la manière dont les dispositifs communiquent les uns avec les autres. Il fait partie de la Communauté Internet, et il a

travaillé à l'IETF depuis 98, ainsi qu'au board sur l'infrastructure de l'internet, et il a travaillé également à l'ICANN pendant la transition IANA. Il travaille également à l'UIT et il est basé en Suisse.

Lise Fuhr est directrice générale de l'ETNO depuis janvier 2016. Elle supervise toutes les activités de l'association. Et au nom de l'association elle est également membre du conseil d'administration de l'organisation sur la cybersécurité en Europe. Elle a été nommée au conseil d'administration de l'IETF depuis mai 2019. Elle a une expérience dans le domaine de l'ingénierie des télécommunications, innovations, où elle met en œuvre des règlementations pour le secteur des télécoms. Ensuite, elle a été à la tête de plusieurs équipes pour travailler dans le domaine des services mobiles.

Eliot, je commence par vous. C'est à vous d'intervenir.

ELIOT LEAR : Merci beaucoup. Diapo suivante.

Alors, je vais vous parler maintenant d'un four. Oui, vous le voyez à l'écran, c'est un four. Il est lié à l'IoT, à l'internet. Mon cousin en a acheté un de ce type, il l'a installé, et tout d'un coup il a été réveillé à 4 h du matin parce qu'il a reçu une notification selon laquelle il fallait qu'il nettoie le four. Donc voilà comment était paramétré ce four.

Ce que mon cousin ne savait pas c'est que pour que tout ceci fonctionne, il y avait beaucoup de composantes dans ce dispositif. Non seulement le four avait plusieurs éléments traditionnels, un

thermostat, un minuteur, bref tout ce que les autres fours ont, mais il avait aussi un CPU, une carte mémoire, et un affichage.

Et cela représente une menace. C'est-à-dire tout ce qui implique ces composantes peut faire l'objet d'une attaque. Donc, que peut-on faire face à ce genre d'attaque ?

Soit, dans le meilleur des cas, on brûle le dîner, soit on peut être réveillé à une heure très inappropriée. Et si tous les dispositifs dans la maison sont activés en même temps, alors il y a coupure d'électricité. Toutefois, s'il y a la clim, le chauffage ou la radio qui est allumée, il y en a plusieurs qui peuvent être connectés les uns aux autres. Donc il faut mettre en place une protection pour tous ces dispositifs interconnectés.

Diapo suivante s'il vous plait.

Donc pour que ce four fonctionne, il ne suffisait pas simplement – ha vous avez ici une image de l'internet, une très belle image de l'internet créée, par KC, il y a un moment maintenant… Donc diapo suivante s'il vous plait.

Donc le four parle aux autres dispositifs dans le nuage. Et il le fait de la même manière que la sonnette d'entrée le fait. Et ce sont les dispositifs en nuage qui communiquent via son appli mobile.

Pour que ces dispositifs puissent parler dans le nuage, ils sont besoin d'utiliser le DNS. Donc il y a un point de sortie, par exemple

.EXEMPLE.COM, et pour que ces dispositifs puissent communiquer il faut que l'information soit routée.

Donc, dans le cas de la sonnette d'entrée, ça passe par le Wifi, mais il y a d'autres moyens de communiquer. Mais tout cela passe par le réseau électrique de la maison.

Donc comment cela fonctionne ? On voit par exemple une requête du four – diapo suivante s'il vous plait – une requête qui dit : voilà .EXEMPLE.CLOUD. COM et reçoit une adresse IP en retour. Ensuite, il y a quelque chose qui va être adressé à un dispositif en particulier. N'oubliez pas ce qu'a dit Cristian à l'instant. Il y a environ 20 milliards de dispositifs de ce genre dans le monde. On a beaucoup de dispositifs sur internet, mais le four n'a besoin que de parler à son cloud, son .CLOUD, son .NUAGE. Il n'a pas besoin de parler à tout. Donc, ce routeur domestique peut fournir un point de contrôle et ce point de contrôle limite le niveau de menace vis-à-vis de ce four. Ce qui veut dire que même s'il y a une vulnérabilité dans le four, le point de contrôle peut le protéger de différentes attaques. Est-ce que ça veut dire pour autant que les fabricants ne devraient pas fournir un logiciel particulier pour ce four ? Probablement pas. Il continue d'y avoir une menace, même avec ce genre de protection de réseau. Mais le réseau aide à réduire les menaces.

Prochaine diapo s'il vous plait.

Donc ici vous voyez le système de communication qui va entre le nuage et l'appareil. Cela est résolu par le DNS. Et ici, cela permet de

voir la requête en réponse de l'autre. Cela signifie que si la requête du DNS est chiffrée et que le point de contrôle ne le sait pas, il ne peut pas fournir de protection, il ne peut pas réduire cette menace.

Prochaine diapo.

Et bien sûr, cela se répète avec différents objets, différents appareils. Aujourd'hui, dans le secteur industriel on essaye d'analyser cela. Nous allons voir cela du point de vue du consommateur, mais il y a différents points, différents secteurs du nuage qui sont utilisés par différents appareils, comme vous le voyez ici.

Alors, qu'est-ce que cela signifie ? Cela signifie que nous… C'est bien de chiffrer, il y a de bonnes raisons de chiffrer les requêtes du DNS. Cependant si le point contrôlé, si cela est destiné à réduire la menace, mais si cela ne peut pas avoir accès à la requête, si ce n'est pas un système autorisé, s'il n'y a pas une partie qui puisse voir la communication qui existe entre la requête et la réponse, à ce moment-là, on ne peut pas fournir la protection nécessaire, le routeur ne peut pas fournir la protection nécessaire. Donc il y a ce problème, cette contrainte entre le DNS et le routeur comme point de protection.

Je ne dis pas qu'il ne faut pas chiffrer, au contraire, je dis qu'il faut chiffrer, mais il faut s'assurer que quand on chiffre, c'est sur une composante ou un composant qui est autorisé à fournir ce service. Voilà.

Je crois que j'ai terminé et que c'est ma dernière diapositive. Alejandra ?

ALEJANDRA REYNOSO : Merci beaucoup Eliot. Nous allons maintenant donner la parole à Lise Fuhr.

LISE FUHR : Merci beaucoup. Bonjour à tous. Je vais vous offrir une autre perspective, puisque je viens du côté de [Taco] de l'ISP, et j'ai une autre vision des choses.

Donc ma présentation va porter sur l'intérêt de l'internet des objets, de la 5G, je vais aussi vous parler de ce que la 5G va nous offrir comme nouvelles opportunités. Mais je voudrais aussi aborder quelques préoccupations concernant la 5G et le DNS. Et je vous parlerai aussi de la situation, où est-ce que nous en sommes actuellement par rapport à l'internet des objets, le DNS et cela sera selon la perspective des [Talco].

Bien, donc ici, si nous parlons de l'internet des objets, qu'est-ce qui est intéressant dans cela par rapport à la 5G ? C'est parce que nous comprenons que la 5G, qui est un mélange de réseaux fixes et mobiles, ce n'est pas une nouvelle technologie, c'est quelque chose de beaucoup plus sophistiqué comme technologie. Et on voit que cela va permettre à ce qu'il y ait une grande composante de croissance dans les IoT.

Donc ici vous voyez des chiffres concernant les IoT mobiles, c'est un chiffre assez bas, mais en 2018 on avait 140 millions de mobiles qui

étaient connectés avec des systèmes d'IoT, et on attend 740 millions maintenant pour l'année 2026.

Ce type de connexion, quelles seront les nouveautés qui vont être intéressantes et qui peuvent nous intéresser dans ce domaine ?

Ça va être d'abord le bas débit d'IoT, il y aura aussi quelques machines, le faible débit, il y aura quelques machines avec des améliorations EMTC, ce sera un petit peu le nouveau développement qui va surgir dans ce domaine de la 5G.

Quand on analyse la 5 G, il va y avoir une série de services, il y a des services qui se construisent déjà, ce qui était déjà en place et qui permettent déjà l'IoT de fonctionner. Mais le nouveau système de l'IoT va être plus basé sur les infrastructures non-IP et sur les infrastructures du DNS.

Donc ce que nous voyons maintenant, ce n'est pas vraiment ce que l'on appelle l'IoT qui est plutôt un système d'IP, mais ce sera un nouveau service qui va être développé. Nous espérons que nous pourrons compter sur une nouvelle utilisation IoT 5G, comparé à ce que nous avons aujourd'hui, nous espérons que ce sera une utilisation meilleure et plus sûre.

Si on regarde les choses, comme vous le voyez ici sur cette diapo, l'IoT 5G est quelque chose qui est construit sur un portefeuille de service plus large, et le DNS - et l'IP en général - va être un système qui va fédérer tout cela ici.

Prochaine diapo.

Alors, si on regarde l'héritage de la 5G et du DNS mobile, la 5G ne va pas être une 5G qui va apparaitre du jour au lendemain. Ce qu'on voit aujourd'hui c'est qu'il y a beaucoup de réseaux 5G qui se construisent sur des réseaux ou des infrastructures 4 G. Donc ce que l'on voit c'est un mélange de 4G et de 5G, d'équipements de 4G et de 5G. Ce n'est pas un réseau 5G qui va être complètement construit.

Et l'utilisation du nom de domaine du DNS dans ce système, dans ce réseau, ce cœur de réseaux mobiles, n'est pas courante. On va utiliser beaucoup de DNS, mais cela va être limité.

Et il y a des exceptions bien sûr, liées au DNS, par exemple dans le cas du « VoLTE » quand cela s'applique, mais quelle est l'utilisation du nom de domaine pour le système mobile ? Donc on comprend que l'interdomaine est limité actuellement et que cela dérive de ID hérités et l'accès mobile à internet est non spécifique.

Donc il n'y a rien de vraiment nouveau ici, on peut dire, entre la 4 G et la 5 G par rapport au DNS, mais nous utilisons tout cela, nous utilisons la 5 G de la même manière que nous utilisions la 4G.

Prochaine diapo.

Alors, pourquoi est-ce que la 5G est intéressante et pourquoi est-ce qu'elle est encore plus intéressante que la 4G ? Et bien c'est parce que, comme je l'ai dit, c'est un réseau beaucoup plus convergent, c'est un réseau qui va utiliser beaucoup plus de logiciels et qui ne va pas

dépendre autant du matériel, il va être beaucoup plus flexible que la 4G. Et, comme nous l'avons dit, il doit être natif IP. Et donc c'est un petit peu difficile de gérer, de travailler avec l'IPv6 et les adresses IPv6 parce que l'on continue à avoir une utilisation importante du DNS, à cause des structures IPv6.

Nous constatons aussi que le système interdomaine sera IP natif, et nous allons peu à peu passer à un système interdomaine IP dans la manière de gérer notre réseau, les réseaux.

Donc en Europe, on continue à travailler de manière interconnectée, de manière interconnectée entre les réseaux mais nous pensons que peu à peu nous aurons davantage d'IP interconnectés. C'est la façon dont les choses avancent dans le domaine des réseaux 5G et de leur connexion entre eux.

Maintenant, si on analyse la façon dont le nom de domaine et son utilisation vont être matérialisés, principalement on peut dire que c'est transparent pour les utilisateurs dans le sens que c'est invisible pour les utilisateurs, ils ne voient pas comment on utilise le DNS. Par conséquent, la façon dont on travaille avec les réseaux est une approche technique, c'est un objectif principalement technique qui va être inclus dans l'appareil. Et donc on ne va pas avoir besoin de saisir un nom de domaine, et le nom de domaine ne sera pas important dans ce cadre, dans le cadre de l'IoT.

Et, à nouveau, je dirais que pour l'IoT la façon dont l'IoT a été mis en œuvre est quelque chose de très important, d'essentiel ici. Parce que

la façon dont on le met en œuvre définit les réglages, la façon dont on fait les différents réglages, quand on regarde le fait que la 5 G… Nous ne pensons pas que la 5G sera une source importante d'enregistrements de deuxième niveau. Nous pensons que cela va être défini à un autre niveau, à un niveau de sous-domaine. Donc nous ne pensons pas qu'il y aura une augmentation ici, parce que cela va être une utilisation basée plutôt sur les sous-domaines. Et, à nouveau, je dirais que beaucoup d'aspects ici ne sont pas résolus à travers l'internet, mais seront résolus à travers les systèmes interdomaines ou inter-noms de domaine.

Prochaine diapo.

Donc pourquoi pensons-nous que la 5G est positive pour l'IoT, pour le DNS ?

Premièrement parce que nous pensons qu'au niveau du cœur de réseaux nous allons avoir beaucoup plus de logiciels et cela va permettre d'avoir beaucoup plus de flexibilités de facilités entre la machine, la communication avec la machine, nous allons pouvoir définir le travail de manière beaucoup plus aisée.

Au niveau de la sécurité, le fait d'utiliser le système de « slicing » ou de couper des tranches de réseau, cela va nous permettre de travailler dans des parties de réseaux dans lesquels nous allons pouvoir définir des utilisations spécifiques. Par exemple nous aurons un système d'IoT qui va avoir besoin de peu de largeur de bande, donc un faible

débit, ce qui va nous donner un type de service pour des systèmes automatisés.

La même chose pour l'utilisation de l'intelligence artificielle, nous allons pouvoir utiliser nos réseaux de manière différente, ce qui va nous permettre de constater s'il y a des menaces ou des problèmes par rapport à nos réseaux.

Nous pensons que l'intelligence artificielle nous permet de travailler de manière beaucoup plus rapide et de trouver beaucoup plus rapidement les problèmes qui peuvent surgir dans les réseaux.

Donc revenons aux défis. Prochaine diapo.

Si l'on regarde un petit peu ce que nous considérons comme des défis, et la façon dont nous pouvons relever et atténuer ces défis, nous pensons que le système de « slicing » des réseaux est très bon. On pensait que ça allait créer une fragmentation de l'internet, mais on constate qu'il n'y a pas de problème dans ce domaine. Pas du tout. Nous pensons que cela… On avait peur, il y avait certaines craintes, mais on se rend compte que c'est un service ciblé pour les utilisateurs finaux, et que cela ne va pas donner lieu à une fragmentation de l'internet.

Si on regarde les noms de domaine et la collision de noms, on utilise les domaines publics et on constate que cela n'est pas un problème et qu'il n'y a pas vraiment de problème. Les domaines que nous utilisons dans notre travail quotidien sont des domaines publics qui ne vont pas donner lieu à des collisions ici.

Alors, du côté du DNSSEC, ça c'est un aspect important, effectivement, ça représente une opportunité, ça n'est pas une norme contraignante pour l'instant par rapport à l'IoT. Nous n'avons pas vu de choses qui seraient susceptibles de faire en sorte que les DNSSEC soient contraignants en termes de réseaux 5G, mais il est utilisé.

Et, par rapport au déni de service, et aux attaques DDOS, bien sûr on peut faire face, mais il y a une tendance de chiffrement, et si on veut s'assurer de pouvoir faire face à ces attaques, il faut pouvoir voir le trafic.

Donc, par rapport au déni de service, si l'on veut prendre activement part à cette défense, il faut pouvoir, je le répète, voir le trafic.

Diapo suivante s'il vous plait.

Donc, à partir de là, dans quel sens pouvons-nous avancer ? Il y a beaucoup de questions ouvertes par rapport à la normalisation dans ce domaine. Comme je viens de le dire, nous n'avons pas beaucoup vu de velléité de normalisation, donc ce qu'on voit pour l'instant c'est des composantes 4 G.

L'infrastructure est onéreuse, donc, d'après moi, 5G ça n'est pas pour demain, parce que ça n'est pas encore une réalité, et ce genre de réseau est extrêmement onéreux.

Dernière chose, nous avons vu la crise de la Covid 19, qui a été terrible, qui nous a tous affectés. On a également vu que dans le monde il y avait une forte focalisation sur le besoin de numériser, sur un désir de

sécurité aussi. Et de ce point de vue, nous avons vu qu'il y a eu une prise de conscience croissante du fait que l'infrastructure est importante, que la sécurité est importante, et aussi, on a observé une utilisation renforcée de notre réseau.

Donc dans l'avenir, il y aura moins de déplacements, on voit un excellent exemple aujourd'hui du fait que personne ne s'est rendu à la conférence de l'ICANN puisque c'est une conférence virtuelle.

Et par rapport à l'IoT, nous pensons aussi que ce sera – et ce sera le résultat de cette crise – cela va créer plus de surveillance à distance et plus d'IoT.

Voilà, j'en ai fini avec cette présentation. Merci.

ALEJANDRA REYNOSO : Merci beaucoup Lise. Et nous allons maintenant céder la parole à Cristian.

CRISTIAN HESSELMAN : Oui, merci. Alors, je change de casquette. Avant je portais ma casquette SSAC, maintenant je porte ma casquette .NL.

Donc c'est le registre des Pays-Bas, petit pays en Europe. Et la semaine dernière nous avons atteint le record de 6 millions de noms de domaine, donc on a beaucoup fêté cela, en ligne bien sûr.

Mais l'une des choses importantes que nous faisons, ou plutôt l'une de nos fonctions importantes, c'est d'améliorer la résilience et la sécurité

de l'internet, comme vous pouvez le voir sur la diapo. C'est pourquoi il y a quelques années nous avons décidé de travailler sur l'IoT, en particulier pour faire face à certains des défis dont je vous ai parlé auparavant, lorsque je vous ai parlé des opportunités, risques et défis dans la présentation précédente.

Et pourquoi nous l'avons fait ? Diapo suivante s'il vous plait.

C'est parce qu'il y a eu une attaque qui a eu lieu en 2016, donc attaque par réseau zombie qui a envoyé beaucoup de trafic, donc infecté des centaines de milliers de dispositifs IoT. Et, résultat, mise hors de fonctionnement de beaucoup d'applications comme Spotify et autres.

Donc on a vu l'impact sur l'internet, c'est pourquoi on a voulu agir. Et on a voulu commencer à développer un prototype « SPIN », que l'on appelle SPIN selon son acronyme. Et l'objectif de ce système, c'est de surveiller. Donc vous placez un dispositif dans votre réseau domestique, avec des fonctionnalités supplémentaires en termes de sécurité, et ces fonctionnalités vont faire que vous pouvez surveiller votre réseau, en termes de trafic DDOS. Donc vous avez un dispositif IoT à la maison qui est affecté par un réseau zombie par exemple, et vous allez participer à toutes ces attaques. Donc ce qu'on a essayé de faire c'est, de manière temporaire, déconnecter ce dispositif de l'internet pour protéger l'infrastructure internet des attaques DDOS.

Donc c'est un petit peu prendre les choses à l'envers si vous voulez.

Donc ça c'est un exemple de choses que nous avons développées au SIDN. On en est à une étape de prototypes pour l'instant, et nous

avons investi dans ce logiciel pour l'amener à un niveau de production puisque ce que nous voulons c'est aider les fournisseurs de services internet et les consommateurs, utilisateurs, à pouvoir acheter ce genre de fonctionnalité pour les installer sur leurs dispositifs.

Mais les choses se sont avérées beaucoup plus difficiles que prévu, parce que l'écosystème est bien différent de l'écosystème DNS traditionnel et c'est également un autre environnement commercial. Par exemple, les fournisseurs de services internet auxquels on s'est adressé nous ont parlé de savoir jusqu'où ils étaient prêts à aller pour fournir ce genre de service à leurs clients. Et ça, ça peut signifier des coûts supplémentaires.

C'est pourquoi le déploiement de ce genre de système est difficile. Autre argument, les fabricants informent leurs clients, donc fournisseurs de services internet de ce genre de choses.

Donc nous savons que c'est un problème parce que, si vous regardez en Europe, l'organe de règlementation néerlandais des télécommunications, il y a une initiative aussi au niveau européen entre autorités de règlementation des télécommunications. Donc il y a une directive en place qui stipule que tout dispositif qui fait de la transmission radio ait certaines conditions requises en termes de sécurité DNS.

Donc, on le voit, il y a beaucoup de choses à faire dans ce secteur, en particulier dans le secteur fournisseurs de service internet, ou secteur connectivité.

Diapo suivante s'il vous plait.

Donc le logiciel que je viens de vous montrer, l'URL se trouve ici. Autre exemple, avec le même prototype que nous avons élaboré, c'est la transparence accrue de l'IoT. Vous vous souvenez, auparavant je vous ai parlé de l'opportunité pour le DNS de visualiser les requêtes DNS pour l'utilisateur. Donc nous avons développé un prototype pour illustrer cela. Vous le voyez à l'écran. Vous voyez en gris, les cercles gris, ce sont les dispositifs sur le réseau. En haut, je pense que c'est le téléphone portable parce qu'il a beaucoup de dispositifs. Et en bleu et vert, ce sont les services à distance auxquels ces dispositifs sont connectés.

Donc ça c'est un aperçu rapide, mais vous voyez les interactions entre les différents services en temps réel. Donc ça, c'est fondé sur l'analyse des requêtes DNS. Et je dois ajouter que le SPIN est vu comme une solution facile puisqu'elle permet de mesurer et d'analyser tous les dispositifs domestiques, donc il n'y a pas d'échanges, dans le nuage, ni rien.

Donc voilà quelques exemples de systèmes qui nous permettent d'essayer de faire face aux menaces et aux risques par rapport au DNS, dont il est question dans le rapport SSAC.

Et, dernier exemple que je voulais vous montrer, l'ISOC il y a quelques années a parlé de sécurité de collaboration, donc travailler tous ensemble pour sécuriser l'internet. Et ça, c'est essentiel pour l'internet, parce que l'internet c'est finalement une grande

collaboration entre tous, donc il faut qu'on soit tous dans le même bateau.

Ce que vous voyez ici, c'est le centre d'échanges DDOS, c'est un système centralisé qui permet aux gens de partager certains des résultats des menaces DDOS dont ils ont été victimes sur leur système. Et, avec le trafic, ils génèrent une empreinte, empreinte qu'ils partagent avec d'autres opérateurs dans ce groupe, pour que les autres opérateurs sachent que ce genre d'attaque s'est produit et qu'ils puissent préparer leurs infrastructures respectives pour faire face à une menace de ce type éventuelle.

Donc ici il s'agit d'être proactif. Pour la personne qui en a fait les frais c'est trop tard, mais pour les autres qui font partie de ce groupe, c'est intéressant parce qu'ils ont plus d'informations sur les attaques DDOS qui ont touché d'autres fournisseurs.

Donc voilà le niveau de sécurité que vous avez, qui s'ajoute à l'infrastructure existante. Donc il ne s'agit pas de remplacer les autres couches, c'est une couche supplémentaire.

C'est quelque chose que nous mettons en place à titre d'activité pilote aux Pays-Bas. Donc il y a plus de DDOS.ORG, ni rien, c'est un nouveau lien. Donc je vous le disais, c'est un projet pilote aux Pays-Bas, dans le cadre d'un projet de plus grande ampleur au niveau européen qui s'appelle CONCORDIA.

Donc nous organisons actuellement un centre d'échanges au niveau national. Ce qui veut dire que les membres qui font partie de notre

organisation aux Pays-Bas, les opérateurs de registre et autres, peuvent échanger. Mais vous pouvez l'organiser d'une autre manière, avec un centre d'échanges pour l'industrie DNS, les opérateurs DNS qui peuvent partager des informations par rapport aux attaques DNS.

Bien donc voilà, je vous ai livré trois exemples que je voulais partager avec vous, pour partager avec vous l'exemple et l'expérience de .NL concernant les opportunités et défis qui se posent.

Merci.

ALEJANDRA REYNOSO : Merci beaucoup Cristian. Diapo suivante s'il vous plait.

Nous allons maintenant passer à la révision des pairs, avec Philippe Fouquart, représentant de l'ISPCP. Philippe est expert sénior dans le nommage, adressage au réseau de laboratoires. Il est à la tête des activités intelligence artificielle et apporte un soutien au sein de ce groupe de par le monde.

Rafik Dammak est ingénieur, et il a vécu au Japon après la fin de ses études à Tokyo. Il a participé aux questions de gouvernance et sociétés de l'information ici à l'ICANN. Il se concentre maintenant sur les processus d'élaboration de politique et il a participé à différents groupes de travail, unité constitutive non commerciale, NCUC et NCSG. Et il fait de la sensibilisation sur la question de la gouvernance dans sa région.

Kimberly KC Klaffy est directrice du centre d'analyses appliquées à l'université de Californie, à San Diego. En 2015, elle a reçu le prix Jonathan B. Postel. En 2019 elle est également professeur au département informatique de cette université. Elle travaille sur le rooting, possibilité de l'infrastructure internet et politique, elle a collaboré à différents rapports SSAC depuis 2003.

C'est à vous. Si vous voulez Philippe, vous avez la parole.

PHILIPPE FOUQUART : Merci Alejandra, est-ce que vous m'entendez ?

ALEJANDRA REYNOSO : Oui, on vous entend.

PHILIPPE FOUQUART : Merci, merci à tous nos panélistes. Je voudrais vous présenter ici quelques conclusions de mon point de vue.

L'introduction faite par Eliot, qui montrait que l'IoT est un appareil qui fonctionne sur des réseaux, c'est un argument pour avoir un système chez soi, avec un IoT, et quelque chose qui permette de répondre aux requêtes du DNS tout en prenant certaines précautions au niveau de la sécurité.

Ensuite, on a fait une différence entre les deux dimensions qu'on utilise, entre les types de réseau, les réseaux IoT pour l'internet des objets, les services application d'IoT fournis pas un opérateur. Et vous

avez dit que le système de découpage permettait d'avoir une architecture différente pour le DNS, par rapport à celle qui est utilisée dans les réseaux classiques et que cela était donc différent. Il y a quelque chose d'intéressant ici.

Puis Cristian a discuté, a abordé le concept de la passerelle et du système de SPIN, et tout cela est pour combattre les attaques de DDOS. Donc voilà.

C'est un petit peu les conclusions que je pourrais tirer de ce qui a été dit. Un commentaire ou une question de ma part concernant les défis.

L'IoT est complexe, parce que cela dépend des personnes qui sont responsables de définir des normes par exemple. Quelles recommandations proposez-vous ? Quelles pratiques ? Quels protocoles en général dans le domaine du DNS en particulier, pour éviter ce type de problèmes de sécurité. Et comment est-ce que vous abordez ces difficultés ?

Peut-être on peut demander à nos panélistes de nous en parler un petit peu, de nous expliquer où est-ce qu'on en est au niveau de l'écosystème, au niveau de l'industrie, où est-ce qu'ils en sont, où est-ce qu'ils sont situés et comment on peut rentrer en contact avec la communauté qui fabrique, la communauté de fabricants d'appareils électroniques aujourd'hui, pour mieux s'assurer que ces systèmes fonctionneront correctement.

ALEJANDRA REYNOSO : Merci Philippe. Je vais demander aux experts de prendre la parole. Est-ce que Rafik, vous voulez prendre la parole maintenant et poser une question ?

RAFIK DAMMAK : Merci Alejandra. Je remercie les panélistes aussi pour leurs présentations. J'ai quelques conclusions auxquelles je suis parvenu, et je voudrais les exposer.

Je pense qu'un message important est qu'il y a apparemment des points qui ne dépendent pas d'ICANN, mais comme le DNS est concerné ici, que l'écosystème peut fournir un système d'IoT, ça nous concerne, ça nous intéresse. Mais j'ai constaté qu'on en parle de la façon que les différents acteurs de l'IoT entrent dans cet écosystème et jouent un rôle dans cet écosystème. Et qu'est-ce qu'ils peuvent faire pour améliorer la sécurité ? Cela a été dit, mais je n'ai pas très bien compris quel était le rôle de l'utilisateur ici.

Ce n'est peut-être pas aussi clair que cela, mais qu'est-ce qu'on peut attendre des utilisateurs, quel type de sensibilisation doit être fait au niveau des utilisateurs, concernant les technologies qui peuvent avoir un impact sur les utilisateurs justement. Et, par rapport à l'IoT, il y a donc des points qui sont importants pour les consommateurs.

Cristian nous a parlé de la façon dont on peut utiliser, je le dirais comme ça – je ne sais pas si c'est exactement cela – le DNS et quelles sont les meilleures pratiques en ce sens.

Et je me demande, vu l'expérience au sein d'ICANN lorsqu'on a commencé à travailler avec les nouveaux gTLD, avec les noms de domaine internationalisés, on a parlé de l'acceptation universelle, comment est-ce que cela peut être utile ou approprié pour les personnes qui étudient tout ce domaine ? Quelle serait la meilleure approche à avoir pour aider à diffuser des meilleures pratiques, une meilleure utilisation du DNS dans le contexte de l'internet des objets.

Alors je me demande si Cristian, qui a beaucoup d'expérience dans ce sens, s'il peut répondre et nous expliquer un petit peu, puisqu'il travaille à .NL et peut nous dire s'il y a des points dans lesquels on peut tirer des conclusions par rapport à leur expérience aux Pays-Bas.

Je pense que ça a été très utile d'entendre parler de l'IoG, de la 5 G, de la relation entre la 5 G et l'internet des objets, et peut-être qu'on pourrait en savoir plus sur la façon dont le DNS est utilisé dans ce domaine. Et peut-être essayer de nous expliquer un petit peu les politiques qui existent et dont il faut tenir compte concernant la 5G.

Voilà, ce serait tout de ma part. Merci.

ALEJANDRA REYNOSO : Merci Rafik. Nous allons donner la parole au reste des auditeurs, c'est-à-dire maintenant nous allons donner la parole à KC.

KC CLAFFY : Je remercie vraiment les présentateurs pour leur travail, c'était très intéressant. Ils ont fait du bon travail sur le DNS.

Et je serais curieuse de savoir, que se passe-t-il au niveau du soutien du gouvernement pour ce type d'activité ? Parce que j'ai travaillé dans ce domaine pendant des années, et je pense qu'il faut parfois aider le secteur des fabricants à savoir comment se situer dans ce domaine.

Donc il peut y avoir une confrontation et avec une difficulté à tenir compte des problèmes de sécurité, des menaces. On a constaté cela à plusieurs reprises, après ça demande beaucoup d'énergie de créer des appareils qui tiennent compte des protocoles, des systèmes de sécurité ou qui existent. Et très souvent ces systèmes ne sont pas vraiment inclus et appliqués.

Donc on a essayé de proposer des pratiques, dans certains espaces, et pour justement tenir compte de ces aspects de sécurité, il y a un code de conduite dans le domaine des fournisseurs internet pour réduire les attaques, pour augmenter la sécurité de ces types de réseaux.

Je voudrais qu'on nous parle un petit peu de la façon dont on pourrait faire quelque chose, un travail de ce type dans le domaine des IoT pour créer et appliquer ce type de protocole. Et je serais curieuse de savoir s'il y a quelque chose qui est fait dans ce domaine.

Voilà, merci. Et vous avez fait du très bon travail. Je vais mettre mes questions dans le chat.

ALEJANDRA REYNOSO : Merci beaucoup KC. Alors qui veut prendre la parole en premier ? Eliot ? Allez-y Eliot.

ELIOT LEAR : D'abord, les auditeurs ont bien compris, ont bien mis le doigt sur certains points importants, il y a eu une bonne conversation dans le chat aussi je trouve, avec de bonnes discussions dans le chat.

KC a tout à fait raison. On a beaucoup travaillé sur les défis de la sécurité et il y a différentes instances, une par exemple qui tient compte de la gestion de l'internet des objets, de la cybersécurité. Il y a une recommandation SP1800-15 qui analyse les attaques dans ce type de système IoT, avec des descriptions des fabricants.

Une question ici qui est importante est le fait que l'IoT est quelque chose de très large, de flou, on se focalise beaucoup sur le consommateur. Il y a aussi le fabricant. Il y a aussi les services de santé, et d'autres. Il faut reconnaitre que beaucoup de ces protocoles sont déjà profondément règlementés.

Je vais vous donner un exemple. Le FTI règlemente tout ce qui concerne les appareils du secteur médical. Ils sont donc règlementés. Ils ont quelque chose à dire, ils ont leur mot à dire concernant la sécurité de ces appareils.

Et c'est la même chose pour d'autres infrastructures critiques importantes. Par exemple dans le secteur industriel, pardon dans le secteur nucléaire. Alors quelles sont les meilleures pratiques, les règlementations qui sont nécessaires dans certains secteurs où on va utiliser ce type d'appareil, avec un secteur très règlementé qui utilise ce type d'appareil.

Voilà, merci.

ALEJANDRA REYNOSO : Merci Eliot.

LISE FUHR : Merci. Je suis ravie de prendre la suite. Je vais répondre à Philippe, la question portant sur les différents acteurs.

Je pense le rapport de SSAC est un très bon exemple de la façon dont on peut contacter les fabricants, les gouvernements, les utilisateurs, et discuter des meilleures pratiques et de la façon dont on peut rendre les choses plus sûres, ces appareils et les réseaux.

Donc je pense que ce dialogue entre ICANN, SSAC, en Europe est un dialogue important. Et donc cette rencontre, cet échange doit avoir lieu. Et je pense que c'est ce que nous faisons en Europe.

Je répondrais à Rafik en lui disant qu'il y a des politiques dans ce domaine concernant le DNS sur la 5G, il y a beaucoup de politiques concernant la sécurité et la 5G. En Europe, actuellement, nous avons une nouvelle loi relative à la sécurité et à la 5G, cette règlementation, cette loi, n'est pas spécifique à la 5 G, mais je pense qu'on se focalise sur le DNS, sur l'IoT et sur la sécurité dans ces domaines.

Et puis on a ce qu'on appelle une boite à outils de la 5G, c'est quelque chose qui était un outil important, une règlementation qui analyse aussi différents aspects de l'utilisation du DNS.

Et à KC, concernant les difficultés à surmonter certains problèmes de sécurité, elle a raison, c'est un domaine dans lequel on a des changements constants. Et concernant la façon dont on affronte les problèmes de sécurité, parce que la technologie évolue très vite, change rapidement, en Europe on a ANISA, qui est un organe de sécurité qui travaille avec la Commission européenne, et ils ont établi un système de groupe de sécurité avec toutes les parties prenantes qui doivent parler de normes liées à la sécurité.

Et je suis sûre que des domaines comme l'IoT et le DNS vont faire partie de leurs discussions.

Merci.

ALEJANDRA REYNOSO : Merci Lise. Oui ?

CRISTIAN HESSELMAN : Oui, je voulais répondre à ce qu'a dit Rafik sur le rôle de l'utilisateur, si vous le permettez. Effectivement, les utilisateurs sont une partie importante de cette équation, ça c'est une évidence. Et je pense que d'une manière ou d'une autre, il faut habiliter les utilisateurs afin qu'ils comprennent mieux les tenants et les aboutissants de l'IoT, qu'ils sachent ce à quoi ils sont confrontés lorsqu'ils utilisent l'IoT. Et savoir que les informations personnelles qu'ils partagent avec des services à distance de l'internet, ce que cela implique.

Ça, ça fait partie d'une discussion, d'une demande des clients en termes de sécurité de l'internet, et là le DNS a un rôle à jouer.

Et je pense aussi que de ce point de vue, les gouvernements, les politiques ont un rôle à jouer aussi à ce niveau-là. On voit que c'est déjà le cas, aux Pays-Bas par exemple, l'organe de règlementation des télécommunications néerlandais agit à ce niveau-là et il y a une activité aussi par rapport aux équipements radio – dont je vous ai parlé auparavant.

Donc, en fin de compte, ça revient à des politiques, aux gouvernements, aux entités comme l'ICANN par exemple, qui puisse fixer une norme comme seuil minimum de sécurité qui devrait s'appliquer dans le domaine de l'IoT.

ALEJANDRA REYNOSO : Merci beaucoup Cristian. Merci à tous.

Nous allons maintenant passer aux questions qui ont été posées dans l'onglet « Q&A », donc questions/réponses. Nous n'allons pas lire les commentaires ou questions posées sur le chat, mais uniquement sur l'onglet questions/réponse.

Donc Ria, est-ce que vous voulez nous les lire ?

RIA OTANES : Oui, Alejandra, nous avons une question de Angie Matlapeng : est-ce qu'il y a peut-être des questions liées à la mémoire qui ont été

présentées par rapport à l'IoT pour protéger les dispositifs et qui pourraient utiliser le DNSSEC ou le chiffrement ?

ELIOT LEAR : Peut-être que je peux y répondre. Merci de cette question Angie. L'IoT présente un certain nombre de défis en termes de chiffrement et d'utilisation de la mémoire.

Le premier de ces défis, c'est que bien entendu quand on parle de dispositifs d'utilisateurs et de petits dispositifs en particulier, la mémoire a un rôle prépondérant. Par exemple, 80bytes. Et ensuite, avec des dispositifs spécialisés, où il y a des fonctionnalités de chiffrement extrêmement optimum, là, la mémoire a un rôle aussi. Par exemple 14 kilobytes, pour vous donner un petit peu une idée de la fourchette.

Donc ces défis, comme Cristian l'a dit auparavant, dans son introduction, ont une durée de vie très longue. Et le rôle du chiffrement change au fil des ans. Ce qui, d'après nous, était acceptable du point de vue du chiffrement il y a 5 ou 10 ans, est aujourd'hui susceptible d'être victime d'une attaque.

Et il y a des plateformes où vous avez un dispositif qui est là depuis 40 ans. Et imaginez ou plutôt souvenez-vous de ce qu'on avait il y a 40 ans en termes de technologie. Et maintenant, imaginez-vous en train de mettre à jour ce dispositif pour utiliser les nouvelles technologies sur un dispositif qui remonte à 40 ans ! Imaginez un peu.

Bref, c'est un énorme défi pour l'IoT. Et il n'y a pas de solution simple à cela. Je pense que c'est Dan Gear de MIT qui a écrit une note très intéressante, en suggérant que l'IoT fait qu'on va pouvoir faire certaines choses avec l'IoT, et d'autres on ne va tout simplement pas pouvoir les faire.

ALEJANDRA REYNOSO : Merci beaucoup Eliot. Une dernière question ? Oui.

RIA OTANES : Oui, d'Anupam Agrawak : pensez-vous que le système des identifiants actuel sera capable de respecter les conditions en termes de confidentialité par rapport à l'IoT ?

ELIOT LEAR : Il y a un grand silence parce que c'est une question très difficile.

CRISTIAN HESSELMAN : Oui, en fait, il y a deux parties ici.

C'est le système des identifiants, dans ce cas c'est ce dont on a parlé, les noms de domaine comme identifiant. Ça, ça peut être protégé pour renforcer la confidentialité des utilisateurs.

Mais ensuite il y a une deuxième dimension. Quels types d'information votre dispositif partage avec les services à distance ? Donc là il s'agit de contenu, oui, mais aussi de tendances en termes de trafic. Donc en

regardant uniquement les tendances en termes de trafic, on a une idée de ce que vous faites. Donc ça ce sont deux choses qu'il faut regarder si vous voulez renforcer la confidentialité.

Si on regarde les messages pour ce qui concerne les identifiants, le DNS, mais aussi les tendances en termes de trafic qui sont échangées, et vous voyez que cela donne des informations en termes de chiffrement et aussi en termes de dispositifs avec lequel vous interagissez.

Donc je suis d'accord avec Aliot pour dire que c'est une question très complexe.

ALEJANDRA REYNOSO : Merci beaucoup Cristian et Eliot. Eliot, vous souhaitiez ajouter quelque chose ?

ELIOT LEAR : J'essayais de répondre à la question de Nigel, qui posait une question par rapport aux défis par rapport à la propriété intellectuelle et au mécanisme de la 5G et des normes internationales en termes d'IoT.

Je pense qu'il y a affectivement un certain nombre de défis qui se posent par rapport à la 5G. Le premier de ces défis c'est : comment limiter les menaces de surface de ce genre de dispositif ? Quel est le rôle du fournisseur pour atténuer ces menaces ? Et quelle est l'interaction entre le contrôle du réseau et le DNS dans un monde fondé sur le nuage ?

Et, ça revient au problème dont je vous parlais pour les applications ou pour les dispositifs domestiques.

On commence tout juste à évoquer ces questions, mais on en est au tout début.

ALEJANDRA REYNOSO : Merci beaucoup Eliot. Dernière question, parce que malheureusement nous n'avons plus beaucoup de temps. Ria, si vous voulez nous la lire.

RIA OTANES : Oui, une question de Suada Hadzovic : si nous avons des fournisseurs de nuages IoT, qu'en est-il de la relation avec les nœuds et périphériques conformément au NIST, les « Fog Nodes » sont en fait des composantes physiques, comme les passerelles, etc. ?

ELIOT LEAR : Bon, je crois que je vais me lancer là aussi pour répondre.

En fait, il y a plusieurs modèles informatiques pour les dispositifs IoT. Et comme je l'ai dit dans l'une des réponses, le coût des biens et services sur les nœuds fait que beaucoup des fabricants essaient de maintenir leurs prix au plus bas. Donc, ce qu'ils font, c'est qu'ils transfèrent beaucoup de cette puissance dans le nuage pour ajouter autant que possible. Et à ce niveau-là, le nuage, c'est extraordinaire.

Mais le nuage a également ses limites. Par exemple la latence, le temps de latence, où on a besoin de capacités locales.

Donc, toute cette notion d'ordinateur mérite d'être approfondie. C'est pas quelque chose qu'on peut voir dans l'espace des clients, mais c'est quelque chose de très courant au sein des contrôleurs locaux où il y a des capacités en termes de processus au niveau local et en termes de communication entre les dispositifs IoT. On le voit, c'est le cas dans le secteur industriel, mais, je vous le disais, ça mérite d'être approfondi.

ALEJANDRA REYNOSO : Merci beaucoup Eliot.

Je vais maintenant passer aux conclusions de ce qui a été dit, très brièvement, rassurez-vous. Il est très important pour nous de poursuivre cette conversation par rapport aux opportunités, risques et défis que pose l'interaction entre le DNS et l'IoT. Il est important d'être conscient du fait qu'il y a une interaction passive, ce qui veut dire que l'utilisateur n'est pas conscient de ce qu'il se passe au niveau de ces dispositifs, et il faut travailler là-dessus.

La confidentialité, c'est un autre problème, la sécurité en est un autre. Et il y a des défis qui se posent à ces deux niveaux-là. Et le travail que la communauté de l'ICANN peut faire c'est de mieux comprendre les tenants et les aboutissants de ces risques et opportunités et la manière dont les différentes organisations et comités consultatifs de la communauté peuvent faire en sorte qu'il y ait une meilleure interaction entre l'IoT et le DNS.

Je tiens à remercier tous les membres du panel et membres également de la révision des pairs, qui ont participé, toutes les personnes qui ont posé des questions aussi.

Excellent travail. Cette plénière touche à sa fin, merci beaucoup et on se retrouve plus tard.

Merci à tous, au revoir.

[FIN DE LA TRANSCRIPTION]