COPENHAGUE – Présentations de NextGen
Lundi 13 mars 2017 – 11h00 à 15h00 CET
ICANN58 | Copenhague, Danemark

DEBORAH ESCALERA: Bonjour. Les NextGen, lorsque vous allez présenter, sachez qu'on va vous chronométrer. Donc lorsque vous voyez ce signal, ça veut dire qu'il vous reste une minute. Quand je vous fais ce signe-là, ça c'est ce que je vais vous indiquer lorsqu'il vous restera une minute.

Et vous saviez que vous aviez dix minutes. Votre présentation ne peut pas dépasser les dix minutes. Vous êtes 15. Donc, je vous préviendrais une minute avant la fin de votre temps de parole. Bon. Si vous dépassez d'une ou deux minutes, ce n'est pas la fin du monde. Mais essayez d'éviter.

Alors je vais lire vos noms rapidement.

[Inaudible]. Matamoros. Est-ce que je dois dire Ferrari…

Je ne sais pas comment dire votre nom de famille. [Inaudible]. [Inaudible], c'est votre nom de famille ? Est-ce que je dois vous appeler Ferrari ou [inaudible] ? Comment se prononce… Attendez, venez. Venez.

Et Desara Dushi. Desara Dushi. Est-ce que je t'appelle Sara ? Oui. Jacqueline Anita ou Jackie. Anita ou Jacqueline ? Jackie. Parfait.

Katharin Tai, Krishna Kumar. Luã, est-ce que vous voulez que je dise tout votre nom de famille ?

LUÃ FERGUS OLIVEIRA DA CRUZ: Non. Non, Luã Fergus.

DEBORAH ESCALERA: Matthias Markus. Est-ce que je dis tout votre nom ? Matthias ? Nertil Berdufi ? Berdufi.

NERTIL BERDUFI: Oui, c'est un petit peu difficile.

DEBORAH ESCALERA: Ensuite, Olga. Comment dites-vous votre nom de famille ? Kyryluk ? Oui, je vais essayer. Peter Cihon. Valeriia Filnovych. J'ai réussi à le prononcer, celui-là. Yousra et votre nom de famille ? Yousra, comment prononcez-vous votre nom de famille ? Allumez votre micro, s'il vous plait.

YOUSRA HSINA: Hsina.

DEBORAH ESCALERA: Alors, j'aimerais vous rappeler que vous allez être enregistrés. Donc lorsque vous vous présentez, parlez lentement. Dites votre nom. Dites-nous d'où vous venez, parce que nous avons des interprètes qui sont en train d'interpréter au fond de la salle. Donc gardez-le présent à l'esprit. Nous allons commencer dès maintenant, parce qu'on est un petit peu en retard.

Petit problème donc technique. Merci au public qui est venu écouter ces présentations NextGen pour ICANN 58. D'abord, nous avons la présentation d'Abderrahman Aït Ali. Est-ce que nous avons sa présentation à l'écran ?

ABDERRAHMAN AÏT ALI: Bonjour à tous. Aujourd'hui, je vais vous parler d'une nouvelle technologie : la technologie blockchain. Et je vais me placer ici entre les deux écrans. J'ai l'impression que ce pointeur ne marche pas. Si, ça marche.

Alors tout d'abord, je vais vous dire ce qu'est le blockchain, ses principales caractéristiques. Ensuite, je vais vous parler un petit peu d'histoire. C'est une histoire récente d'ailleurs. Je vais vous faire la liste de certaines applications qui sont très intéressantes, dont l'un des projets sur lequel je travaille.

Et l'autre, c'est une idée pour que l'ICANN puisse y travailler. Ensuite, plusieurs conclusions. Alors qu'est-ce que le blockchain ? C'est un registre public entre pairs qui permet de maintenir un réseau entre ordinateurs. Donc, l'idée consiste en une transaction et en un système de stockage.

C'est un outil cryptographique. L'idée est d'avoir une liste en chaine d'archives et de registres. Voici certaines des caractéristiques de blockchain qui sont très intéressantes lorsqu'il s'agit des services liés à l'Internet. L'une de ces caractéristiques, c'est l'ouverture. C'est ouvert à tous pour pouvoir éditer et contribuer.

Ensuite, la décentralisation, autre caractéristique essentielle. Personne ne contrôle ce registre. C'est quelque chose de décentralisé. Aussi la sécurité, ça c'est une autre caractéristique très importante. Le registre, le système de stockage et le système de vérification utilisent la cryptographie, qui est très intéressante au niveau de la recherche.

Aussi, la résilience, il s'agit d'un système de distribution. Donc, nous avons un système de réplication qui est en cours et d'autres caractéristiques comme l'immutabilité, tout ce qui figure dans le registre ne peut pas être modifié ; le consensus aussi ; la confiance, exemple Bitcoin ; et la traçabilité. On peut suivre toutes les transactions.

Vous voyez ici un exemple, Bitcoin qui est une application très connue. Il s'agit d'une devise cryptographique qui est fondée sur des chaines de blocs. Et ça, c'est une application qui lance toute une série d'autres applications.

Vous voyez un petit peu ici tout l'historique. Tout a commencé au début des années 90. Donc, c'est relativement récent. Ça a commencé avec un travail de recherche sur la cryptographie et ensuite, il y a eu un mécanisme introduit par Nick Zabo. C'est un concept, ce bitcoin. Mais ensuite, l'exécution, la mise en œuvre, de ce concept a été effectué plus tard par Satashi Nakamoto.

Et ensuite, il y a une autre vague d'applications qu'on appelle blockchain 2.0 qui va au-delà de l'application financière et de la technologie de chaines en bloc. Je vais parler de ces applications après. Donc, vous voyez ici le spectre un petit peu des différentes applications de blockchain. Il s'agit d'un sac d'où sort tous les jours de nouvelles applications. Donc tout commence avec les devises numériques, les contrats intelligents, la sécurité et l'enregistrement de données.

Mais on peut imaginer toutes sortes d'applications qui utilisent ce concept et imaginer ensuite une nouvelle application. L'application la plus connue est dans le domaine des finances. Il s'agit d'une devise cryptographique. Je l'ai dit, Bitcoin. Il y en a une autre, c'est Ethereum, qui a commencé comme une devise

cryptographique et a évolué pour faciliter les transactions et les contrats.

Un autre projet très connu, le projet Dao (D-A-O), pour appliquer des chaines de blocs pour les contrats intelligents. Il y a aussi le financement. C'est une autre partie du projet sur lequel je travaille. Et vous voyez ici à l'écran une liste des différentes entreprises ou projets sur lesquels je travaille pour des applications financières.

Vous voyez qu'il y a beaucoup d'entreprises ici sur cette liste, parce qu'il y a énormément de potentiel dans ce domaine.

Maintenant, l'Internet des choses. Il s'agit d'un domaine d'application où peuvent s'appliquer les chaines de blocs. L'une des applications importantes qu'on a modifiées, c'est l'identité numérique. Donc il y a beaucoup de projets en cours visant à utiliser les chaines de blocs pour identifier les gens de manière numérique.

Il y a également beaucoup de projets en cours liés à l'Internet des choses pour ce qui concerne la sécurité, réduire les vulnérabilités. Et autre application, l'une on en a parlé, parce que l'ICANN pourrait l'utiliser. Hier, on a participé à la réunion du DNSSEC, et l'une des manières de renforcer la sécurité du système du DNS, c'est d'utiliser une infrastructure de système distribué.

Ça, c'est une application intéressante pour l'ICANN. Et autre application intéressante, c'est un projet sur lequel je travaille. C'est lié à la fusion entre les fondateurs d'ONG de sorte que les ONG et les philanthropes ou les bailleurs de fonds puissent échanger entre eux des transactions sans avoir à passer par une autorité centrale comme les banques.

Donc voilà un petit peu l'objectif de ce projet. Si vous voulez obtenir des informations supplémentaires, vous avez ici le site web.

Beaucoup de communautés sont en train de travailler sur ces applications de chaines de blocs, sur ces différents projets et initiatives, dont deux : le Sommet blockchain IEEE ou le groupe de travail d'intérêt spécial sur blockchain de l'ISOC.

Alors conclusion. La technologie blockchain est très, très récente puisque, je vous le disais, elle date des années 90 et elle a des caractéristiques très intéressantes. Elle a toute une série d'applications. Mais il y a beaucoup de problèmes qui, nous l'espérons, pourront être améliorés grâce au travail de notre communauté. Ça pose toute une question, toute une série de questions par rapport à la réglementation à l'extensibilité.

Et voilà. Merci.

DEBORAH ESCALERA: Merci. Alors je vais demander à ce que si vous avez des questions dans la salle, vous puissiez les poser maintenant. Mais je vais demander aux autres membres NextGen d'attendre la fin de toutes les présentations pour poser les leurs.

PERSONNE NON IDENTIFIÉE: Bonjour, je me demande si vous pourriez nous parler un peu plus de la manière dont vous pensez que la technologie blockchain peut contribuer au DNSSEC et à la sécurité du système dans son ensemble ?

ABDERRAHMAN AÏT ALI: Alors est-ce que vous voulez que je réponde à la question ? Alors le DNSSEC, comme vous l'avez vu dans ma présentation sur les caractéristiques du blockchain, il y a une caractéristique qui est celle de la résilience. Donc le fait que c'est un système distribué augmente la résilience du système DNS. Mais il y a un problème par rapport à l'extensibilité. Ça, il faut y travailler.

Et je pense que l'une des applications pour lesquelles on aimerait qu'il y ait plus de recherche et de développement, c'est justement cette application vis-à-vis du DNS.

DEBORAH ESCALERA: Y a-t-il d'autres questions ? Merci. Ensuite, nous avons Carolina Matamoros.

CAROLINA MATAMOROS: Bonjour à tous. Carolina Matamoros au micro. Je suis là pour parler de la perspective de la défense et de la sécurité et du besoin d'avoir un Internet sécurisé plutôt que de n'avoir, pardon, plutôt que d'avoir un Internet ouvert.

Alors pour ce faire, je vais donc parler de cette intersection, de cette problématique, de cette intersection de la défense et de la sécurité, mais de manière plus large avec la perspective de parler de la définition de la sécurité et de la défense, plutôt que de parler uniquement de la sécurité telle qu'on la définit dans ce débat en principe.

Alors, commençons par une présentation simple de ce à quoi on fait référence en matière de défense et de sécurité. Alors en général, on parle des États et des individus. Donc comment se protéger ? Alors qu'en fait, c'est beaucoup plus. Il faut parler également de la souveraineté, pardon, des États. Comment les défendre et comment les protéger ?

Et comment le faire dans tous les domaines. Donc dans tous les domaines. Il faut défendre tous les domaines d'un État. Également, ici, en Europe, il y a le concept de la sécurité des

hommes et des femmes. Donc comment est-ce qu'on protège les personnes de toutes les sphères ?

Comment est-ce qu'on peut leur permettre d'être entièrement épanoui, de s'assurer que leur liberté est totale ? Et c'est ce que cela veut dire, la sécurité, n'est-ce pas. Alors pour le faire, il y a bien sûr l'armée, les polices nationales, et ce sont ces agences qui s'assurent de l'application des lois. C'est eux qui garantissent les lois. En tout cas, en théorie.

Ils sont là pour nous protéger. Alors encore une fois, je ne vais pas passer beaucoup de temps là-dessus. Mais donc, l'Internet est ouvert et mondial. C'est une plateforme qui est réellement ouverte, qui nous permet d'innover, de créer, de connecter, de nous connecter les uns les autres. Nous sommes tous là, parce que l'Internet a un impact sur notre vie à un niveau assez élevé.

Pour les gouvernements, et bien c'est la possibilité de gouverner quelque chose de manière adéquate, un État, des individus, toute une organisation. Donc, la définition de ce que c'est, ça peut être local, national, international, etc. Mais il faut que quelqu'un gouverne quelque chose qui gouverne. Alors revenons à cette intersection entre la sécurité et la gouvernance.

Pour que ça fonctionne, il faut savoir qui vous gouvernez, qui vous protégez. Donc ce qui est intéressant, c'est de savoir qui c'est. Et en général, on le définit dans la constitution, dans un

traité, etc. Donc, on définit qui ont défend suivant les différentes lois, suivant la gouvernance.

Donc ça, c'est très important. Il n'y a pas de force de sécurité internationale en fait. Il y a une coordination entre les États, mais il n'y a pas de force internationale. Donc, les États discutent de la manière dont on va protéger ceci. C'est un processus assez complexe qui est basé sur le consensus et la coordination, et qui est d'ailleurs difficile à atteindre.

Alors, il faut noter qu'il n'y a pas de gouvernance sans la défense et la sécurité. Donc, cette défense et cette sécurité internationale dépend de la coordination entre les États. Alors qu'est-ce que cela veut dire en matière d'application de la loi ? Si on dépend de la coordination, est-ce qu'on peut réellement appliquer les lois ? En fait, c'est très difficile à faire. Donc maintenant, quand on revient en arrière, quand on reparle de la gouvernance d'Internet, il y a beaucoup de choses qui sont complexes, commencer par les lois nationales, les lois des États qui ne sont pas alignées.

En fait, on peut avoir en fait des approches très différentes sur ce qui est autorisé et ce qui n'est pas autorisé suivant les États. Qu'est-ce qui constitue un crime et qu'est-ce qui n'en est pas un. Maintenant, l'Internet doit rester ouvert et neutre, mais c'est assez complexe. Premièrement, il y a le problème de

l'anonymité. Toute personne peut dire ce qu'elle souhaite dire. Donc personne n'est en fait responsabilisé par rapport à ce qu'il ou elle fait sur l'Internet.

Alors bien sûr qu'on connait tout ce qui est faux sur Internet, les faits qui sont faux. Nous sommes un petit peu dans l'ère de la désinformation. Il y a tellement d'informations qui sont fausses sur le web que c'est très difficile à gérer, parce qu'en fait on ne sait plus vraiment ce qui est vrai et ce qui ne l'est pas.

Donc, en fait il n'est pas du tout clair de savoir comment en fait organiser ces politiques de l'Internet. On ne sait pas qui le fait. Alors passons maintenant à la défense et la sécurité avec l'Internet. Alors, première question. On ne sait pas en fait qui est l'auteur de la cyberattaque et ce serait très important de le savoir.

Ce que l'on peut faire, c'est identifier l'adresse IP. Mais même ça, c'est difficile. Donc, il est très complexe de savoir qui a fait quoi et il est également très difficile de se focaliser sur l'attaque en elle-même. En quoi elle consiste ? Vous pouvez attaquer mon identité, vous pouvez attaquer mon compte en banque, et suivant ce qu'on attaque, il y a une difficulté là.

Et finalement, la focalisation de l'État va dépendre. Si, par exemple, l'attaque vise la souveraineté de l'État, bien sûr que l'État va s'en préoccuper. Nous sommes tous menacés. Nous

sommes tous là, mais en en fait il y a différentes mesures en matière de sécurité qui assurent notre protection et donc, vous savez, ce dont je parle en fait, c'est la question du domaine.

La question du domaine. Donc pensez un petit peu aux océans, aux territoires, etc. Donc ça en général, ce sont des domaines spécifiques que l'on protège. Mais l'Internet, c'est un autre domaine qui existe, sur lequel nous avons des droits et dans lequel nous devons être protégés tout comme les États. Mais les juridictions ne sont pas claires. Donc comment peut-on se défendre dans ces conditions ? Donc, c'est très complexe comme question.

Et étant donné cette difficulté, il y a différentes réactions. Il y a donc un traité qui a été fait à Munich dans le domaine de la défense. Et la question de la cybersécurité est vraiment une priorité actuellement. C'est vraiment un domaine très intéressant, et d'ailleurs, c'est un moyen très facile d'attaquer un pays.

Donc, c'est vraiment une priorité pour toutes les nations. Alors qu'est-ce que cela veut dire ? Eh bien, cela veut dire qu'il y a vraiment une grosse implication sur l'ouverture de l'Internet puisque les pays doivent protéger leurs propres intérêts. C'est donc quelque chose qui préoccupe les différentes nations. Cela veut donc dire que cela a un impact sur l'ouverture de l'Internet.

Si on ne s'occupe pas de ce problème, et bien en fin de compte, on va se retrouver avec un Internet fragmenté. Il y a des États qui vont dans ce sens, à différents niveaux. Vous avez la Chine, la Corée du Nord, même l'Allemagne, qui se préoccupent de savoir ce qu'il faut faire par rapport à ça.

C'est donc très complexe comme question. Chaque État cherche à voir comment mieux défendre ses intérêts. Donc nous, ici, nous devons nous préoccuper de cette question. Alors pour terminer, donc premièrement, les pays pourront s'Intéresser à fragmenter, pourraient avoir un intérêt à fragmenter l'Internet justement pour protéger leur nation.

Deuxièmement, il n'y a pas actuellement d'agence qui soit responsable de cette application des lois au niveau international. Vous savez que c'est un problème. Nous sommes tous d'accord pour ça. Maintenant, comment faire ? C'est ça le problème. Troisièmement, la gouvernance internationale de l'Internet, comme on le sait à l'ICANN, en fait est consultative.

On peut faire des recommandations, mais c'est tout. Ce ne sont que des recommandations. Et on continue de vivre avec cette menace sur l'Internet. Et donc ce que je veux faire avec ceci, c'est créer un petit peu un sentiment d'urgence ici à l'ICANN. Il faut faire quelque chose par rapport à ça.

Alors pour conclure, tant qu'on ne sait pas quelles sont les juridictions, comment définir les juridictions et quelles sont les nations qui sont affectées par cette menace, et bien l'idée de la défense dans le cyberespace ne peut pas être réel et ne peut pas exister. Donc, cela veut dire qu'il nous faut absolument protéger cette ouverture et interopérabilité de l'Internet.

Alors voilà des options, des choses que nous pouvons faire. Nous pouvons déjà reconnaitre la fiction et la différencier de la réalité. Il y a une partie historique : ça, c'est la nouveauté. Il faut également faire attention à l'anonymité des utilisateurs de l'Internet. Et bien sûr, il nous faut chercher des moyens d'appliquer les réglementations du point de vue international.

Voilà. C'est tout ce que j'avais à dire.

[Applaudissements]

DEBORAH ESCALERA: Merci Carolina.

Alors y a-t-il des questions ? Là-bas ?

PERSONNE NON IDENTIFIÉE: Est-ce que vous pensez par rapport aux stratégies de défense et de sécurité que la cyber-paix puisse être une stratégie qui

permette de mieux communiquer en fait avec les différents pays ?

CAROLINA MATAMOROS: Qu'est-ce que vous voulez dire par cyber-paix ? La paix donc telle qu'on la définit d'habitude, c'est ça ?

PERSONNE NON IDENTIFIÉE: Oui, oui.

CAROLINA MATAMOROS: Donc en fait, ça dépend de la confiance qu'on a dans les différents citoyens. Est-ce qu'on peut simplement partir du principe que les gens vont simplement respecter la paix, disons qu'ils vont respecter la paix. C'est un petit peu un principe. Bon. C'est possible, mais c'est ambigu.

Il nous faut quand même des mesures, des garanties, comme quoi lorsque quelqu'un n'est pas d'accord avec cette confiance, il nous faut avoir des moyens pour pouvoir les traduire en justice et appliquer la loi. Donc il faut absolument qu'il y ait des mesures en justice pour s'occuper des différentes attaques possibles.

Donc, c'est vrai qu'il peut y avoir un principe, mais il faut quand même s'occuper, c'est préoccupant, de cette situation.

DEBORAH ESCALERA: Y a-t-il d'autres questions ?

PERSONNE NON IDENTIFIÉE: Vous avez dit que pour équilibrer tout ceci, vous avez parlé donc de la fin de l'anonymité des utilisateurs sur Internet. Comment est-ce qu'on équilibre ceci avec la question justement de la protection de la vie privée ?

CAROLINA MATAMOROS: Bien sûr que la protection de la vie privée, c'est quelque chose d'important. Donc la manière de traiter ceci, ça va dépendre des pays. On peut par exemple dire : vous pouvez faire ceci de manière volontaire. Donc en fait, donner votre identité de manière volontaire. Ça, c'est une option.

Et vous pouvez le faire dans différents domaines. Donc par exemple, peut-être que vous ne souhaitez pas être anonyme lorsque vous allez dans votre compte en banque, parce que lorsque vous allez sur un domaine de banque, vous allez en fait faire une transaction en théorie.

Donc tant qu'on peut identifier les personnes qui vont sur leur compte en banque, et bien on peut se sentir en sécurité. Par contre, si vous allez naviguer sur Wikipédia, peu importe, on

peut rester anonyme. Donc, ce n'est pas un gros problème. Peut-être que certains sites peuvent rester anonyme et d'autres noms. Mais la préoccupation par rapport à la protection de la vie privée, c'est une question de confiance de gouvernement. Donc qui va utiliser les informations, hein ?

Donc si, par exemple, je donne une ID, est-ce que quelqu'un va pouvoir utiliser cette ID ? Ça dépend de la question, mais tant que les informations existent, et bien cela reste une menace. Mais je dirais que, pour l'instant, de toute façon il n'y a pas vraiment de protection de la vie privée. Donc si, effectivement, vous donnez votre identité, si vous faites confiance à votre gouvernement comme quoi il va vous protéger, et bien à ce moment-là, peut-être que vous pouvez obtenir davantage de protection de vos droits privés par d'autres entités.

Mais bon, c'est la question. Je comprends qu'il y a un dilemme.

DEBORAH ESCALERA: Merci. Nous avons quelques difficultés techniques. Donc, nous allons attendre un instant et après, on passera à la présentation suivante.

Alors notre prochain présentateur, Chawana Huangsuntornchai.

CHAWANA HUANGSUNTORNCHAI: Bonjour mesdames et messieurs. Je vais vous demander votre attention pendant dix minutes. Alors est-ce qu'il y a d'autres personnes de la même nationalité que moi dans la salle ? Oui ?

Bonjour mesdames et messieurs. Je m'appelle Chawana Huangsuntornchai. Alors, je suis étudiant à l'Université de Leiden, aux Pays-Bas. Et aujourd'hui, nous allons parler de ce qui suit.

Nous allons avoir l'IPv6, qui va être le nôtre pour les prochaines années. Alors j'ai eu une idée très novatrice qui est la suivante : que se passerait-il si nous avions une adresse IP personnelle, une adresse IP statique pour nous tous ?

C'est comme si c'était un chiffre d'identification pour chaque personne dans le monde. Donc, taper une adresse IP et voilà. Ça serait l'adresse IP personnelle pour chacun. Donc comme le présentateur, la présentatrice précédente, il y a une partie essentielle de l'Internet. C'est l'anonymat.

Alors l'absence d'anonymat. Il n'y aurait pas d'anonymat. Certains disent que l'anonymat dans le monde de l'Internet, on ne sait pas si vous êtes un canard par exemple. C'est un exemple. En fait, ce que ça veut dire, c'est qu'on ne sait pas qui vous êtes. Mais si les adresses IP représentent quelqu'un, ça va être vous. Donc, il n'y aura plus d'anonymat.

Et que se passera-t-il en termes juridiques ? Et là, je fais une petite réserve, c'est hautement subjectif, parce que ça dépend de votre point de vue pour voir si c'est une bonne chose ou pas. Quels seraient les effets pour le gouvernement ?

La surveillance deviendrait plus facile, parce que normalement, les adresses IP sont collectées auprès des fournisseurs de services Internet. Mais ensuite, il est possible que les gouvernements aient une base de données qui indiquent qu'à telle personne correspond telle adresse IP. Donc s'ils veulent identifier quelqu'un, ça va être beaucoup plus facile à faire. Alors pour l'application de la loi, les enquêtes, ça va être beaucoup plus efficace aussi. Laissez-moi vous expliquer brièvement.

Si quelqu'un veut commettre un délit en termes de cybercriminalité, alors les autorités chargées de l'application de la loi vont travailler sur les adresses IP d'abord. Et ensuite, comme ils ne savent pas qui est derrière cette adresse IP, grâce à ce système, ils auront une idée plus claire de qui se trouve derrière cette adresse IP. Si vous avez une adresse IP personnelle, ça va permettre de surmonter certaines difficultés. Ils pourront vous trouver beaucoup plus facilement.

Mais il y a, d'après moi, des bonnes choses, parce que ça va permettre de renforcer la protection des citoyens vis-à-vis des

procédures illégales. Parce que si on sait où on est, on peut être protégé et dire, « ne viens pas me causer de problèmes ».

Et ensuite, la protection des données. Les adresses IP deviendraient des données personnelles, ce qui veut dire qu'il s'agirait de données qui peuvent identifier des personnes, en particulier dans le domaine de l'Internet des choses. Maintenant, nous avons des smartphones, des montres intelligentes. Tout est intelligent.

Peut-être qu'on aura bientôt des chaussures intelligentes aussi, des chaussures rechargeables. Je ne sais pas. Et donc, ces données par la connexion de l'Internet sont accessibles. Avec un seul numéro d'identification, vous pourrez vous connecter à tout, vous connecter à toutes ces choses.

Mais le bon côté de cela, c'est que ça va renforcer la capacité de gérer la protection des données personnelles en ligne. Toute information concernant une personne sera réunie dans un seul lieu. Pour faire des réclamations en termes de protection des données personnelles, ça devrait être beaucoup plus simple.

Ensuite, un Internet pacifique. Moi, personnellement, je pense que l'Internet, c'est une bonne chose. Mais lorsqu'on est derrière son écran, il y a une personne de chair et d'os qui réfléchit. Donc si vous êtes chez vous et tout le monde sait qui vous êtes, parce

que vous vous identifiez, parce qu'ils peuvent découvrir qui vous êtes grâce à votre adresse IP.

Alors vous allez penser à deux fois avant d'appuyer sur Enter. Ça, c'est important. Il y a en ce moment beaucoup de cyberharcèlement et ça, ça pourrait avoir un effet dissuasif. Lorsque vous savez que tout le monde vous regarde et que tout le monde sait qui vous êtes, peut-être que ça pourrait avoir un effet négatif sur la liberté d'expression.

Alors là, je vous ai mis une petite image de singe. N'y prêtez pas d'importance. Alors peut-être que les adresses IP pourraient dépasser les numéros d'identité. Pensez à vos numéros de téléphone ou à vos numéros de carte d'identité. En Thaïlande, on en a 13.

Donc peut-être que ça pourrait devenir une opportunité commerciale. Mais qu'en penserait les entreprises de téléphonie. Ça, ça produit un conflit d'intérêt. Et voilà. Merci de votre attention.

[Applaudissements]

DEBORAH ESCALERA: Merci. Y a-t-il des questions dans la salle ?

PERSONNE NON IDENTIFIÉE: Oui, je suis d'accord.

Vous avez parlé de l'anonymat. Et moi, je suis un peu préoccupé par la mise en œuvre de ça, parce que les fournisseurs de services Internet reposent sur la flexibilité.

Pour créer une seule adresse IP pour une personne, ça peut entrainer quelques problèmes. Il faut coordonner toutes ces informations dans une seule base de données. Toutes ces entreprises vont être en concurrence ou en conflit les unes les autres par rapport aux bonnes informations.

Vous pourriez avoir plusieurs adresses IP gérées par plusieurs personnes. Donc pour que cela soit mis en place, en tout cas, d'après moi, ça me semble trop difficile.

CHAWANA HUANGSUNTORNCHAI: Oui, je suis d'accord avec vous. C'est une idée très créative, très novatrice, mais qui sait, peut-être que ça pourrait être mis en place. J'aimerais simplement dire que la mise en œuvre serait quelque chose d'horrible pour les experts techniques. Excusez-moi de le dire, mais moi, je n'ai pas vraiment pensé à la mise en œuvre, à l'application.

Mais effectivement, ça produirait un conflit d'intérêt.

DEBORAH ESCALERA: Merci. Notre intervenant suivant est Clément Genty.

CLÉMENT GENTY: Bonjour à tous. Je suis français. Je suis ingénieur dans le domaine industriel. Donc rien à voir avec la diplomatie, rien à voir avec la comptabilité, mais je voulais simplement vous parler des politiques de nommage. Alors, je ne sais pas si vous avez remarqué que j'étais français, mais en tout cas, je vais parler de la France.

Voilà un avion, un avion magnifique. Oui, c'est un avion français, bien sûr. Et maintenant, c'est un avion américain. D'accord. Alors qu'est-ce que s'est passé ? Je ne sais pas si vous avez remarqué, mais sur – attendez, est-ce que ça fonctionne, voilà – donc sur la queue, il y a une identification, un code. En fait, en 1944, à Chicago, il y a eu une convention pour créer, cette convention sur l'aviation qui donc a lancé l'utilisation de ces codes.

Alors parlons de la radio maintenant. En 1927, nous avons créé le code de télécommunication comme vous le voyez peut-être ici. Je ne peux pas revenir en arrière. D'accord. Si, c'est bon. Donc en 1927, comme je le disais, nous avons lancé ce code et vous le voyez ici sur cette carte QSL d'Inscription pour un club.

Donc le W, c'est US et le F est pour la France. Alors si on continue, lorsque les scientifiques ont créé le système de nom, de domaine ils ont eu en fait la même idée. L'idée, c'était, par exemple, pour le .fr, le ccTLD français, l'idée était à la NRIA, qui est un laboratoire français, de créer des sous-domaines.

Donc en haut, vous avez la gendarmerie, enfin au début, vous avez la gendarmerie qui dépend du ministère de l'Intérieur. Et vous savez que vous êtes un site gouvernemental, parce que vous avez le .gouv.fr. Ensuite, pour l'École militaire française, vous avez St-Cyr, le nom, ensuite terre pour l'Armée de Terre, défense pour la Défense, et gouv. pour le gouvernement, et ensuite, fr pour la France.

Donc même chose pour les États-Unis. Jon Postel qui s'est occupé du .US a créé exactement la même chose. Donc à droite en haut, vous voyez, pardon, [inaudible], k12 pour école, k pour Californie et US. pour les États-Unis.

Donc même chose pour [inaudible], California, US. Donc, ils ont essayé de lancer le kids.us. Mais ça n'a pas marché malheureusement. Alors là, vous avez une université magnifique en Californie, dans la ville de Pomona. Alors regardez bien ce qui se passe.

Vous pouvez en fait lire le nom de domaine et faire confiance à ce nom de domaine, parce que vous savez que c'est Pomona

College State, donc école universitaire. Même chose pour la police de New York. Vous allez sur police, city, New York, États-Unis (US). Mais les opérateurs de registre se sont rendu compte qu'ils pouvaient gagner d'argent en retardant tous ces sous-domaines.

Donc qu'ont-ils fait ? Oui, ils ont gagné beaucoup d'argent. Mais que s'est-il passé ? En fait, ils ont retardé cette identification, cet outil d'identification des domaines. Donc maintenant, je peux enregistrer un nom de domaine. Je ne sais pas, par exemple clement.avocat.us. Rien n'est interdit.

Les sociétés ont essayé de créer des barres de navigation pour aider l'utilisateur final à faire confiance aux informations sur l'Internet. Mais ça ne fonctionne pas réellement. C'est un fait. Et ensuite, on a créé la sécurité SSL, donc une belle histoire également.

Par exemple, vous avez deux sites web PayPal qui ont tous les deux le SSL. Mais, comme il y a toujours un mais dans la vie, à gauche, comme vous le voyez, c'est le site web PayPal avec sécurité SSL. À droite par contre, vous avez le summary support qui a la sécurité SSL et si vous regardez bien à droite, le domaine a le SSL également. Mais le premier niveau de SSL est différent, parce qu'en fait il y a trois niveaux de SSL.

Donc en fait, on ne peut pas faire confiance aux informations sur l'Internet. C'est la réalité d'aujourd'hui. Par exemple, aujourd'hui, on peut dire : bon, je connais bien le site français gouvernemental, mais je ne peux pas réellement faire confiance. Je sais que, par exemple, en mai nous avons les élections en France et quand j'ai vu ce qui s'est passé dans d'autres pays à cause des fausses nouvelles, et bien ça me fait peur.

Alors, voilà ce qui se passe. Je pense qu'il n'y a pas de possibilité d'avoir confiance dans l'Internet. C'est ma conviction. Je suis donc enseignant à l'université et je demande toujours à mes étudiants de me donner des idées. Comment peut-on faire confiance aux pages sur Internet ?

Par exemple, donc si on recherche des informations médicales sur Internet, par exemple sur l'avortement, on peut chercher beaucoup d'informations. Mais on se retrouve avec différents sites web. Différentes informations. Comment faire confiance à ces informations ?

Alors on a demandé aux étudiants en fait de donner une note aux différentes sites web : donc 3, je peux faire confiance et 0, je ne peux pas. Donc comme vous le voyez, le .gouv.fr, c'est vraiment le niveau le plus élevé de confiance que les étudiants ont pu noter.

Donc ce que je veux présenter, c'est en fait un outil gratuit pour les utilisateurs français. Pourquoi les utilisateurs français ? Parce que j'utilise un ccTLD qui n'est pas utilisé. Comme vous le savez, la France est un petit peu partout dans le monde. Vous avez la Guyane, vous avez la France en Amérique du Sud. Vous avez la Réunion qui est plus proche de l'Afrique. Vous avez des territoires en Antarctique, etc.

Donc, nous n'utilisons pas deux ccTLD. En fait, vous avez [inaudible] ici, à l'ouest du Mexique. Et l'autre, le ccTLD pour la France métropolitaine qui est le .fx. Donc, je veux en fait utiliser ce fx pour recréer de la confiance sur Internet.

Alors voilà ce qui se passe. Nous allons créer un espace de confiance avec des sous-domaines gérés par certaines autorités. Et donc, qu'est-ce que je veux dire par autorité ? Par exemple, l'Association des avocats, parce que la profession donc des avocats est gérée par le Conseil national des barreaux en France.

Donc mon idée, ce serait qu'on gère le .avocat.fx en utilisant ce Conseil national des barreaux. Même chose pour les ambassades, même chose pour les aéroports. Donc, que chaque association gouverne son propre site web. Pour les ambassades par exemple, n'importe qui peut enregistrer son propre domaine .org.

Donc, imaginez-vous un petit peu qu'en France, tous les domaines ccTLD qui peuvent exister sont en fait des faux sites. Donc voilà ce que je propose.

En fait, on ne peut pas… Comment m'exprimer ? On ne peut pas… Ce que je suggère, c'est d'utiliser des sous-domaines selon la certification Diderot-Alembert. Je ne sais pas si vous vous souvenez, c'était il y a 300 ans. Diderot et Alembert pensaient qu'on pouvait diviser les informations en trois catégories : mémoire, raison, imagination. Donc, j'en parlerais un peu plus par la suite.

Ce que je suggère, c'est d'avoir une structure de TLD avec un bureau d'enregistrement qui accrédite. Donc voilà ce que je propose. Voilà un petit peu mon idée. On ne peut pas nécessairement faire confiance à tout sur l'Internet par le biais des outils qui existent actuellement. Il faut absolument qu'on trouve une solution à ça. Merci.

[Applaudissements]

DEBORAH ESCALERA: Merci beaucoup. Donc encore une fois, pour les NextGen, les questions seront à la fin. Mais s'il y a des questions dans l'auditoire, allez-y.

PERSONNE NON IDENTIFIÉE: J'ai une question par rapport à la confiance. Est-ce que vous considérez dans votre travail un projet qui a été fait par un chercheur français, Louis Pouzin, qui a inventé la racine ouverte ? Ça pourrait être utile justement dans cet objectif pour toutes les personnes qui ne font pas confiance à l'ICANN.

CLÉMENT GENTY: Oui, effectivement. Je rencontre Louis Pouzin la semaine prochaine. Donc, Louis Pouzin a inventé la racine ouverte et il a créé une alternative à l'Internet il y a plusieurs décennies.

DEBORAH ESCALERA: Alors un petit instant, Sara, on a quelques difficultés. Bien. Prochaine présentatrice. Dara Dushi.

DESARA DUSHI: Bonjour, je viens d'Albanie. Et je fais un PhD à l'Université de Bologne…

DEBORAH ESCALERA: Excusez-moi. On va changer d'ordinateur. On a un problème avec votre présentation.

Excusez-moi dans le public. Un instant, s'il vous plait.

Alors, nous faisons une pause déjeuner entre 12 h 00 et 13 h 00, 12 h 30 et 13 h 00 et on se retrouve à 13 h 00.

On va avoir une pause déjeuner très, très courte.

Donc, on reprend. Sara.

DESARA DUSHI: Je suis une candidate au PhD. Je fais une recherche sur l'abus sexuel des enfants sur Internet et l'exploitation sexuelle des enfants sur Internet. J'aimerais commencer cette présentation avec cette citation qui date de 1995 : « Tout comme l'ordinateur a commencé à révolutionner la vie sociale, il va révolutionner la criminalité et la déviance, en particulier les paramètres de comportement sexuel déviant ». Et c'est de ce fait en train d'arriver.

La cybercriminalité a commencé depuis de nombreuses années maintenant. Je n'arrive pas à faire avancer ma présentation. Vous voyez ici certains événements de 2015-2016. À l'heure actuelle, il y a 2,4 milliards d'utilisateurs Internet. Mais comme vous vous souviendrez de la présentation de Göran, on est passé à 3,9 milliards d'utilisateurs Internet maintenant.

En 2016, l'Internet Watch Fondation a identifié plus de 68 000 sites web ayant un contenu d'abus sexuel pour les enfants, soit une augmentation de 417 % depuis deux ans. 69 % des enfants

sur ces images ont 10 ans ou moins, et la plupart d'entre eux sont des filles, des petites filles.

Conformément aux chercheurs, il y a un comportement en ligne comportant des risques. Par exemple, fournir des informations personnelles à des personnes qu'on ne connait pas ou se mettre d'accord pour rencontrer des étrangers ou des amis virtuels.

Alors voici des formes d'abus sexuels d'enfants en ligne. Ça se produit par l'intermédiaire d'images. Et maintenant avec l'Internet, tout est beaucoup plus facile. Ça devient un problème mondial. Alors les types d'abus sont : abus sexuels des enfants, abus sexuels en ligne, harcèlement sexuel, incitation sexuelle, exploitation sexuelle, prostitution des enfants, trafic des enfants à des fins sexuelles, production et consommation pornographique infantile.

Quelle est l'illustration de ce problème dans la vie réelle ? En 2007, il y a eu un cas au Royaume-Uni où ils ont trouvé des images d'abus sexuel d'enfants, des petites filles qui provenaient d'Asie du Sud-Est. Ils n'ont pas pu prouver la personne à l'origine de ces abus. Ils avaient un suspect qui a été détecté, parce qu'Il voyageait très souvent en Asie du Sud-Est. Mais ils n'ont pas pu prouver que c'était la personne qui avait perpétré ce délit, parce que sur les images on ne montrait que sa main et l'enfant qui faisait l'objet de cet abus.

Donc, ils ont demandé l'aide d'un centre de recherche qui utilise une technique très spéciale pour croiser des caractéristiques de peau. Et ils ont pu croiser cela avec celle qui apparaissait sur les images. Donc cet exemple montre bien le lien entre les images en ligne qui circulent sur Internet et ces images.

Ces images sont réelles et ces enfants sont effectivement victimes d'abus dans la réalité. Donc l'application de la loi. Les forces chargées de l'application de la loi ne peuvent pas agir seuls. Il faut une coordination entre les différentes parties prenantes. Cela démontre aussi l'échelle internationale du problème, parce que les criminels en général ont pour habitude de perpétrer ces délits dans des pays où il n'y a pas de juridiction très forte en termes d'application de la loi et de lutte contre la cybercriminalité.

Il y a également un besoin de coordination entre différentes institutions. Autre exemple, en novembre 2015, lorsque vTech, c'est une grande entreprise à Hong Kong qui fournit des technologies utilisées à des fins éducatives pour les enfants, a été victime d'un hacker qui a mis en danger les comptes de 6,4 millions d'enfants.

Donc l'identité et l'adresse de ces enfants a pu être découverte. Des statistiques mondiales maintenant. Les images d'abus d'enfants ont surtout lieu en Amérique du nord et en Europe.

Vous voyez ici un graphique qui vous montre le nombre de domaines qui hébergent des contenus d'abus sexuels d'enfants. Le niveau le plus haut date de 2007 et depuis, même s'il y a une baisse régulière, il y a une nouvelle augmentation à partir de 2011 avec en 2015 plus de 1 991 domaines qui hébergent des contenus d'abus sexuels d'enfants.

Alors, quelles sont les mesures juridiques les plus efficaces pour faire face à l'abus sexuel des enfants en ligne ? D'abord, le renforcement des capacités internationales au niveau juridique, application de la loi et capacité technologique.

Alors pour répondre à ces questions, j'ai prévu de suivre quatre axes : les causes du délit ; la prévention ; l'identification ; et la réponse.

Quelle a été la méthodologie que j'ai utilisée jusqu'à présent ? Des analyses normatives des normes internationales, des analyses au cas par cas, des entretiens avec les victimes, les gouvernements, les universités et la communauté technologique.

Points critiques que j'ai détectés jusqu'à présent : il n'y a pas de définition uniforme, unique, de contenu d'abus sexuel des enfants et de limite d'âge pour consentir à s'engager dans des activités sexuelles. Il n'y a pas de définition standard non plus d'abus sexuel des enfants. Également, la criminalité

transfrontière, ça pose des problèmes en termes de juridiction. La communication entre les différents pays pose problème aussi et il y a un taux très faible de plainte déposée dans ce domaine. On détecte que de manière occasionnelle ce genre de délit. Dans la plupart des délits, il y a un manque d'effort de la part des services de recherche.

Les enquêteurs manquent d'expérience dans le domaine de l'abus sexuel des enfants. Il y a un grand besoin aussi de définir l'âge universel commun pour consentir à avoir des activités sexuelles. Et ça, c'est un gros problème lorsqu'il s'agit de criminalité transfrontière et que l'enfant peut être considéré adulte dans un pays et l'auteur du délit ne peut pas être poursuivi.

On peut également adopter une approche multi parties prenantes vis-à-vis de ce problème que j'ai dit auparavant. Conclusion jusqu'à présent. Nous avons besoin de nouvelles technologies pour le processus d'enquête. L'une de ces technologies a été introduite ces dernières années aux États-Unis par [inaudible]. Ils ont une technologie Spotlight que la plupart des pays aujourd'hui utilisent pour leurs enquêtes et c'est plus facile grâce à cette technologie de détecter les images d'abus sexuels des enfants.

On a également besoin d'une coopération multi parties prenantes dans la prévention et la recherche des cas d'abus sexuels des enfants en ligne. La possibilité aussi de se retirer vis-à-vis des dispositions des documents internationaux concernant l'abus sexuel des enfants. Ça, c'est un obstacle pour l'uniformité des normes juridiques au niveau international.

Également le nombre de personnes qui s'occupent d'enquêter ce genre de délits est très faible. Il y a également un commissaire ou un médiateur qui est chargé de ce type de problèmes comme, par exemple, en Australie. Merci.

[Applaudissements]

DEBORAH ESCALERA: Merci Sara. Est-ce qu'il y a des questions dans la salle ?

Bien. On va faire une petite pause déjeuner. On va se retrouver à 12 h 40. Oui, vous êtes d'accord. Merci. 12 h 40.

Bonjour les NextGen. J'espère que vous êtes prêts. Nous allons bientôt commencer.

Donc, j'aimerais vous rappeler que vous ne devez pas ouvrir vos ordinateurs pendant que quelqu'un fait sa présentation, même chose pour les téléphones. Vous ne consultez pas vos téléphones. D'accord. Donc ça, c'est pour la session.

D'accord. Si vous prenez vos notes, je comprends si vous les prenez sur ordinateur. Mais l'idée, c'était quand même de ne pas utiliser les ordinateurs et de prendre les notes su cahier. C'est pour ça qu'on vous a donné des blocs-notes.

Je pense que l'auditoire va revenir, mais pour des raisons de temps, il vaut peut-être mieux commencer. Nous allons donc recommencer. Ensuite, nous avons donc Jacqueline Eggenschwiler. J'ai même réussi à prononcer son nom.

JACQUELINE EGGENSCHWILER: Bonjour à tous. C'est vraiment difficile de revenir du déjeuner. Je sais, c'est complexe. Et on le voit, il n'y a personne ici. Donc comme vous l'avez dit, je m'appelle Jacqueline Eggenschwiler. Je fais des recherches à l'Université d'Oxford et je me concentre sur la réglementation dans le cyberespace. Donc ce que je vais vous présenter aujourd'hui, c'est en fait un projet qui est connecté à ces informations et qui est en lien avec la redevabilité. Donc, c'est un terme qu'on utilise énormément. Je vais également parler du modèle multi-acteurs. C'est donc le deuxième terme à retenir de cette présentation.

Alors pour vous donner un petit peu l'historique, la motivation en fait de ce projet, ce que l'on voit qui émerge dans l'espace, qui existe dans l'écosystème de la technologie numérique et

dans cet environnement, et bien ce sont différents acteurs, différentes sphères de règlementation qui se retrouvent.

Et puis, bien sûr, différents domaines de préoccupation. Ce n'est pas uniquement la gestion du DNS, mais c'est aussi la question de la vie privée, la protection des données, la cybercriminalité. C'est aussi la question de gérer un IP personnel comme on a mentionné tout à l'heure.

Donc, il y a beaucoup de questions qui sont rassemblées dans tout ceci. Ce que cela veut dire, c'est que nous avons un modelage de structures de redevabilité. Étant donné la multiplicité des acteurs et des questions auxquelles on est confronté et étant donné également les différents lieux de discussion qui sont impliqués dans cette réglementation, on ne peut pas vraiment dire : okay, cet organe sera responsable de ceci et celui-là de cette autre question.

Il y a des conflits en fait. Donc une des questions initiales dans le cadre de ce projet, c'est du point de vue du contexte. Quels sont les enjeux auxquels la redevabilité se trouve confrontée ? Et également étant donné la prévalence de ces acteurs qui se retrouvent, étant donné l'importance de l'influence qu'ils ont dans cet environnement, en fait qu'est-ce qu'on voit émerger en matière de redevabilité dans ce contexte ?

Est-ce que c'est un type de redevabilité ? Est-ce que la redevabilité est multiple, etc. ? En ce qui concerne la première question, je pense que la première partie de la réponse, en tout cas pour moi dans le cadre de mon projet, c'est que les enjeux auxquels on est confronté dans cet environnement viennent des questions de base.

Ce qui se passe en fait, c'est qu'il y a beaucoup de personnes qui sont impliquées dans cet environnement. Il y a beaucoup de questions et donc, il y a une certaine hybridité en ce qui concerne les arrangements institutionnels. Alors en ce qui concerne les différentes personnes impliquées, comme je le disais, ce n'est pas uniquement un acteur, par exemple, les gouvernements qui ont quelque chose à dire. C'est également le secteur privé, c'est les constitutions des différentes nations. C'est les organisations de la société civile.

Donc, il faut vraiment comprendre qu'on a du mal à identifier qui est responsable de quoi dans cette complexité. La profusion des domaines à considérer, encore une fois. Il peut y avoir convergence. Par exemple, le nommage et le numérotage. Il peut se trouver tout d'un coup certaines questions relatives à l'IP.

Donc que peut-on faire et qui est redevable par rapport à ça ? Alors l'hybridité des dispositions prises au niveau institutionnel,

c'est, par exemple, le type de situation selon lequel il y a différentes institutions, des institutions qui sont impliquées dans la réglementation du cyberespace. Mais en fait, ces institutions sont parfois transitoires : elles émergent ; parfois, elles disparaissent selon les besoins ou selon les questions.

Donc voilà l'enjeu dans ce domaine. En ce qui concerne la deuxième question, étant donné la prévalence de ces différents acteurs, quelles sont les structures de redevabilité que l'on peut observer ? Alors à mon avis, il y en a trois. Elles ne sont pas exclusives. Elles peuvent d'ailleurs fusionner et former de nouvelles structures.

Mais il y a donc la redevabilité hiérarchique qui, en fait, fait référence par exemple à une situation étatique. Donc, on a des lignes très claires de commandement. Donc, c'est toujours le point le plus haut de la hiérarchie qui est redevable pour le reste des différents niveaux de la hiérarchie.

Donc ce type de structure existe dans le domaine de la cybersécurité où les gens sont en fait redevables par rapport à ce qu'ils doivent fournir en matière de sécurité. Alors on voit également une redevabilité de type secteur privé, de type entreprenariat. C'est au-delà du voile de l'individu. C'est donc la société ou l'entreprise qui est responsable, qui est redevable.

Donc ce sont des acteurs sur l'Internet qui parlent, qui font référence par exemple à Google, à Microsoft, etc. Donc ça, c'est une redevabilité qui est importante. C'est un type important de redevabilité et on a déjà vu ce type d'exemples de redevabilité qui était demandée de ces entreprises.

Et le dernier point, et sans doute le plus important, c'est la redevabilité collective de la communauté. Étant donné que les différents acteurs sont un impact sur les résultats, que ce soit technique, financier ou autre, et bien s'ils ne sont pas redevables de manière individuelle, parce qu'il n'y a pas une seule entité qui décide. Et bien il faut avoir un instrument qui nous permette de nous assurer qu'ils sont redevables. Donc c'est la communauté. Cet outil.

Donc que ce soit un résultat technique ou autre, il faut absolument définir un certain niveau de redevabilité. Et la redevabilité, c'est vraiment un concept relationnel, parce qu'il y a le devoir d'un acteur à être redevable par rapport à un autre acteur.

Alors, je n'ai pas pu trouver de réponses pour résoudre ces questions que j'ai mentionnées de manière assez directe. Mais en tout cas, j'ai pu considérer les possibilités. Je n'ai pas de recommandation à faire, mais d'une manière générale, ce que nous pouvons dire, c'est que la gouvernance du cyberespace

représente pour les chercheurs donc une certaine complexité de relation, de redevabilité.

Donc, je vais parler des relations justement. Et ce qui est également assez fascinant, c'est que la redevabilité est une question qui est liée avec les éléments mêmes qui constituent la gouvernance du cyberespace. Donc, il y a discussion, débat là-dessus.

Alors ce qui pourrait éventuellement être requis, c'est donc la répétition délibérée et explicite des structures de redevabilité. C'est ce que fait l'ICANN. Donc comment peut-on en fait s'assurer que ces structures soient transparentes et redevables au plus haut niveau possible de manière à ce qu'on puisse voir le processus, le processus qui permette de définir la redevabilité.

Donc voilà la conclusion de mon projet. Je suis tout à fait prête à répondre à vos questions dans l'auditoire et aux questions des personnes du panel plus tard.

[Applaudissements]

DEBORAH ESCALERA: Merci Jacqueline. Y a-t-il des questions dans l'auditoire ? Alors une question dans l'auditoire.

ADIL SABI: Adil Sabi du Pakistan. Je suis ambassadeur NextGen. Donc ma question avec quelques commentaires. Donc tout d'abord, pour Stephane, Andre, Lauren, je voudrais vous féliciter d'être arrivés à ce niveau. Donc, c'est la première chose.

Ensuite, Deborah et Janice, merci pour tout le travail que vous faites pour nous. Je suis NextGen, je suis boursier, et je m'occupe de beaucoup de séances. Mais j'aimerais quand même vous remercier tous et toutes les deux en particulier.

Et puis, bien sûr, la chose la plus importante, pour les personnes dont je m'occupe dans le programme NextGen. Vous savez qu'à l'ICANN tout est transcrit. Donc à chaque fois que vous vous présentez, vous devez donner votre nom, votre affiliation et votre commentaire. Par exemple, vous allez dire : je m'appelle Carolina de Mexico, je suis avec le programme NextGen et voici mon commentaire.

Mais je vous demande s'il vous plait de ne pas simplement poser votre question sans vous présenter. Et il faut savoir également que les NextGen et les boursiers, ce sont deux programmes différents. Il y en a qui disent, je suis NextGen boursier. Non, on ne peut pas être les deux. Donc, il faut savoir faire la différence.

Enfin, le commentaire le plus important, s'il vous plait revenez. Ce n'est pas la fin de votre parcours. C'est uniquement le début.

Quand on est NextGen, on reste NextGen. Je suis là pour vous et j'espère que vous allez revenir. Merci.

DEBORAH ESCALERA: Oui, on a encore quelques petites difficultés techniques. Donc, on va reprendre nos présentations d'ici quelques minutes.

Notre prochaine présentatrice, Katharin Tai.

KATHARIN TAI: Bonjour. Je m'appelle Katharin. J'étudie les relations internationales à l'Université d'Oxford et je me suis concentrée sur la cyber-souveraineté comme récit pour la politique d'affaire étrangère chinoise. Ce projet consiste à définir ce qu'est la cyber-souveraineté. D'abord, ce qui est important, c'est de vous parler de mon parcours et de l'objectif de cette recherche.

Donc, mon parcours d'études. Je me suis concentrée sur les politiques en Asie, la société, l'histoire. Et ensuite, pour ma maitrise, j'ai travaillé sur les relations internationales et je me suis concentrée moins sur la question de ce qu'on devrait faire pour atteindre quelque objectif, mais qui se concentre plus sur la politique et plus théorique et se concentre plus sur l'idée de créer des concepts et de nous aider à comprendre ce qui se passe dans la sphère politique.

Est-ce que cela fonctionne ?

L'idée de cette présentation, c'est de vous donner un aperçu rapide de la cyber-souveraineté et de ce que cela semble être, et en quoi ça consiste, en quoi ça représente un problème. Voir si notre théorie nous donne des outils qu'on pourrait utiliser pour conceptualiser cette idée dans le cyberespace.

Parce que Carolina, dans sa présentation, a parlé d'un État et avec une note en bas de page : juridiction nationale, etc. Alors d'abord, qu'est-ce que la cyber-souveraineté et quels sont les défis que cela pose ?

C'est quelque chose qui a été central et ça fait partie du discours des autorités chinoises depuis 2014, l'époque où en Chine on a créé un petit groupe sur la cybercriminalité. Il s'agit d'une entité au sein du gouvernement qui se consacre uniquement à cette question dans le cyberespace.

Donc, c'est une perspective beaucoup plus nationale, mais ce groupe travaille également sur les relations internationales. Donc, ça fait trois and qu'ils y travaillent. Toutefois, on ne sait pas très bien ce que cela veut dire, la cyber-souveraineté.

Et c'est devenu un mot à la mode, la cyber-souveraineté, par rapport à ce que fait la Chine en termes de cyber-politiques. Et

on a tendance à dire, ah ça c'est que disent les Chinois, mais on va passer à la chose suivante.

Toutefois, personne n'a réellement essayé de voir ce que cela signifie exactement en tant que concept, en tant que mot. Deuxièmement, cela nous force aussi à mettre le doigt sur la question de savoir quelle est la place de l'État dans le cyberespace et comment conceptualiser le rôle de l'État dans ce domaine. Je reconnais que beaucoup de gens disent à l'ICANN qu'on a un modèle multi parties prenantes, on n'a pas besoin de répondre à cette question.

Mais on ne se concentre pas beaucoup sur l'État en tant qu'acteur. En plus, on peut voir que l'État va continuer à avoir un rôle important dans le cyberespace. Donc la question est de savoir comment conceptualiser la souveraineté lorsque nous sommes dans le cyberespace ?

Pour répondre à cette question, il est important de répondre à la question de savoir ce qu'est la souveraineté d'abord. On parle souvent de l'idée selon laquelle la souveraineté mine le cyberespace, que le cyberespace va au-delà des frontières, et en tant que tel, cela mine l'État.

Donc, on a l'idée que l'État est étroitement lié au territoire et qu'il ne peut pas être déconnecté du territoire. Et une fois que le territoire est déconnecté, c'est plus difficile de définir l'État et la

souveraineté des États. Toutefois, si on regarde ce qui s'est passé dans l'histoire et d'où vient la souveraineté, on s'aperçoit que c'est un ensemble de droits qui n'était pas vraiment associé à l'État.

Mais c'est plus associé au roi par exemple, au souverain. Le souverain, ça n'était pas le peuple au début. Ça a été développé au fil du temps en cette notion de peuple. Mais au début, c'était l'idée d'un pays, d'un souverain en tant qu'entité politique.

Aux alentours du XV^e^ siècle, ça a été beaucoup plus lié à l'idée du territoire. Donc, une entité abstraite qui est souveraine et les gens ont commencé à penser à cette entité souveraine avec une référence particulière à un territoire.

Donc, on peut penser à un cercle sur une carte et quelqu'un est souverain à l'intérieur de ce cercle. Ça, c'est une idée qui s'est enracinée au XIX^e^ siècle en Amérique latine avec la décolonisation et le droit à un territoire en particulier.

Donc l'idée que les États en Amérique latine voulaient s'affranchir de la colonisation, la souveraineté des États et le droit à un territoire qui avait été colonisé. Donc, ce ne sont pas des groupes, mais la souveraineté d'une nation sur ce territoire.

Donc soudainement, cette notion de souveraineté ne concerne pas simplement les droits d'une entité spéciale, mais liée à cette

idée d'un territoire. Donc ça, c'est l'idée d'un universitaire qui l'a formulée de la manière suivante : « l'État-territoire a colonisé notre imagination. Donc, on ne peut pas penser à l'État comme étant différent de quelque manière que ce soit, différent de ces lignes sur la carte, ces cartes dimensionnelles donc. »

Si vous pensez au cyberespace, il est difficile de dire où se trouvent les choses sur une carte et d'imaginer deux dimensions. Ça, ça ne s'applique plus.

Et un problème particulier est la question de l'autorité qui nous ramène à la question de la responsabilité, du fait de rendre des comptes ? Parce que si vous avez une carte, vous dessinez une ligne, vous dites : voilà, à droite ça m'appartient et à gauche, ça ne m'appartient pas.

Ça ne peut plus être ça m'appartient et ça ne m'appartient plus en même temps. Et le problème ici, c'est l'exclusivité de cette souveraineté. On ne peut plus l'appliquer. Soudainement, on ne peut plus penser à un espace qui divise les choses, l'espace, en différentes parties en fonction des différents États, parce que les différents États ont clairement une autorité sans que les autres puissent avoir une incidence là-dessus.

DEBORAH ESCALERA: Je vais vous demander de ralentir un petit peu votre rythme, Katharin.

KATHARIN TAI: Maintenant, j'aimerais parler de deux approches à la théorie de la souveraineté qui pourrait nous aider, une idée sur la manière dont on peut aborder cette question de la cyber-souveraineté. D'abord, l'idée de [inaudible] qui disait que la souveraineté, ce n'est pas quelque chose qui peut vous appartenir. Ça n'est pas un gâteau entier, ça n'est pas quelque chose qui peut être divisé en parties.

Certaines parties concernent le contrôle, le contrôle sur les choses, sur un territoire donné. Mais certaines autres parties de la souveraineté concerne l'autorité. Vous avez une part de souveraineté qui consiste à être reconnu comme État légitime par les autres États. Ça, c'est quelque chose qui peut exister en dehors du contrôle.

Conclusion de cet auteur : il dit si c'est le cas, les États peuvent être souverains de manière différente. Certains États sont souverains par la manière dont ils sont reconnus par exemple. Ça, ça fait partie de la souveraineté que d'autres États n'ont pas. Ça ne veut pas dire que la souveraineté dans ces États n'existe pas.

Donc ça, c'est une approche importante concernant le cyberespace, parce que les territoires ont une souveraineté spéciale qu'on utilisait avant et qui ne s'applique plus maintenant. Ça ne veut pas dire que la souveraineté est minée, affectée ou menacée par rapport à d'autres accès, d'autres aspects, pardon.

Deuxièmement, c'est important. C'est intéressant par rapport à ceux qui s'occupent de la mondialisation. Anne Marie Slaughter par exemple, elle travaille sur les réseaux internationaux des professionnels. Et pour elle, la souveraineté en cette époque de mondialisation s'est transformée. On ne pense plus à la souveraineté en tant que différentes caractéristiques, en disant un État a un territoire, une autorité.

Elle dit que les États doivent avoir l'autorité de contrôler leur territoire. Et si ce qu'ils font va dans ce sens-là, ça c'est la souveraineté. Donc la souveraineté, c'est un outil, mais ça n'est plus quelque chose qui va de soi.

Et pour revenir à la Chine, c'est quelque chose qui est très présent dans le récit du gouvernement par rapport à leur compréhension de la souveraineté. Ils disent que la cyber-souveraineté est très importante, parce que sa raison essentielle, c'est le développement économique.

C'est l'objectif qu'on veut atteindre et c'est ainsi qu'on sait que la souveraineté existe. Merci.

[Applaudissements]

DEBORAH ESCALERA: Merci Katharin. Y a-t-il des questions dans le public ?

Présentateur suivant, Krishna Kumar.

Krishna, attendez deux petites minutes.

Okay, allez-y.

KRISHNA KUMAR: Bonjour. Krishna Kumar. Avant de commencer ma présentation, sachez que vous pouvez me trouver sur LinkedIn, Twitter, Facebook. J'utilise les mêmes identifiants partout.

Je vais parler d'une analyse institutionnelle de la transition IANA. Il s'agit de voir comment les… de discuter des différentes approches. Je vais expliquer le concept de gouvernance à travers cela et c'est un sujet qui m'intéresse.

Qu'est-ce que la gouvernance ? La gouvernance, c'est la coordination des actions sociales dans la société humaine. C'est simple. Nous avons plusieurs acteurs qui livrent de la gouvernance. Cela peut venir du gouvernement, de la hiérarchie,

des réseaux et des marchés. La chose qu'on doit savoir, c'est que le gouvernement est seulement un des acteurs qui livre cette gouvernance, pas le seul acteur.

On essaie de comprendre les choses d'une bonne façon. Il ne faut pas que cela mine la souveraineté et cela cause souvent un problème. L'autre chose qui rend la gouvernance essentielle, donc ce sont les institutions. Les institutions sont les règlements que nous, en tant que personne, on utilise pour échanger avec d'autres personnes ou avec d'autres organisations.

Pour que le système fonctionne, les institutions ont donc un rôle clé, et moi, j'ai recherché les éléments, ces éléments-là par rapport à l'ICANN et aux gouvernements. J'ai utilisé pour faire mes études les études qui ont été faites à [inaudible] en 2010.

Pendant très longtemps, les économistes avaient une vision très simple pour voir les choses. Ils ont étudié les marchés et les gouvernements qui livraient donc des biens publics ou privés à des personnes qui étaient considérées comme des personnes rationnelles. Mais en tant qu'être humain, nous savons très bien que nous sommes très complexe. Il y a donc un besoin de comprendre ces systèmes qui sont très compliqués.

Douglass [inaudible] a dit, les humains, nous les êtres humains, nous avons des structures… nous mettons en place des structures motivationnelles très complexes et nous établissons

des arrangements très divers du privé, pardon, des programmes divers privés, gouvernementaux, institutionnels et communautaires.

Pour comprendre ces systèmes, nous avons étudié un modèle polycentrique. Comment cela marche-t-il ? Il suffit donc d'analyser des centres multiples de prises de décision. On doit aussi définir si les fonctions sont dépendantes ou interdépendantes. On doit définir les mécanismes contractuels ou coopératifs. On doit déterminer les juridictions politiques.

Et on doit déterminer des modèles de prédiction d'échanges. Pour les qualifier, ils ont étudié un cadre de travail qui s'appelle l'analyse institutionnelle et le cadre de travail de développement. Il s'agit de définir quels sont les problèmes.

Dans le cas de la transition d'IANA, l'Internet était donc la caractéristique biophysique, les caractéristiques de la communauté. Comment est-ce que la communauté travaille ensemble ? Comment elle participe ensemble et qu'est-ce qu'ils apportent à la table des négociations ?

Les règlements en usage aussi, on doit en parler. Parce que chaque groupe ou unité constitutive a des règlements propres qu'ils utilisent pour interagir avec les autres. La scène d'action, dans ce cas-là, on parle de la situation de la transition d'IANA et

je suis aussi les modèles d'échanges entre les unités constitutives et les résultats.

Durant la transition, je pense que ça a été le cas d'étude le plus intéressant. Parce que beaucoup de personnes du monde entier se sont rassemblées dans un seul effort et ils ont travaillé de nombreuses heures. Ils ont échangé des milliers de courriels. J'ai donc tous mes chiffres sur la diapositive. Ce qui rend cela très spécial, c'est que toutes ces personnes du monde entier qui ont donc grandi dans des systèmes, dans des cultures différentes, se sont rassemblées pour travailler au sein de l'ICANN et ont décidé de souscrire aux valeurs de l'ICANN et donc tout cela… ces agissements très spéciaux.

Aussi, nous avons étudié les situations, les participants, la position de tous les participants, les résultats du contrôle des informations et tous les échanges qui ont eu lieu. On a aussi parlé des différents acteurs, les connaissances qu'ils avaient et les ressources qu'ils apportaient donc à la table.

Quel besoin avions-nous de faire cette étude ? L'ICANN, c'est spécial. L'ICANN, c'est spécial, mais ce n'est pas un système parfait. Ce qui rend cet événement spécial, c'est qu'on s'est rendu compte que c'était fonctionnel : le concept multipartite…

C'est un modèle que certains gouvernements ont essayé d'utiliser depuis les années 90. Ils ont essayé cela avec d'autres

programmes, mais en 1998 avec l'ICANN, lorsqu'on a discuté des défis d'Internet à travers le monde, ce système a été mis en place. C'est donc pour cela que c'est aussi spécial.

Cette étude nous aide à comprendre comment les systèmes de gouvernance sont complexes. Cela nous permet de comprendre les efforts qui ont été faits précédemment et cela nous fait comprendre comment tous les systèmes, les expertises sont valables. Ça nous importe énormément. Merci.

[Applaudissements].

DEBORAH ESCALERA: Merci Krishna. A-t-on des questions dans la salle pour Krishna ?

Merci. Notre prochaine présentation, Luã Fergus Oliveira da Cruz.

LUÃ FERGUS OLIVEIRA DA CRUZ: Est-ce que ça marche ? Alors pour ceux qui ne me connaissent pas, je m'appelle Luã. Je suis brésilien et étudiant, mais actuellement, je vis à Lisbonne. Je vais à l'Université de Lisbonne et je vais vous parler aujourd'hui de la gouvernance de l'Internet et des jeunes. Pourquoi cette thématique ? Parce que ça fait trois ans que je m'y consacre et que je participe à une

organisation qui s'appelle l'Observatoire des jeunes qui dépend de l'ISOC au niveau mondial.

Nous sommes comme un groupe d'intérêt spécial, groupe de travail spécial. Alors la question suivante, est-ce que le monde appartient aux jeunes ? Obama a déclaré que l'avenir appartient aux jeunes qui disposent d'une éducation et de l'imagination suffisante pour créer. Ça, c'est la source du pouvoir de ce siècle.

Ce sont les jeunes qui vont être les dirigeants futurs de notre monde. Mais que se passe-t-il actuellement ? Est-ce que les jeunes ont réellement leur mot à dire par rapport à la formation de l'avenir dans la société dans laquelle on vit ? Est-ce qu'on a réellement la possibilité de dire ce qu'on pense ?

Oui, non, peut-être. J'aimerais vous parler maintenant des défis et des opportunités qui existent pour que les jeunes participent aux discussions relatives à la gouvernance de l'Internet. Nous avons l'expérience de la déclaration des jeunes écrite en 2015 qui, et je cite, « déclare que nous avons eu l'expérience de voir que le principal problème qui s'oppose à la participation active des jeunes sont les limitations linguistiques et l'aspect économique », fin de citation.

Donc la première question qui se pose, c'est comment plaider en faveur d'un plus grand parrainage et d'initiatives visant à renforcer les capacités. En ce qui concerne les débats qui

existent au niveau international sur la gouvernance de l'Internet, que ce soit au niveau de l'ISOC, de l'ICANN, etc., faire participer les jeunes dans les débats sur la gouvernance de l'Internet. Quelles sont les opportunités actuelles qui existent à l'ICANN ?

On a NextGen, gouvernance prime, c'est un programme sponsorisé par l'ICANN. Pendant un mois, les étudiants… Une personne va dans les universités et donne des cours sur tout ce qui concerne l'Internet et les problèmes de l'ICANN.

À l'ISOC, il y a également deux programmes : Youth IGF programme et également le comité directeur du Brésil à l'ISOC, et une personne ici présente dans la salle a aidé à coordonner ce programme. Il y a des programmes de renforcement de capacité, sur trois mois, qui sont très durs. Il y a deux tuteurs.

J'ai été boursier la première année, tuteur la deuxième année. Donc, c'est un cours très, très complet. Et ensuite, les jeunes qui participent à ce programme ont créé un nouvel observatoire des jeunes où ils essaient de faire participer les gens en Amérique latine et dans le monde maintenant dans son ensemble pour participer aux débats, aller aux forums et participer à ce travail de renforcement de compétences. E donc, cette organisation Youth Observatory est très active.

Nous avons également des écoles sur la gouvernance de l'Internet, la South School of Internet governance. Au Brésil,

nous avons la Summer School of Internet governance. Ça, ça donne la possibilité aux jeunes de participer aux débats sur la gouvernance de l'Internet.

La question est de savoir si ces actions seront suffisantes parce qu'il semblerait qu'on vit dans une espèce de bulle de la gouvernance de l'Internet avec les mêmes qui réunissent toutes les responsabilités, les fonctions. On retrouve les mêmes personnes dans les universités, le secteur privé qui nous parlent de l'Internet, mais qui ne vivent pas réellement l'Internet.

Ils utilisent l'Internet… Autre question importante, qu'est-ce qui influence ? Quelle est l'influence, pardon, des bailleurs de fonds ? Parce que dans la plupart des débats sur la gouvernance de l'Internet et dans le processus multipartite (parties prenantes), les bailleurs de fonds et les intérêts économiques sont négligés à un moment ou à un autre. Parce qu'il semblerait qu'on se dise à chaque fois, il faut désigner une personne de l'Afrique, de l'Asie.

Il faut également un équilibre des genres, un équilibre géographique, mais qui paie pour ces personnes ? Qui finance la présence de ces personnes et la participation de ces personnes aux débats ? Ce qui m'amène à une autre question, pourquoi est-ce qu'on ne veut pas que les jeunes participent à ces discussions ? Ça, c'est une question qu'on doit se poser et c'est

une question que je vous pose d'ailleurs pour que vous y réfléchissiez.

Et là, je vous présente un extrait d'un article écrit par Belli. On devrait considérer l'idée selon laquelle la participation des parties prenantes aux processus de développement des politiques pourrait être motivée par l'approche qui consiste à se fixer un objectif qui pourrait être optimal s'il y avait un intérêt propre ou l'intention de faire pression pour que ce résultat puisse avoir un effet optimal sur l'intérêt du bailleur de fonds.

Ceux qui obtiennent des fonds peuvent participer à ce genre de débat, et uniquement ces personnes-là, et présenter leur point de vue.

Et les autres groupes sont totalement exclus de ce genre de discussion. Ça, c'est un autre problème que j'aimerais soulever, parce qu'à chaque fois qu'on va sur le site web de l'ICANN ou de l'IGF, on nous dit : « Voilà, c'est un espace ouvert. Vous pouvez nous dire ce que vous pensez, donner votre point de vue, etc. » Mais pour les jeunes, c'est difficile de se financer pour voyager, suivre ces débats, ces discussions.

Alors bien sûr, il y a la participation à distance, mais c'est faible. Je sais que certaines personnes essaient d'améliorer cette participation à distance. Alors combien de personnes engagées dans les débats sur la gouvernance de l'Internet sont attentives

aux intérêts de leurs bailleur de fonds et quels sont les intérêts en jeu dans la promotion d'une plus grande participation des jeunes ?

Il y a deux aspects que j'aimerais vous présenter maintenant : la représentativité et la légitimité. La représentativité, il s'agit d'individus qui élisent des représentants pour représenter leurs intérêts. C'est quelque chose de volontaire. Vous pouvez venir ici et dire, voilà je représente la société civile, le secteur académique et les autres vont penser que votre opinion, c'est l'opinion de l'ensemble de la société civile ou du secteur académique.

Donc, il y a une représentativité symbolique. Et comme je le disais, seules quelques parties prenantes de ce processus ont les fonds nécessaires pour participer à ce débat sur la gouvernance de l'Internet. Il y a une élite aussi mondiale concernant la gouvernance de l'Internet.

Par rapport à la légitimité, j'en parlais il y a un instant. Il se pose le problème suivant. Est-ce qu'on peut dire qu'il y a tant de jeunes qui représentent les jeunes connectés ou est-ce qu'il y a une légitimité pour parler en leur nom, au nom des jeunes ? Parce qu'on voit beaucoup de [inaudible]. Celui du forum sur la gouvernance de l'Internet ou bien d'autres où on voit des jeunes s'exprimer au nom de tous les jeunes.

Alors que se passe-t-il maintenant ? On veut être entendu. D'accord, mais après qu'est-ce qui se passe ? On veut être assis à la table des discussions pour voir ce qui va se passer et il y a trois éléments que j'ai soulignés ici.

On a besoin de plus d'espace dans les débats et il doit y avoir également une diversification dans le répertoire des jeunes. Parce que dans les discussions, on continue de dire, voilà, les jeunes ils veulent dire quelque chose. D'accord, oui. Ils veulent dire quoi ? Qu'est-ce qu'ils veulent dire exactement les jeunes.

Ensuite, privilégier la qualité à la quantité. Si vous avez une vingtaine de jeunes qui parlent sans arrêt et qui, finalement, parlent sans fondement, sans connaissance, on ne va pas les prendre au sérieux. Donc, c'est important d'améliorer la qualité. Merci de votre attention.

[Applaudissements]

DEBORAH ESCALERA: Merci Luã. Et, veuillez m'excusez pour le format de cette présentation à l'écran. On a quelques difficultés avec cet ordinateur. On essaie de le formater.

Y a-t-il des questions dans la salle pour Luã ?

[FRANK]: Oui. Bonjour, [inaudible]. Je fais partie des bureaux d'enregistrement. J'aimerais parler de l'impact économique de votre participation. Vous avez parlé de la participation à distance. Vous n'avez pas l'impression que la participation à distance qu'offre l'ICANN et l'IGF, et les listes de diffusion par courriel, vous permettent de participer comme vous aimeriez le faire ?

LUÃ FERGUS OLIVEIRA DA CRUZ: Oui. Vous parlez des listes de diffusion, de l'IGF, etc. Oui, je suis d'accord. Mais en termes de participation des jeunes, on ne voit que les jeunes participent par l'intermédiaire de cette participation à distance. Il faut les faire participer.

Effectivement, à distance, mais aussi en venant à ces événements. Ce sont deux choses qu'il faut faire, d'accord. Liste de diffusion par courriel, participation à distance très bien. Mais il faut aussi qu'ils soient ici, qu'ils vous voient, qu'ils vous regardent dans les yeux et qu'ils vivent cette expérience. Les jeunes n'ont pas les moyens financiers nécessaires pour venir ici, donc s'ils font simplement partie d'une liste de diffusion et qu'ils peuvent uniquement participer à distance, ça n'est pas juste.

[FRANK]: Oui. Je sais qu'il y a des plateformes qui sont créées dans certains pays. Vous pouvez y participer.

LUÃ FERGUS OLIVEIRA DA CRUZ: Oui. Au Brésil, on a organisé une plateforme récemment. On a réuni 20 personnes dans une université pour parler des problèmes liés à Internet sur une plateforme. Donc, on essaie de faire participer les gens, qu'il y ait de nouvelles opportunités qui soient créées pour que les personnes qui sont soit trop démunies, soit trop éloignées, puissent participer.

PERSONNE NON IDENTIFIÉE: Y a-t-il des personnes dans la salle qui ont une autre question ?

JANICE DOUMA LANGE: J'aimerais répondre à votre question en disant que nous proposons par l'intermédiaire de notre équipe d'engagement. Danielle Think, Rodrigo Susido et Albert Daniels dans les Caraïbes seront très heureux de vous aider, parce que par rapport à ce qui vient d'être dit et à ce que vous avez dit. Je pense que c'est une excellente chose de se voir physiquement, mais cette rencontre physique, ce n'est pas nécessaire qu'elle ait lieu lors des conférences. Vous pouvez vous rencontrer à d'autres occasions.

Mais je comprends vos préoccupations et je pense que c'est un appel à l'action que vous avez lancé. Et il faut répondre aux jeunes, les faire participer, leur faire sentir qu'ils font partie de tout cela. Donc, je réponds à votre question et je pense que l'intervention de la personne dans la salle voulait vous dire qu'il existe d'autres options. Il faut simplement qu'on se concentre sur les jeunes et qu'on les amène à la table des discussions.

Il peut y avoir un financement des voyages pour que ces jeunes viennent, mais il y a également le soutien de la part de plusieurs équipes de l'ICANN qui vont permettre de faire en sorte que cette question de la participation des jeunes fasse partie des priorités.

Donc commencez à parler avec Rodrigo et à voir comment il peut vous aider pour faire en sorte que ce groupe très important, celui des jeunes – les jeunes, c'est ceux qui ont entre 18 et 30 ans à peu près, grosso modo – pour qu'ils puissent participer.

Merci beaucoup. Merci.

DEBORAH ESCALERA: Y a-t-il d'autres questions ?

Bien. J'espère maintenant que les présentations à l'écran vont mieux fonctionner. Notre présentateur suivant, Matthias Markus Hudobnik.

MATTHIAS MARKUS HUDOBNIK: Est-ce que cela fonctionne maintenant ?

Oui. Très bien. Bonjour à tous. Je m'appelle Matthias. Je viens d'Autriche. J'ai étudié le droit et je vais donc parler des réglementations de l'environnement numérique. Nous allons examiner différents concepts : le cyber-libertarisme, le cyber-communautarisme.

Tout d'abord, qu'est-ce que l'espace cyber ? Qu'est-ce que le cyberespace ? Cela peut être assimilé à l'Internet. L'Internet peut être défini par un réseau d'ordinateurs interconnectés. Est-ce que c'est donc l'endroit ou est-ce que cet endroit virtuel qui consiste en toutes les données, les informations ou est-ce que c'est un moyen de support ?

J'ai lu un article de [Orin Esker] qui étudiait cela. Comme vous voyez, il a donc l'opinion de l'utilisateur et on peut aussi étudier le point de vue tel que celui de réseau physique de l'Internet. Cela dépend bien sûr du point de vue de chacun.

Voilà. Cela m'amène à la prochaine question. Est-ce que le cyberespace devrait être règlementé ? L'espace cyber, est-ce que c'est un support ou un moyen ? Comme le disait Mike [inaudible], qui disait que l'espace est donc un nouveau medium, un nouveau moyen, donc ce n'est pas comparable à la

télévision ou au téléphone, ou aux autres sortes de supports ou de moyens de communication.

L'espace cyber dans la définition de [inaudible] était défini comme un espace public tel que celui-ci. Son argument disait que dans le passé les médias, les distributeurs, les personnes qui publiaient les articles n'étaient pas publiés donc dans un espace physique, et maintenant, ce nouvel espace est numérique, donc comporte des caractéristiques différentes.

Qu'est-ce qu'on veut dire par règlementation ? Il s'agit de contrôler, de surveiller les processus ou les comportements selon les requêtes et les demandes de certains protocoles ou normes. Il y a donc deux aspects de règlementation. On peut règlementer les contenus ou les processus. Les régimes de règlementation physique comportent ces deux règlementations. Ensuite, qui doit être responsable pour ces fonctions de règlementation ? Est-ce que ça doit être les gouvernements, les utilisateurs ?

Donc le premier concept a été établi en 1996. Il s'appelait monsieur John Barlow. C'était un libertarien cyber, si on peut dire, et son opinion était que l'espace cyber ne pouvait pas être règlementé. Il y avait donc deux papiers qui ont été écrits là-dessus de John Berry, de David Johnson et David Post.

Et la thèse clé de ces articles était que cet espace cyber ne pouvait pas être règlementé puisque les lois, le droit, étaient contenues à l'intérieur de certaines frontières et que l'Internet n'était pas une loi qui pourrait être efficace dans cet espace cyber. Donc, il nous fallait des règlementations spécifiques.

Il y avait certaines opinions aussi un peu paternalistes de certains professeurs de droits tels que Joël [Inaudible] et de Laurence [Inaudible]. Ils disaient qu'il devrait y avoir un régime de règlementation très puissant et qu'il devrait y avoir une architecture de règlementation.

Donc, cet espace numérique était fait de codes. Donc, il fallait qu'il y ait une loi appropriée. Un exemple est donc un concept de modalité de règlementation. Il s'agit de parler de droits, de normes sociales, de marchés ou d'architecture.

Je vais vous donner un exemple rapide. Par exemple, pour règlementer les cigarettes, il y a eu des droits, des lois qui ont été mises en place avec un âge pour acheter des cigarettes.

Cela voudrait dire que personne ne pourrait… s'il y avait une autre loi aussi qui dirait qu'on ne peut fumer que dans les endroits publics, qu'on ne peut pas fumer dans les endroits privés, etc. Donc cela veut dire que directement on pourrait manipuler le niveau de nicotine des cigarettes, par exemple. Il y

a des tas… Il y a une architecture de droits qui pourrait être mise en place.

En dernier, le concept du communautarisme de raison était en place et discuté par quelqu'un qui s'appelait Andrew Murray, qui disait qu'on pouvait passer du contrôle à la communauté. Dans la plupart des temps, du temps, les régimes de règlementation posaient des problèmes.

Il disait dans son concept que l'utilisateur, par exemple, avait un point actif. Comme vous voyez sur l'écran, il fallait mettre en place une règlementation un peu symbiotique. Il faudrait construire un échange et que la communauté elle-même mette en place une règlementation.

Un exemple, c'est Spotify, parce que dans ce cas-là, beaucoup de personnes utilisent ce service, mais ne téléchargent pas de la musique illégalement. Si vous donnez à la communauté ce qu'ils veulent, Ils ne vont pas utiliser des services illégaux. Du moins, ils vont les utiliser beaucoup moins.

En plus, le dernier argument fait par Andrew Murray. Il disait certains des points bien sûr avaient plus d'autorité que d'autres. Par exemple, les entreprises très influentes telles que Facebook, Google ou Yahoo ont beaucoup d'influence sur la société de l'Internet. Les plus petits points comme vous le voyez sur l'écran : B et C sont des entreprises ou des organisations plus

petites, des sites moins importants qui ont moins d'autorité sur l'Internet.

Pour résumé, Andrew Murray et Collin Scott ont critiqué la théorie de [inaudible] dans leur définition des modalités de règlementation. Comme quoi elles étaient trop élargies, elles échouaient à saisir la véritable essence des modalités de règlementation.

L'opinion cyber-libertarien n'est pas très pratique parce qu'il faudrait règlementer l'Internet et cela pourrait causer des tas de problèmes comme on le sait.

Finalement, j'ai étudié des cas tels que CDB contre newsgroup, newspaper. C'était un cas où il y a eu des informations qui avaient été publiées sur les réseaux sociaux. Il y avait donc eu une injonction contre CDB d'un joueur de football qui s'appelait [inaudible], Ryan [inaudible]. Il s'était plaint parce qu'il s'est dit qu'il y avait beaucoup de commérages sur les réseaux sociaux à son sujet.

Et c'est donc un bon exemple. Parce que dans ce cas-là, la communauté avait pu faire part de son opinion et il était difficile pour le tribunal de passer un jugement. On s'est rendu compte que tous ces processus n'étaient pas utiles.

Merci et si vous voulez, posez-moi des questions.

[Applaudissements]

DEBORAH ESCALERA: Merci Matthias. Y a-t-il des questions dans la salle ?

Très bien. Notre prochain présentateur ou intervenant s'appelle Nertil Berdufi.

Je vous demande un petit moment pendant qu'on télécharge votre présentation.

NERTIL BERDUFI: Bonjour. Je m'appelle Nertil Berdufi. Je viens d'Albanie. Je travaille comme professeur à l'Université [inaudible]. Je vais vous parler aujourd'hui des enquêtes sur la cybercriminalité en Albanie, et c'est lié aux priorités européennes ou sur la convention du Conseil de l'Europe.

Je vais commencer cette présentation avec une photo qui illustre bien les armes qu'on a utilisé dans cette lutte contre la cybercriminalité auparavant et c'est extrait du magazine de l'OTAN, l'édition 2013. Vous voyez la différence entre 1913 et 2013, et en 2013, donc grand changement. Maintenant, on combat avec des armes électroniques, en appuyant sur un bouton.

Et on voit ici au lieu du bouton de la touche entrer, on a une touche cybersécurité. Le directeur de la CIA en 2011, je crois, a parlé d'un nouveau Pearl Harbor qui pourrait être l'objet d'une grande cyberattaque, et ça, ça vous montre bien l'ampleur du problème qu'on a dans le domaine de la cybercriminalité maintenant.

Alors le phénomène de la cybercriminalité, comme on le sait, la cybercriminalité aujourd'hui est l'un des plus grands défis juridiques. La cybercriminalité, c'est une activité criminelle ou [inaudible] qui inclut l'infrastructure technologique de l'information, l'accès illégal, l'interception illégale, l'interférence des données, la falsification électronique et la fraude.

C'est ce qui figure également mot à mot dans la législation de mon pays, l'Albanie. Comme on l'a vu, entre 2000 et 2016, le taux d'expansion d'Internet au niveau mondial a augmenté de 918,3 % et il y a environ 4 milliards de personnes connectées, parce qu'on l'a vu ce matin, on a parlé de 3,7 milliards.

La plupart des délits sont commis par l'intermédiaire d'ordinateurs et toutes les analyses liées à la situation actuelle en Albanie sont liées à des normes juridiques, des mécanismes pour l'enquête et la poursuite des délits de la cybercriminalité, l'identification des problèmes et des défis rencontrés par les enquêteurs et juges, ainsi que les forces de police.

Vous voyez ici les trois piliers clés, à savoir réseau et sécurité de l'information, application de la loi et défense. Chaque pilier ayant ses propres priorités et services de sécurité constitués par la commission, NISAS, RTU, les autorités compétentes, etc.

Et l'aspect national concerne les national threats et les autorités nationales compétentes. On a également au niveau européen : Europol, C-Pol et Euro-Justice. Dans le domaine de la défense, on a des unités nationales de cybercriminalité, et la défense est un autre domaine ou on a un problème avec la cybercriminalité.

L'Union européenne a fait son travail en créant l'agence de défense européenne, qui travaille dans ce domaine, et les nations aussi ont fait leur travail en créant des agences nationales de défense contre la cybercriminalité. Ce qui est très intéressant ici, c'est que le secteur industriel et le secteur académique doivent participer pour créer les outils nécessaires pour lutter contre la cybercriminalité.

Vous voyez ici un graphique qui vous montre qu'en Albanie, on a commencé à lutter contre la cybercriminalité depuis 2008. Avant cette date de 2008, la cybercriminalité n'était pas inscrite dans la loi. Donc il a fallu écrire une législation sur la cybercriminalité et considérer que c'était un délit. À partir de cette date de 2008, on a eu les premiers cas et les premières personnes inculpées de cybercriminalité.

On se prépare à être membre de l'Union européenne et dans ce cadre, on utilise les normes les plus hautes en termes de cybercriminalité. Alors il s'agit d'une information sur les faits et les circonstances relevant du délit criminel qui sont obtenues par des sources fournies par le système juridique et procédurier en termes de délit, conformément aux règles prévues par cette loi et qui sert pour prouver…

Et ça, c'est l'article de notre cour juridique. Vous vous souviendrez que Katharin a parlé du problème de la juridiction. Ça, c'est un gros problème pour nous. La juridiction, ça fait partie de la lutte contre la cybercriminalité. Là, je ne vais pas répéter ce qu'a dit Katharin avant parce que c'était très, très intéressant et très poussé.

Les preuves électroniques. Qu'est-ce qu'on peut utiliser comme preuve ? Comme vous le voyez, il existe des outils comme les smartphones, les PAD, les GPS, etc. Tout ça, ça fait partie des preuves électroniques qu'on peut utiliser.

En Albanie, en 2009, la police nationale albanaise avec l'aide de l'ONU a élaboré un guide pour les enquêtes sur la cybercriminalité concernant la manière de lutter contre la cybercriminalité et de collecter des preuves.

Parce qu'il est très important que les forces de police et les structures responsables de ces enquêtes soient conscientes de ces mesures.

DEBORAH ESCALERA: On va vous demander de ralentir un petit peu pour les interprètes.

NERTIL BERDUFI: En 2014, nous avons créé la première équipe d'enquête sur la cybercriminalité en Albanie avec des spécialistes des forces de police et du bureau du procureur de justice… avec un bureau qui a été créé. C'est la première fois que nous avons créé un responsable pour nommer une personne hautement qualifiée dans cette équipe d'investigation, d'enquête.

Aussi, dans le secteur de l'enquête et lutte contre la cybercriminalité, il y a un groupe de travail constitué par les forces de police. Parce qu'en 2014, on a enregistré plus de 180 délits et 76 ont été élucidés, donc plus de 100 cas n'ont pas été résolu.

Donc ça, c'est un énorme problème pour nous. Ce que j'ai fait également, c'est d'avoir des entretiens avec les personnes les plus importantes dans la lutte contre la cybercriminalité en Albanie – le chef de l'unité d'enquête et de lutte contre la

cybercriminalité – pour essayer de voir comment échanger des informations plus rapidement plutôt que par l'intermédiaire de lettres, de courriers, etc.

Donc une grande solution, c'était d'utiliser Facebook. Ils peuvent ainsi obtenir des informations en deux semaines, et ça, c'est réellement un progrès. Parce que dans notre pays, il y a beaucoup de délits qui sont commis sur Facebook en utilisant Facebook.

Quels sont les défis qui se posent ? Les fournisseurs de services Internet n'ont pas les installations nécessaires pour stocker les informations minimums requises par la loi. Il y a un manque également de ressources humaines et de technologie moderne. La qualification des ressources humaines également est très faible.

Il manque également d'experts pour les enquêtes et la protection des preuves numériques, ainsi que la présentation des preuves devant la justice. Également, l'absence de volonté de coopérer avec les autorités nationales. Chaque nation devrait avoir sa propre équipe d'enquête. Or, ça ne fonctionne pas de cette façon et il n'y a pas d'équipe à proprement parler qui fonctionne de cette façon.

Autre défi qu'on a, conformément aux experts de sécurité, chacune des infrastructures doit disposer d'une stratégie

nationale et nous, jusqu'à présent, nous n'avons pas ces infrastructures de base.

Et même par l'intermédiaire de la formation, on s'aperçoit que les organisations étrangères telles que le FBI, le ISITAP, le PAMECA, etc. … sont hautement qualifiés, ce qui n'est pas le cas du gouvernement albanais. Les personnes formées ne restent pas dans leurs fonctions très longtemps.

Le problème, c'est qu'on peut avoir une personne qualifiée qui fait ses études, etc., à l'étranger, qui devient experte. Ensuite, cette personne vient en Albanie, travaille au même poste et après deux ou trois ans, cette personne s'en va dans le secteur privé ou autre pour obtenir un meilleur salaire ou autre.

Conclusion : la législation albanaise est conforme aux normes européennes et conventions internationales. L'Albanie a signé, ratifié toutes les conventions internationales liées à la cybercriminalité. La législation doit encore être actualisée afin d'être conforme aux conventions ratifiées. Donc, on en est au processus de ratification. On doit maintenant l'incorporer à notre système de procédures au niveau de notre cour pénale.

Également, la prévention est essentielle. On a fait la mise en œuvre. On a rédigé les textes de loi, maintenant il faut les appliquer.

Voilà tout ce que j'avais à vous dire. Merci.

[Applaudissements]

DEBORAH ESCALERA: Merci Nertil. Y a-t-il des questions pour Nertil ?

Merci. Intervention suivante, Olga Kyryluk. Oui, je sais que ce nom de famille est difficile. J'espère que je ne l'ai pas écorché.

OLGA KYRYLUK: Bonjour. Cette discussion a déjà été étudiée par Jackie, Katharin, Krishna et Matthias, mais je vais regarder, observer plus en détail les processus de gouvernance de l'Internet, et pour un peu comprendre où on en est maintenant.

DEBORAH ESCALERA: Si vous voulez bien parler plus lentement pour les interprètes. Merci.

OLGA KYRYLUK: Alors, j'ai donc regardé un peu quels était les processus mondiaux d'institutionnalisation de l'Internet pour voir un petit peu où on en était maintenant, quelle coopération on pouvait observer.

Donc, je suis Olga. Je viens d'Ukraine et je suis ici parce que j'ai été élue pour venir donc en tant que NextGen, boursier NextGen, non alors pas boursier, mais NextGen. Et j'ai choisi ce sujet, car j'ai toujours été intéressée dans ces processus de gouvernance de l'Internet, et aussi parce que c'est devenu une partie de ma thèse. J'ai inclut ça dans ma thèse.

Au cas où vous voulez continuer cette discussion avec moi, vous pouvez toujours me trouver sur Facebook ou sur LinkedIn. Et je reviens donc à mon sujet. Je voudrais commencer par ce qu'a dit [inaudible] et vous le connaissez, c'était comme on l'appelle le fondateur de l'Internet.

Quoi que vous fassiez, tous les pays du monde vont avoir la capacité de se règlementer en interne. N'importe quel pays peut aussi arrêter d'un jour à l'autre. Ce n'est pas une question de problème technique. Ce n'est pas une question de vrai ou de faux. Ce n'est pas une question de gouvernance d'Internet mondiale qui soit vraie ou fausse. C'est juste pour nous. C'est une question pour nous.

Ce n'est pas donc une question d'acceptation. Tout ce qu'on peut faire, c'est vraiment essayer de comprendre quelle est la meilleure manière de gouverner ces processus, d'essayer de rassembler le plus de personnes possibles et de les engager dans ce processus.

Pendant longtemps, c'était la norme que les États ou les pays étaient les seuls qui avait donc le pouvoir de mettre en place les normes pour les relations internationales. Ils étaient donc les seuls et les plus puissants, mais maintenant, ce n'est pas le cas. Il y a plusieurs parties prenantes qui se rassemblent et qui prennent des décisions.

On va essayer de voir l'exemple… des exemples de gouvernances d'internet. J'ai un peu imaginé comme si c'était un mécanisme avec un vélo. Donc si vous avez un vélo et pour qu'il puisse fonctionner, il faut qu'il y ait deux roues, il y a une roue qui va fonctionner rapidement et l'autre va ralentir la première roue.

Donc imaginez que la première roue soit l'exceptionnalisme de l'Internet. Pourquoi cela ? Parce qu'Internet, c'est une structure très unique, qui est mondiale, qui n'a pas de frontières. J'essaie de parler lentement, mais je ne sais pas comment faire.

Donc Internet, c'est vraiment une chose exceptionnelle qui demande un espace et un mécanisme dans un espace pour pouvoir être gouverné. Durant… ce mécanisme… celui qui est donc le plus approprié pour gérer cela est le multipartite, le modèle multipartite.

Ce qui veut dire que chaque partie prenante qui a quelque chose à voir avec l'Internet devrait avoir une opinion et se faire

entendre. Chaque partie prenante a un effet sur les décisions qui affectent l'Internet. Chacun doit avoir le droit de participer dans les processus de gouvernance mondiale.

Donc les deux modèles qu'on a, c'est le modèle multilatéral et multipartite. Je vais commencer donc à parler du modèle multilatéral. C'est le modèle qui est utilisé quand il s'agit de participation et qui est connu depuis assez longtemps. C'est un modèle qui est reconnu à travers l'histoire comme un modèle pour donc gérer les processus mondiaux.

C'est celui qui est utilisé pour l'ITU qui, en ce moment, essaie de participer à la gouvernance d'Internet, et cela est basé sur la souveraineté des États. Cela ne donne pas assez de possibilité pour que toutes les parties prenantes soient intéressées par la gouvernance d'Internet.

L'idée, c'est d'influencer l'écosystème de l'Internet en mettant en place des conférences plénières pour essayer d'élargir ces notions qui ont été utilisées par d'autres institutions telles que… qui ont essayé de contrôler Internet au niveau de la gouvernance d'Internet.

On va parler aussi de l'UNESCO qui est bien connue pour ses programmes sur l'éducation et qui essaie de rendre Internet multilingue pour que toutes les personnes à travers le monde

puissent comprendre et recevoir les informations à travers Internet.

Dans ce sens, les IDN font du bon travail, parce qu'ils aident les personnes à accéder aux contenus dans leur langue régionale. On va aussi parler de l'organisation sur la propriété intellectuelle mondiale qui travaille sur ce sujet aussi.

Il y a aussi le partenariat gouvernemental ouvert dont on ne parle pas beaucoup. Ils ont des initiatives en place, et en ce moment, cela consiste en 75 pays du monde qui travaillent ensemble. Ils essaient de rendre les opérations de chaque État un peu plus transparentes. Ils essaient de démontrer que les États peuvent faire beaucoup pour que les gens, les personnes, puissent exercer leurs droits.

Et pour moi, la conférence qui m'intéresse le plus, c'est ce qu'on appelle la Conférence de l'Internet mondial. C'est un sommet qui a eu lieu en Chine. Cela fait trois ans que cela prend place et c'est une conférence intéressante puisque la Chine nous dit qu'elle a son propre, est partie prenante dans la gouvernance d'Internet sur la scène mondiale.

On sait très bien que les problèmes de cybercriminalité ont un rôle… doivent être étudiés dans l'espace Internet.

Toutes ces études doivent être complémentaires. Quand on parle de sécurité, on ne parle pas qu'avec la sécurité vient la surveillance et cela…

Quand on parle de vie privée, on parle… On ne vous dit pas que vous pouvez faire tout ce que vous voulez. Vous avez des droits, mais ces droits-là ne doivent pas dépasser les droits des autres personnes.

Ensuite, on passe au prochain modèle qui est complétement différent. Il s'agit du modèle multipartite. Il est basé sur la participation de toutes les parties prenantes et c'est pour cela qu'on l'appelle multipartite. Cela a commencé entre 2003 et 2005 avec [inaudible] même si ça a suivi une initiative de l'ITU, mais c'est quand même…

C'était la première fois que la gouvernance d'Internet a été étudiée. À EuroDIG aussi, l'initiative avait été mise en place. À Netmondial au Brésil aussi, on s'est rendu maintenant que cela devait… On s'est dit que ça allait remplacer l'IGF, mais ça n'a pas été le cas. Notre modèle préféré donc, c'est l'ICANN. Et c'est l'organisation qui a un gros potentiel pour bien sûr suivre tous ces processus.

C'est ce qui s'est passé il n'y a pas très longtemps ici sur l'écran. On a vu la transition de la supervision d'IANA, de la NTIA à la communauté multipartite mondiale. On s'est rendu compte

qu'il fallait qu'on ait beaucoup de règlementation, de transparence, de responsabilité et d'ouverture pour l'avenir.

Une autre raison… Une autre de mes raisons dans mon choix de ce sujet était que j'avais étudié un petit peu cette révision qui avait été faite sur la responsabilité à l'ICANN. Si pour moi il y avait une opportunité de participer à ce processus, j'en serais très ravie. Je n'ai pas beaucoup plus de temps.

Mais comme vous voyez sur la photo, sur l'écran, vous voyez ici…. [Inaudible] croyait en ce monde interconnecté, mais on doit se poser la question, est-ce que c'est un espace sans frontières ou un endroit sans frontières ?

Si c'était mon choix, moi, j'aimerais choisir ce modèle multipartite, ainsi toute personne et toute partie prenante auraient son mot à dire. Merci.

[Applaudissements]

DEBORAH ESCALERA: Une question pour Olga ?

Non. Donc notre prochaine intervenant, c'est Peter Cihon. Parlez donc lentement pour les interprètes. Merci.

PETER CIHON: Bonjour à tous. Je m'appelle Peter Cihon. Je suis étudiant à l'Université de Cambridge et je travaille sur les politiques des sciences informatiques et technologiques. Maintenant, je suis boursier pour Learn Asia, un groupe de travail qui se concentre sur la technologie des nouvelles technologies en particulier dans l'Asie Pacifique.

Et je travaille surtout sur le taux zéro. Pour ceux qui ne connaissent pas ce zero rating en anglais (taux zéro), 'est une pratique opérée par les opérateurs de téléphonie mobile. Donc, ils offrent des données gratuites, mais avec un contenu limité. On parle de données mobiles.

Cette caractéristique de taux zéro est utilisée pour un certain nombre de raisons, mais dans un marché compétitif surtout dans les pays du Sud. On l'a utilisé pour l'accès au développement. L'infrastructure du réseau est en place pour servir environ 70 % de la population mondiale, pour connecter environ 70 % de cette population à l'Internet aujourd'hui. Toutefois, aujourd'hui 45 % de cette population est en ligne.

Ce qui montre bien qu'il y a une préoccupation en termes de coût, et pour les gens qui y ont accès… Les gens ne comprennent pas bien quel est leur intérêt, dirais-je, d'avoir accès.

Ce qui nous amène à l'idée d'un contenu gratuit par rapport à l'accès en termes financiers et à ce que peut m'apporter d'avoir accès à Internet. Et ça, c'est un peu controversé. Vous vous souviendrez de la version la plus connue de zéro rating dans le monde et il y a d'autres versions dans le mode.

Facebook, non pardon, Wikipedia free. Ça, c'est une autre option bien connue. Donc, ce débat se concentre autour de l'idée d'un jardin emmuré, donc si les gens pour la première fois ont accès à quelque chose qui est limité et ils ne s'ouvrent pas vers d'autres choses plus ouvertes.

Et ça, c'est un débat sur la neutralité du net qui a lieu au niveau international. Peut-être que certains d'entre vous savent qu'en Inde il y a eu un cas en 2016 bien connu. Mais je dirais que ce débat se concentre surtout sur des hypothèses empiriques.

Question essentielle en particulier, lorsque les gens se connectent avec free basics, est-ce qu'ils le font dans le cas de ce jardin emmuré ou dans le cas de free basics ? Donc, dans ma recherche, je me suis concentré sur le cas de [inaudible]. Ça a fait l'objet de ma recherche.

Au cours des dernières années, on a commencé depuis 2012, le marché de la téléphonie mobile a changé puisque le prix… On a vu une pénétration de la téléphonie mobile beaucoup plus importante, au-dessus des 90 % depuis l'année dernière. En

Asie, il y a une enquête qui a été faite et qui a placé ce chiffre à 83 %.

Mais cette disparité mondiale entre le réseau, l'accès au réseau et l'utilisation d'Internet continue d'être présente à Myanmar aussi. Seuls 40 % de ceux qui ont accès se connectent effectivement à Internet. Et donc, zéro rating, le taux zéro, c'est une option qui a été utilisée par les opérateurs de télécommunication à Myanmar en particulier.

Donc, en 2016, on a Facebook free basics qui a été lancé. Certains d'entre vous le connaissent certainement, et je devrais expliquer ce qu'est la free basics. Il s'agit de Facebook sans images et sans vidéos, et c'est gratuit.

Messenger gratuit et un certain nombre de pays qui offrent Wikipédia, l'UNESCO et d'autres contenus sponsorisés par l'ONU. Ça, c'est free basics.

Ensuite Télénor, un autre opérateur à Myanmar, a lancé un mois après pour rentrer en concurrence avec free basics. Et leur promotion était un petit peu différente. En termes de structure, ils offraient un accès à Facebook totalement gratuit avec contenu libre.

Pour 150 mégabits par jour et tax free sur Viber. Donc, ma recherche a consisté à voir comment les gens utilisaient ces

outils. Donc, je me suis concentré sur la région de [inaudible] avec des groupes cible, 8 dans les villes et 2 dans des villes autour ou des villages autour de ces villes.

Donc, j'ai choisi un échantillon de personnes, ceux qui utilisent les données Internet et qui représentent un échantillon plus large.

Et j'ai également organisé des entretiens avec plusieurs parties prenantes pour voir quelles sont les parties prenantes à Myanmar. Alors, j'en arrive aux principales conclusions. J'en ai surtout trouvé trois, mais je vous invite à consulter ma recherche pour plus de détail.

Même si free Facebook est vu comme un moyen pour introduire les gens à Internet pour la première fois, il s'avère que dans la pratique on n'a pas atteint cet objectif. Et à Myanmar, ceux à qui on a parlé ne connaissaient pas que Facebook free basics, c'était plus que Facebook.

Donc, ça peut être lié à la manière dont ça a été vendu là-bas, c'est-à-dire qu'on vendait cette promotion comme Facebook gratuit point. Donc je dirais qu'étant donné cette compréhension, même si c'est permis dans le monde, il est important que les juridictions analysent la manière dont c'est vendu avec un œil critique.

Autre conclusion importante : les choix en termes de conception, en termes de construction de promotion et d'interphase, et ça, c'est très important pour voir comment les gens utilisent les offres ou les promotions. Donc, les deux offres qui ont ce contenu très limité en termes de vidéo étaient très différents de l'autre offre de Télénor.

Avec free basics MPT, parce qu'il n'y avait de contenu vidéo ni photo, les gens se sentaient obligés de passer sans arrêt du service gratuit au service payant.

Facebook sans ce contenu visuel, c'est un petit peu comme un curry sans sauce. Il manque un petit peu la carotte. Donc, ils ne cessaient de passer du service gratuit au service payant et donc ça a fait que beaucoup de gens ont cessé d'utiliser ces services et d'autres se sont sentis restreints dans l'utilisation de ce service.

Ils voulaient continuer à être en contact avec les gens, donc ils utilisaient la version gratuite de manière temporaire. Et cette limitation en termes de contenu a amené les gens à comprendre relativement bien quand est-ce qu'ils utilisaient un service gratuit par rapport au service payant.

Et ça, c'est très différent par rapport à l'offre Télénor. Parce que dans le cas de l'offre Télénor, les gens utilisaient beaucoup

l'offre. Donc, certaines personnes pour la première fois faisaient l'expérience des vidéos grâce à cette promotion.

Donc, il y a eu un effet inattendu qui est lié à Facebook. Les gens utilisaient plus de données, mais ils restaient dans ce jardin emmuré. Donc, il y avait des données gratuites pour Facebook qui s'opposaient à des données gratuites au sens plus large, sans être vraiment explicite par rapport aux limitations qui étaient contenues.

Donc, on a analysé la conception dans l'interface, mais aussi voir si vraiment ce contenu est suffisamment ouvert ou pas.

Toutefois, lors des entretiens, je me suis aperçu que la plupart des personnes interviewées n'avaient pas accès aux contenus à taux zéro, que beaucoup de gens utilisaient d'autres applications comme Google, [inaudible] qui est une application de messagerie très populaire à Myanmar.

Et autre conclusion importante, même si les gens utilisaient énormément Facebook et utilisaient énormément ces promotions. Ils souhaitaient également sortir de ce jardin emmuré.

Et dernière conclusion, la plus importante pour l'ICANN en particulier, c'est l'idée selon laquelle ceux qui se connectaient

utilisaient davantage les applications que les navigateurs. Donc, ils n'utilisaient pas un navigateur pour avoir accès à Internet.

Ils le faisaient par l'intermédiaire de l'application et ça c'est particulièrement important pour l'ICANN et ce à deux titres. Parce que ces derniers jours, on entend beaucoup parler de l'utilisateur final. Qui est cet utilisateur final et comment incorporer l'utilisateur final au modèle multi parties prenantes ?

Et je dirais que pour… Il faudrait séparer l'utilisateur final de la mission de l'ICANN. Donc, si personne ne tape une URL dans un ordinateur et se concentre uniquement sur une application, ça, ça réduit le rôle de l'ICANN pour cette nouvelle personne.

Donc, je pense que comme le PDG de l'ICANN l'a dit ce matin, pour augmenter l'universalité de l'ICANN, ça c'est un défi important à relever : continuer à être pertinent et essayer de rechercher ces nouveaux utilisateurs. Et deuxièmement, je pense que ça pourrait peut-être nous amener, ici à l'ICANN, à définir plus facilement ou clairement ce que sont les applications et voir qui sont les personnes qui utilisent les domaines, les applications.

Ça, c'est peut-être une solution de facilité qu'on va être amené à prendre ou à adopter. Voilà ce que j'avais à vous dire. Si vous voulez obtenir plus de détail sur ma thèse, et bien n'hésitez pas à me trouver sur Twitter.

DEBORAH ESCALERA: Merci Peter. Y a-t-il des questions ?

Bien. Présentation suivante, Valeriia Filinovych.

VALERIIA FILINOVYCH: Je m'appelle Valeriia Filinovych. Je suis ukrainienne. J'ai un doctorat en droit et je suis professeure à l'université. Je suis spécialisée en droits sur la propriété. Et je vais parler des problèmes de règlementation nationale des noms de domaine en Ukraine.

Je vais aussi parler des atteintes aux droits d'auteurs.

Donc, les noms de domaine. Tout d'abord, on veut voir les problèmes dans le sens où on a donc des problèmes de règlementation nationale sur la délégation des droits sur les noms de domaine en Ukraine. Il n'y a pas de législation spécifique sur le transfert de ceux-ci en Ukraine. Ce transfert est seulement une concession de droits sur ces noms de domaine.

Et ces droits prennent place au moment de la conclusion du contrat pertinent entre le propriétaire potentiel et le bureau d'enregistrement. Le prochain problème est celui-ci. Regardez cette diapositive. C'est un formulaire qui devrait être rempli pour pouvoir donc enregistrer un nom de domaine en Ukraine.

Il est très inconvénient. Tout d'abord, pour enregistrer un nom de domaine dans UA, il faut une marque avant de s'enregistrer. Si vous n'avez pas une marque déposée pour le domaine dont vous avez besoin, vous n'allez pas pouvoir l'obtenir.

Mais si vous voulez enregistrer un domaine de plus bas niveau, comme avec .EA, etc., votre processus d'enregistrement est très, très souple. Vous n'avez seulement besoin que de quatre choses. Tout d'abord, vous avez besoin d'inscrire votre nom et prénom, même s'il est faux puisque personne n'ira vérifier.

Vous avez besoin d'un numéro de téléphone au cas où vous oubliez un jour votre mot de passe et que vous voulez le récupérez. Vous devez avoir une adresse courriel et ensuite tout ce que vous avez à faire, c'est d'être en accord avec les termes du contrat. Telle situation d'enregistrement pose un problème.

Tout d'abord, personne… Toute personne peut enregistrer donc un domaine très facilement et mettre du contenu illégal sur le site à travers ce domaine. Le prochain problème est celui-ci : la preuve d'identité de la personne qui pourrait porter atteinte devient une cause très compliquée puisqu'on ne sait pas qui est qui. Qui sera le propriétaire potentiel de tel ou tel domaine ?

Le prochain problème est-celui-ci : l'UDRP n'est pas applicable en Ukraine. Un de nos domaine .UA a présenté donc une

proposition pour rendre cette politique acceptable, mais cette proposition n'a pas reçu de soutien.

Donc, nos citoyens doivent défendre leur propre droit par les moyens traditionnels, légaux connus chez nous. Si on compare cela avec l'UDRP, on voit que ce moyen donc de défendre ses droits à travers le système traditionnel est beaucoup moins cher et plus rapide pour tout le monde.

Donc, il y a des choses qui devraient être faites pour régler les problèmes dont je vous ai parlés. Tout d'abord, on devrait pouvoir fournir des procédures plus strictes pour l'enregistrement des domaines, qui devraient consister en une vérification obligatoire de toutes les données personnelles du propriétaire du domaine.

Par exemple, en Russie, vous devez fournir une copie scannée de vos papiers d'identité, tels qu'un passeport, pour pouvoir obtenir un nouveau domaine. Ils ont aussi un règlement qui dit aussi que les noms de domaine ne devraient pas contenir du langage abusif ou du contenu abusif. Dans ce cas-là, l'enregistrement n'est pas possible.

Chez nous, nous n'avons pas de législation à ce sujet, mais nous avons des réglementations qui sont mises en place par des entités qui sont non-gouvernementales, et ces réglementations temporaires sont en place. Ces réglementations contiennent

une liste de données qui ne doivent pas être contenues dans le domaine.

On devrait crier, créer – pardon – un registre national uniforme de tous les propriétaires de nom de domaine dans la zone du domaine national .ua, en incluant bien sûr le régional tel qu'org.ua ou kiev.ua, etc. On devrait aussi élaborer des réglementations spéciales qui pourraient mettre en place des règles et réglementations sur l'enregistrement du nom de domaine.

Est-ce que j'ai assez de temps ? Je vais maintenant parler des atteintes au droit d'auteur sur l'Internet, en Ukraine. Tout d'abord, je voudrais souligner que les moyens pour pouvoir prouver ces atteintes aux droits de l'auteur sur l'Internet en Ukraine…

Devant la Cour suprême en Ukraine, il y a le fait qu'on doit apporter des preuves d'atteinte aux droits d'auteur sur l'Internet. Ce sont, par exemple, des pages imprimées du web. Mais toutes ces pages ne sont pas forcément acceptées en tant que preuve. Ces pages doivent être vérifiées par une institution ou par une personne autorisée dans sa juridiction. Elles doivent être scellées avec le sceau officiel d'un des membres états.

Quand il s'agit des vidéos ou des bandes audio, on sait qu'elles doivent contenir le processus de recherche à travers le site web

par une personne intéressée et qu'elles doivent être faites d'une façon électronique ou sur un autre transport matériel pour être soumises devant le tribunal. Ces bandes doivent indiquer le temps, les conditions dans lesquelles elles ont été enregistrées, et elles doivent contenir les données de la personne qui l'ont créée.

Il doit y avoir un certificat qui doit être reçu de la part des fournisseurs de réseaux et autres services de recherche.

Désolé.

Alors les choses qu'on devrait faire pour pouvoir défendre donc les droits d'auteur sur Internet. Tout d'abord, il faudrait faire des mises à jour de la liste des objets de droits d'auteur. Cette mise à jour doit être faite avec les données sur le site. Notre code civil devrait ajouter une liste des directives spécifiques sur les responsabilités, sur la violation des droits de la propriété privée à travers, sur l'Internet et contenir aussi toutes les informations intermédiaires des propriétaires et des utilisateurs sur ce site, sur le site.

Ensuite, on devrait développer un ensemble commun de contrats sur la création du site web qui fournit des services hôtes dans le cas de l'enregistrement des noms de domaine. On devrait pouvoir donc créer un système unifié de protection pour les droits d'auteur.

Ensuite, les fournisseurs devraient devenir responsables pour superviser les documents qui sont téléchargés par les utilisateurs. Les personnes qui portent atteinte à ces droits d'auteur devraient être poursuivis.

Ensuite, on devrait emprunter certaines des provisions que l'on trouve dans le SOPA aux États-Unis qui permet de bloquer des domaines et on devrait aussi utiliser le modèle [inaudible] pour l'échange des données sur les atteintes aux droits d'auteur entre les gouvernements et les organisations commerciales.

Merci.

[Applaudissements]

DEBORAH ESCALERA: Merci. Y a-t-il des questions ?

PERSONNE NON IDENTIFIÉE: Quand vous avez parlé des droits de protection pour les atteintes aux droits d'auteur, toutes ces choses sont-elles vos idées ? Ce sont des suggestions de votre part ?

VALERIIA FILINOVYCH: Oui, j'ai donné certaines de mes suggestions sur la diapositive.

PERSONNE NON IDENTIFIÉE: Les données dont vous parlez sont très controversées.

VALERIIA FILINOVYCH: Quand il s'agit des données qui sont téléchargées sur Internet, sur les pages Internet, je donne certains exemples à mes étudiants. Je leur dis qu'il y a des endroits sur les sites auxquels il faut faire attention, puisqu'il y a des données qui sont là. Il faut toujours vérifier les informations des propriétaires des sites web. Il faut faire attention, parce qu'il y a des choses qui sont dangereuses.

Il faut qu'ils aillent voir qui est le créateur du programme informatique pour tel ou tel site. Il faut qu'ils aient accès au contrat utilisateur et toutes les choses qui peuvent être faites ou ne pas être faites.

PERSONNE NON IDENTIFIÉE: Donc, ça n'a rien à voir avec des sites web de parties tierces. Vous dites que les fournisseurs hôtes devraient faire attention aux atteintes aux droits d'auteur. Non, ce n'est pas grave. Tout ça est bien compliqué.

VALERIIA FILINOVYCH: Oui, je suis désolée. Je suis très nerveuse. Je ne peux plus rien dire.

DEBORAH ESCALERA: Oui, je pense que Valeriia pourra peut-être échanger des courriels avec vous pour pouvoir s'expliquer. Merci Valeriia. Y a-t-il d'autres questions ?

Notre dernier intervenant ou présentateur s'appelle Yousra Hsina.

YOUSRA HSINA: Bonjour. Ma présentation va porter sur les fournisseurs de services Internet et la protection de la vie privée en ligne.

DEBORAH ESCALERA: Veuillez parler bien fort dans le micro et lentement.

YOUSRA HSINA: Je vous disais que ma présentation va porter sur les FSI et la protection de la vie privée en ligne. Nous savons tous que les réseaux sociaux et les sites web sur lesquels on va contiennent des informations qui nous concernent et qui les utilisent à des fins de publicité. Toutefois, on ne prend pas toujours conscience que les FSI (les fournisseurs de services Internet) peuvent également collecter des informations sur nous.

Le fait est que vous pouvez choisir d'aller sur un site web ou pas, de participer aux réseaux sociaux ou pas. Mais une fois que vous choisissez un FSI, c'est différent.

Parce que lorsque vous choisissez un FSI, il n'y a aucune manière de revenir en arrière. L'utilisateur n'a pas la possibilité de changer d'avis et il ne peut pas échapper à ce réseau. Pensez-y une seconde. Votre fournisseur de services Internet gère tout le trafic de votre réseau, ce qui veut dire qu'il a un aperçu très large de tout ce que vous faites sur Internet : les sites web que vous visitez, les applications que vous utilisez, tout.

Toutefois, on ne peut pas remettre en compte, en cause, pardon, qu'aujourd'hui les FSI sont limités d'une certaine manière par certains développements technologiques, tels que les VPN, les protocoles d'encryptage et la multiplicité et la diversité des outils. Bien entendu, aujourd'hui, personne n'a un seul outil technologique, mais plusieurs.

Donc, je vais revenir aux VPN. Lorsque vous utilisez des VPN, l'ordinateur de l'utilisateur crée un code encrypté en fonction du VPN et en fonction du VPN utilisé, on peut utiliser un message au serveur VPN.

L'autre problème, c'est que même si les VPN ont été, existent depuis longtemps, ils ne sont pas beaucoup adoptés. Ils ne peuvent pas non plus fournir une protection totale aux

utilisateurs. Pour ce qui concerne les protocoles d'encryptage, on est encore très loin d'un véritable encryptage, parce que si vous comparez, pardon, le trafic sur Internet qui est encrypté au trafic non encrypté, vous vous apercevrez que le dernier est plus important que le précédent.

La structure de l'Internet qui n'est pas encryptée n'est pas d'utilité pour ce qui concerne la protection de la vie privée des utilisateurs. Je vais vous donner l'exemple d'une catégorie de recherche qui est celle de la santé, les achats et l'utilisation.

Les études ou les statistiques ont démontré que plus de 85 % des principaux sites qu'on visite ne peuvent toujours pas, n'adoptent toujours pas de protocoles d'encryptage sur le site web. Donc bien entendu, les FSI peuvent avoir tout type d'informations. Par exemple, lorsqu'on cherche des produits médicaux, des conseils médicaux, ou quand on achète un produit quelconque.

Autre aspect important dans la même veine, c'est que même avec le HTTPS, le FSI peut encore obtenir des informations sur l'utilisateur. Parce qu'avec le HTTPS, le FSI peut continuer à voir le site web visité par l'utilisateur. Et ça, ça peut être très révélateur. Donc même avec les sites web encryptées, les FSI peuvent avoir accès à beaucoup de données sensibles concernant les utilisateurs.

Et un groupe de chercheurs informatiques ont découvert que les FSI peuvent avoir accès à un grand nombre de contenus concernant leurs utilisateurs, des contenus cryptés, pour être plus précise, sans les casser, mais simplement en analysant les caractéristiques du paquet tel que le temps, la destination.

Les FSI peuvent en apprendre beaucoup sur les habitudes de leurs utilisateurs. Par exemple, identifier les sites web visités et d'autres informations concernant les contenus consultés.

Maintenant, je vais vous parler de l'aspect réglementaire en prenant l'exemple spécifique des États-Unis. Les utilisateurs Internet aux États-Unis l'année dernière ont vu un changement lorsqu'il y a eu une réglementation adoptée par la NTIA, l'année dernière donc.

Une réglementation qui stipulait que les FSI, devaient avant de partager des informations sensibles sur leurs utilisateurs, devaient d'abord obtenir l'autorisation de leurs utilisateurs afin de pouvoir partager ces informations. La règle impliquait que les FSI devaient protéger ces informations sensibles des utilisateurs et devaient spécifier certaines mesures techniques pour y parvenir.

Et ça, c'est un exemple. C'était censé être un exemple de réussite. Malheureusement, ça ne l'est pas, parce que la réglementation devait entrer en vigueur il y a deux semaines,

mais ça n'a pas été le cas. Parce que les gens se sont plaints du fait que les fournisseurs de services Internet et d'autres grandes entreprises en ligne ont également accès à nos informations. Donc la question qui s'est posée est la suivante.

Est-ce que les réglementations en termes de la protection de la vie privée du gouvernement protègent les données sur l'Internet des consommateurs de l'invasion de la part des entreprises d'Internet ou seulement quelques-unes ? La réponse est la réponse B, bien sûr. Le problème, c'est que ce qui a été remis en cause, d'autres entreprises en ligne telles que les moteurs de recherche, les sites web et les systèmes d'opération de téléphone portable n'appliquaient pas cette règlementation, n'étaient pas concernés par cette réglementation, simplement les fournisseurs de services Internet.

Donc, il s'agissait d'une certaine forme de discrimination à l'encontre des FSI et ça a été contesté. Ça n'a pas été adopté, cette réglementation.

Donc là c'est ce que je vous ai dit : intrusion FSI dans la vie privée en ligne, qui est aussi importante que les FSI. Donc il est clair qu'il reste encore beaucoup de chemin à parcourir pour réglementer les FSI. Ça requiert du temps et c'est encore un sujet polémique.

Et je conclurais en vous rappelant ce que veulent les consommateurs, ce que nous voulons, c'est de la cohérence, de l'uniformité, de la simplicité et de la transparence. Merci.

DEBORAH ESCALERA: Merci beaucoup, Yousra. Des questions dans la salle ?

Alors ça, ça a conclu nos présentations de la journée pour le public. Je remercie le public de nous avoir accompagné et on va poursuivre avec les questions des membres NextGen. Rachel ?

[RACHEL]: Je ne sais pas si je pourrais faire des commentaires généraux sur le déroulement de la journée jusqu'à présent. Je vais essayer d'être rapide.

D'abord, oui, je voulais intervenir sur les présentations. Je peux le dire devant le public. Il n'y a pas de problème.

Donc, je voulais simplement dire aux quinze membres NextGen les féliciter, les remercier de leurs efforts. C'était très intéressant. J'ai beaucoup appris sur beaucoup de sujets que je ne connaissais pas : blockchain et d'autres technologies que je ne connaissais pas. Donc, ça a été réellement intéressant.

Je voulais faire un petit commentaire ou un ajout sur ce qui a été dit, parce je travaille dans ce domaine, sur la diapo sur le

modèle multipartite et le modèle multilatéral. Ajouter, parce que je travaille à l'UNESCO. C'est une institution multilatérale qui a adoptée fortement le modèle multi parties prenantes. Donc, peut-être que vous pourriez l'ajouter dans la liste des aspects positifs dans votre présentation.

Ensuite, un commentaire plus général qui s'Inspire de mon travail dans le domaine de la liberté d'expression. Je pense que, dans certaines des présentations, il y avait des idées qui ont été présentées très intéressantes. C'est toujours important d'avoir un nouveau point de vue, e nouvelles idées, sur certaines questions qui ont peut-être des incidences, des implications en termes de droits de l'homme. Par exemple, quelle incidence ça aurait en termes de liberté d'expression, en termes de droits de l'homme ? Le fait que des noms de domaine soient fermés.

Donc toutes ces questions n'ont peut-être pas été suffisamment creusées, toutes ces implications en matière de droits de l'homme. Il y a une séance cet après-midi à 15 h 15 avec les commissaires chargés de la protection des données personnelles.

Ça, ça va être une séance très intéressante à 15 h 15. Et d'une manière plus générale, une suggestion : faire des commentaires et apporter votre expérience et vos idées, mais aussi être ouvert aux autres points de vue. Si, vous, vous avez de l'expérience

dans le domaine des droits de l'homme, de la sécurité, etc., écoutez vos collègues, soyez ouverts à leurs arguments, parce que pour moi, pour que ce modèle multi parties prenantes fonctionne, il faut parvenir à un compromis et écouter les autres.

Par rapport à cette question de la participation des jeunes qui a été évoquée, je pense que ça touche une question critique. Moi, j'ai le sentiment qu'on peut effectivement participer à distance.

Mais on peut aussi faire en sorte que les jeunes participent et aient une interaction face à face, physique, qu'ensuite il y ait une participation en ligne, par email, etc. Donc, je voulais simplement me montrer solidaire vis-à-vis du programme NextGen, parce qu'il me semble que c'est une initiative très importante.

Et le PDG de l'ICANN l'a dit hier, les jeunes sont l'avenir de l'Internet, de la gouvernance de l'Internet. Donc l'ICANN a besoin de vous et merci de tous vos efforts. Merci.

DEBORAH ESCALERA: Andrea, avais-tu des questions ?

[ANDREA]: Est-ce que les membres NextGen peuvent rester dans la salle, parce que j'aimerais discuter de certaines choses avec vous.

DEBORAH ESCALERA: Est-ce que vous avez des questions encore, membres NextGen, à l'attention des autres membres ? Sur les présentations, vous avez des questions ? Allez-y.

PERSONNE NON IDENTIFIÉE: Question stupide : serait-il possible d'avoir toutes les présentations qui ont été faites ?

[Discussion hors micro]

DEBORAH ESCALERA: Y a-t-il d'autres questions à l'attention des autres membres NextGen ? Carolina.

CAROLINA MATAMOROS: Merci de cet espace qui nous a été réservé pour poser des questions. D'abord, je voulais parler de la présentation faite par Desara sur la pornographie infantile. J'aimerais savoir du point de vue des poursuites judiciaires : est-ce que ça nous permet de

savoir où le délit a été commis ? Comment est-ce que ça se produit, cette poursuite judiciaire ?

Si je fais un parallèle avec les drogues, en général, il y a des poursuites vis-à-vis de la production et de la commercialisation, ainsi que de la consommation. Donc, j'aimerais savoir comment ça se passe dans le cas de la pornographie infantile et des délits commis à l'encontre des enfants.

DESARA DUSHI: Ça dépend des législations nationales de chacun des pays. Mais en général, on pénalise la production et la consommation.

DEBORAH ESCALERA: Allez-y. Présentez-vous, s'il vous plait.

PETER CIHON: Peter Cihon. J'ai une question sur le blockchain et sur votre travail sur le projet Tech 40 et tout le projet que vous avez fait pour faciliter le travail des ONG. Je ne suis pas expert, absolument pas, dans ce domaine. Mais j'ai l'impression que ce blockchain peut aider à la concurrence dans les transactions et faciliter les transactions. Mais est-ce que ça permet de régler un problème, qui me semble central, le financement des ONG, c'est-à-dire une fois que la transaction est faite, une fois que les

fonds arrivent, comment est-ce que vous vérifiez que ces fonds sont utilisés aux fins qui étaient prévues ?

En d'autres termes, une fois que l'ONG obtient ce financement, est-ce que le blockchain peut vérifier que ces fonds sont utilisés de la manière dont l'ONG est censée les utiliser ?

ABDERRAHMAN AÏT ALI: Merci Peter. C'est une excellente question que tu viens de poser. Ce qu'on fait en fait, parce qu'il y a une phase d'utilisation de blockchain pour, comme un moyen dans les contrats. Il y a ensuite d'autres fonctions qu'on a ajoutées à cet outil. D'ailleurs, on en est aux premières étapes du développement de cet outil. On est en train encore de le tester, cet outil.

On a un prototype pour l'instant et on a une ONG qui travaille avec les réfugiés en Syrie, à la frontière avec la Turquie. Donc ce qu'on fait d'abord, c'est qu'on utilise le blockchain [inaudible]. Donc, on n'a pas choisi notre propre logiciel blockchain, parce qu'il y a déjà beaucoup de FSI pour [inaudible].

Donc, on a utilisé cela et les ONG obtiennent des financements de la part de plusieurs bailleurs de fonds. Et une fois… Parfois il y a des financements multipartites, et ensuite, on lance le premier niveau de financement. Lorsqu'il est terminé, on l'arrête et lorsque l'ONG obtient le financement, une fois que c'est sur le

terrain, il y a un processus de suivi de l'ONG et de ses activités. Donc ça, dans le prototype, il y a une plateforme de retour d'Informations et ensuite, on passe au niveau suivant du financement et ainsi de suite jusqu'à ce que le projet soit totalement financé.

Ça, c'est notre suivi. Et bien entendu, notre prototype est ouvert à des fonctions supplémentaires en fonction des réactions ou des commentaires qu'on obtiendra de la part des ONG, mais également des bailleurs de fonds qui nous permettront d'ajouter de nouvelles fonctions.

Mais en tout cas, à l'heure actuelle, c'est à ça que ressemble le prototype.

OLGA KYRYLUK: Ce qui… Quand j'ai parlé de l'UNESCO, je voulais vous dire qu'il y a la différence dont vous parlez entre les deux modèles est basée sur une organisation qui va, qui est maintenant sur une voie différente et qui est en train de faire des changements.

C'est donc la tendance maintenant. Je sais que ce modèle dont vous parliez a été utilisé pendant longtemps, mais maintenant, ils essaient d'utiliser donc un nouveau modèle. Ce modèle multipartite avait été conçu pour que toutes les parties prenantes soient représentées.

CLÉMENT GENTY: Clément Genty de France. Je fais un doctorat sur l'évaluation des noms de domaine et je pensais au .ua qui disait qu'en Ukraine, l'UDRP n'était pas appliquée, qu'il leur fallait un système de contrat.

Je me souviens que ce sujet a toujours été un problème depuis 1985. Il y a trois ans, si je me souviens bien, l'ICANN a lancé un programme de nouveaux gTLD et nous avait dit qu'en deux ans, il y aurait beaucoup de gTLD. Maintenant, nous en sommes à 3 000 et quelques gTLD. Donc est-ce que c'est utile maintenant, en 2017, de développer des ccTLD ? Est-ce que c'est intéressant de développer un ccTLD quand vous savez que vous pouvez créer un nom de domaine avec un lien et un sujet tout simplement.

VALERIIA FILINOVYCH: Les politiques de l'UDRP seraient suffisantes pour les résolutions de nom de domaine en Ukraine, mais la proposition d'hôte master dans l'administration du nom de domaine public .ua n'a pas été approuvée. Donc peut-être qu'ils devraient encore une fois fournir une nouvelle version, un nouveau projet pour pouvoir évaluer la situation pour qu'il y ait donc approbation.

DEBORAH ESCALERA: Y a-t-il d'autres questions ? Peter, vous avez quelque chose à dire ?

JACQUELINE EGGENSCHWILER: Jacqueline au micro. J'ai une question pour Carolina au sujet du triangle qu'elle nous a montré. J'ai une question de haut niveau. Pensiez-vous à des mécanismes de coordination qui pourraient donc faire face à ce diagramme de défense et de sécurité d'un côté et de l'Internet, de l'autre côté, et de l'autre élément dont vous avez parlé.

CAROLINA MATAMOROS: Oui, vous avez raison. Comme vous le savez, maintenant, j'ai amené ce sujet sur la table à l'ICANN, parce que je sais qu'ils auront l'opportunité d'obtenir cet espace. Certaines organisations sont préoccupées de la sécurité ou de la sécurité des États, mais pas dans le sens de ce diagramme dont je vous ai parlé.

En théorie, il y a donc des préoccupations, mais ils n'offrent que des avis. Il est donc très difficile de trouver une manière de le faire. Mais dans mon idée, je pense qu'ils peuvent faire quelque chose à ce sujet.

Les noms de domaine sont utilisés. Donc il y a des organisations telles que celles-ci qui peuvent faire quelque chose à ce sujet. Et

je voulais aussi commenter sur ce que vous avez dit en ce qui concerne la protection des droits de l'homme et surtout vous poser une question. Nous avons tous des responsabilités différentes. Par exemple, à l'ICANN, moi, j'avais demandé quel était le problème le plus important au niveau de la sécurité. Qu'est-ce que vous protégez ? Est-ce que vous protégez l'utilisateurs, l'Internet, ou les droits de l'homme ?

Dans certains cas, ces choses, ces sujets deviennent contradictoires. Certaines entités ont besoin d'éclairer un petit peu le sujet, de démontrer ce qu'ils protègent et cela soit commencer. C'est encore une question un peu trop générale qui n'a pas été clôturée.

PERSONNE NON IDENTIFIÉE: Je voudrais faire un point de clarification. Je pense qu'il est important de se souvenir de la mission de l'ICANN et de son espèce de travail limité. Quand il s'agit d'adresser la cybercriminalité, la cyber-guerre, si vous voulez, ce n'est pas quelque chose qui est dans la mission de l'ICANN.

Il y a des préoccupations qui sont différentes telles que la sécurité du DNS et puis, la sécurité du citoyen. C'est donc un rappel pour tous. L'ICANN protège le DNS, mais pas plus que ça.

CAROLINA MATAMOROS: Donc si on suit la mission, on sait qu'il faut que l'Internet soit ouvert et interconnecté. Donc l'objectif pour la sécurité doit être relier à cela. Je sais que ce n'est pas la focalisation, que c'est plus technique, mais que c'est un espace qui manque maintenant. Personne ne fait vraiment attention à ça. Et donc, cela met l'Internet en danger.

C'était juste une question comme ça ouverte.

PERSONNE NON IDENTIFIÉE: Il faut aussi prendre en compte qu'il y a beaucoup d'organisations qui se préoccupent de la sécurité et de la gouvernance de l'Internet. Donc ce n'est pas seulement à l'ICANN que revient la responsabilité de parler de ces choses-là. Quand on parle de protection, il faut prendre en compte tous les acteurs, toutes les autres parties prenantes qui ont un rôle à jouer dans cette protection.

PETER CIHON: Peter Cihon au micro. J'ai une question pour Chawana. J'ai vraiment apprécié votre présentation. Je ne suis pas forcément d'accord avec l'idée que vous avez présentée, mais vous avez posé beaucoup de questions qui sont intéressantes. Donc, je voudrais vous poser une question.

Si vous proposez à toutes les personnes du monde une adresse personnelle IP, et vous pouvez imaginer que cela faciliterait donc le suivi de chaque individu, de chaque personne par les gouvernements et par tout le monde dans le monde, donc cela pourrait mener… Donc, cela pourrait apporter un problème que les nations veulent protéger leurs citoyens. Donc, ces nations se retireraient de l'ICANN et de l'Internet au niveau mondial. Cela mènerait à une fraction, si vous voulez, de l'Internet.

DEBORAH ESCALERA: C'est seulement pour vous dire qu'il y a une autre réunion qui va commencer après nous. Donc, il faut qu'on termine dans la minute qu'on vient.

CHAWANA HUANGSUNTORNCHAI: Merci Peter pour vos commentaires. C'était intéressant. Si on va parler de cela, si les choses vont fonctionner, il faut qu'on travaille plus sur le fait de savoir qui est propriétaire des données. Peut-être que certains des États ou des nations ne pourront pas avoir les données pour identifier les personnes comme d'autres pays. Mais à mon avis, ça devrait fonctionner comme ça. Mais il y a beaucoup de discussion à faire sur ce sujet.

DEBORAH ESCALERA: Merci à tous pour vos présentations aujourd'hui. Je pense que vous avez fait un travail extraordinaire. Applaudissez-vous.

[FIN DE LA TRANSCRIPTION]