TERRI AGNEW : Bonjour à tous. Bienvenue au Webinaire At-Large de renforcement des capacités en ce 15 avril, qui vous explique un petit peu les activités qui se passent au niveau de la cybernétique, donc il est 21 h UTC. Nous allons maintenant présenter les personnes qui sont présentes pour ce Webinaire.

Nous vous demandons d'éteindre le son de votre micro, de votre ordinateur afin de permettre à nos interprètes de bien entendre. Nous vous demandons également de vous identifier lorsque vous parlerez pour que nous puissions vous présenter.

Merci d'être présent. Je vais maintenant passer la parole à Alan Greenberg qui s'occupe de cette séance.

ALAN GREENBERG : Alors, je remplace, en fait, Tijani parce qu'il n'est pas présent actuellement. Il ne pouvait pas participer. Mais je lui donne quand même le crédit d'avoir organisé ce webinaire.

Alors, nous avons ce qui, à mon avis, sera intéressant aujourd'hui. Nous allons donc nous focaliser sur ce sujet qui est lié aux activités d'ICANN, sur ce qui se passe dans la sphère de l'ICANN. C'est un domaine un petit peu plus général ou un sujet un peu plus général. Donc, je vais passer en revue les différentes diapositives. Je pense que ce sujet va nous intéresser. J'espère que cela va également vous intéresser, vous. Je suis

intrigué, en fait, parce qu'il n'y a pas de majuscules dans mon titre, donc je ne sais pas ce qui s'est passé…

STEVE CONTE : Merci, Alan. Je ne fais pas ma présentation, en fait, c'est la présentation de Dave Piscitello, qui, malheureusement, n'a pas pu être présent parce qu'il est en déplacement justement pour – au compte de l'ICANN. Donc, les erreurs sont les miennes, elles ne sont pas celles de Dave et donc, c'est moi qu'il faut blâmer pour ces petites erreurs de majuscules.

Alors, je me présente un petit peu pour commencer. Sur la liste, je vois des personnes que je connais et d'autres que je ne connais pas. Alors, je vais me présenter simplement. Je m'appelle Steve Conte. J'ai commencé à l'ICANN en 2002, et j'ai travaillé en tant qu'administrateur assistant. Et à l'époque, l'ICANN était toute petite. Donc, on était beaucoup moins nombreux. J'étais, je crois, l'employé numéro 13. Et donc, j'ai fait les technologies de l'information, je me suis occupé de l'IANA, j'ai également travaillé dans les technologies de l'information. J'y suis retourné en tant que gestionnaire. Ensuite, je suis parti de l'ICANN; j'ai travaillé à l'Internet Society pendant cinq ans. Et il y a un an, je suis revenu pour m'occuper – ou plutôt travailler au sein de l'équipe de Sécurité, Stabilité et Résilience avec John Crane. Donc, je me suis investi dans ce travail actuellement.

Je suis très heureux de voir les nouvelles personnes qui sont présentes et je suis aussi ravi de voir les anciens. Je suis quelqu'un qui aime, en fait, ouvrir mes présentations à toutes vos questions. N'hésitez surtout pas. Je surveillerai également le chat. Si vous souhaitez intervenir dans

la conversation par téléphone, n'hésitez pas. Ensuite, je continuerai la suite.

Alors, aujourd'hui, j'aimerais parler de la compréhension, de la distinction entre les différentes activités sur l'espace cybernétique. Donc, c'est une présentation à niveau assez élevé. Et ensuite, je reviendrai sur les points spécifiques qui concernent l'ICANN et sur tout ce qui concerne l'équipe de Stabilité, Sécurité et Résilience, et ce que nous faisons du point de vue juridique en termes d'activités illicites.

Alors, je ne vais pas lire la diapositive mot pour mot, mais vous voyez donc le – « cyber », c'est un mot quand même assez large qui à trait à tout ce qui est numérique, tout ce qui est à trait à l'Internet. C'est un terme qui est difficile à étiqueter parce que les agences de presse parlent d'attaques cybernétiques. C'est assez large. Donc, on va parler de la définition de l'activité cybernétique, quels sont les types d'activités qui ont lieu et ensuite, on tirera les conclusions par soi-même.

Alors, premièrement, nous allons voir les différents modèles d'activités cybernétiques. Alors, les moyens, les motivations et les opportunités. Alors, vous pouvez peut-être regarder simplement ce que vous avez à l'écran. Donc, il y a déjà des questions financières, les moyens financiers, les moyens technologiques et moyens intellectuels, motivations politiques, professionnelles, financières, notoriété et opportunités, accès à l'Internet.

Donc, s'il faut regarder d'un peu plus près les moyens dans les activités cybernétiques. Donc, vous avez, en fait, des m — le financement de ces activités. Donc, on ne parle pas simplement des activités de criminalité

pour l'instant, d'accord? Il y a beaucoup d'entreprises ou d'entités tout à fait légitimes. Donc, le financement doit exister pour ce genre d'entreprise. Donc, les moyens de ces activités utilisent l'Internet. Pour ce qui est du commercial, des ONG, du financement gouvernemental, ces activités permettent paient des biens numériques, il y a aussi l'*open source* et bien sûr, le financement criminel. Tous, vous recevez 40 000 e-mails par jour qui vous invitent à gagner de l'argent, etc. Donc, tout ceci, ce sont des moyens utilisés par les activités criminelles pour que vous souscriviez à quelque chose et que vous leur fournissiez vos informations bancaires ou de carte de crédit. Donc, l'objectif, c'est donc de pirater votre ordinateur pour obtenir vos données, vos informations et les utiliser à leur compte. Et puis, tout ce qui est activiste ou les militants qui utilisent l'*open source* pour, en fait, promouvoir leur propre cause. Et puis, on parle d'*hacktivism* avec un « h » en anglais. Donc, tout ce qui le piratage de sites Web de différentes organisations.

Alors, si nous considérons de plus près l'opportunité. L'Internet, c'est un accès ouvert, une infrastructure des technologies communes. Donc, le pouvoir, en fait, vient de l'adaptabilité, son pouvoir vient de sa capacité à s'adapter. Donc, cette capacité à s'adapter, c'est important de bien comprendre qu'en fait, il y a un modèle un petit peu nébuleux, organique. L'Internet s'adapte constamment. Il y a un temps, on parlait des *gophers* et des nouveaux http qui étaient lancés à l'époque. Donc, en fait, l'Internet s'adapte comme nous, nous nous adaptons. Il y a là différentes options qui existent actuellement. Donc, les nouvelles organisations, comme l'IETF comme l'UIT, les nouveaux protocoles évoluent à la mesure des besoins des utilisateurs. Donc, tout ceci

s'adapte. Donc, c'est la même chose pour tout ce qui est activités illégales et illégitimes.

Alors, maintenant, en termes de motivation, eh bien, il y a différents objectifs. Il y a les objectifs politiques; les objectifs commerciaux; il y a également la question de la notoriété. Donc, on peut déterminer si une activité est basée sur une motivation en regardant, par exemple, les e-mails qu'on reçoit. Vous avez, par exemple, une campagne politique, pour ainsi dire. Et puis, parfois, c'est mélangé avec un intérêt commercial. Et donc, parfois, ce sont les deux qui sont combinés. Mais tout ce qui est commercial, c'est aussi, par exemple, les *cookies* sur votre navigateur suivant ce que vous, en tant que consommateur, vous faites sur l'Internet. Donc, ça peut être, par exemple, Google ou un grand outil de recherches, Amazon qui fournit des services et qui, en fait, sait ce qu'ils doivent vous fournir pour, justement, vous proposer un service plus focalisé. Donc, c'est à vous de décider si oui ou non, vous aimez ce genre de choses, ce genre d'activités.

Alors, lorsqu'on considère la cybersécurité en général. Nous allons passer en revue certains scénarios. Ces scénarios ne sont pas définis de manière très claire. Il n'y a pas de définition très claire de la cybersécurité parce qu'il y a différentes facettes, différents aspects de la cybersécurité suivant le type d'activités.

Donc, la définition que nous avons, c'est donc « [l] » ensemble des pratiques et des mesures qui permettent de protéger les réseaux, les ordinateurs, etc., et puis également l'ensemble de l'Internet aujourd'hui ». Donc, il ne s'agit pas uniquement de votre ordinateur

portable ou de votre ordinateur de bureau, c'est la protection des différents dispositifs et des données qui sont contenues contre ces attaques qui ont lieu par le numérique. Ces attaques prennent différentes formes. Ça peut être du *phishing*, de l'hameçonnage, ça peut être aussi des e-mails frauduleux, ça peut être un fichier qui a été téléchargé sur votre ordinateur et qui tout d'un coup permet à quelqu'un d'avoir accès à votre ordinateur ou à votre dispositif. Donc, il y a différents types de cybersécurité.

Alors, une cyberattaque, qu'est-ce que c'est? Eh bien, il s'agit d'une attaque en ligne, numérique contre certains atouts, certains atouts physiques ou numériques. Et je sais qu'il y a un certain nombre d'années, il y a eu une attaque contre Microsoft. C'était il y a environ huit ans. Donc, contre Microsoft, et la personne qui avait attaqué Microsoft avait utilisé le serveur racine comme ressource pour les attaquer. Il y a eu une demande au serveur racine et donc, il avait répondu, ce serveur, et donc, on sait qu'il y a eu des paquets qui ont été envoyés. Donc, nous avons envoyé beaucoup de données à Microsoft. Microsoft lui a dit : « Pourquoi est-ce que vous nous attaquez? – on leur a dit – Non, ce n'est pas le cas ». Donc, il y a à la fois l'espace de l'Internet, mais il y a aussi une attaque, il y a des méthodologies qui permettent d'attaquer d'autres infrastructures, des infrastructures et des atouts physiques, par exemple les machines de distributeurs de billets.

Alors, pour ce qui est de la cybercriminalité, donc, c'est une activité en ligne qui a été classifiée comme un crime ou comme une activité en ligne qui a enfreint une loi.

Donc, lorsque vous considérez tout ce qui est sécurité publique, organisme de l'application de la loi dans le monde entier, eh bien, on essaie de voir un petit peu ce qu'ils cherchent à poursuivre en ce moment. Eh bien, très souvent, ce dont ils s'occupent, ç'a une composante numérique, ne serait-ce qu'un message texte. Eh bien, il y a beaucoup de criminalité actuellement qui inclus une composante numérique, que ce soit, par exemple, un profil avec un numéro d'identification, donc tout ce qui est Internet est très souvent impliqué dans la criminalité actuelle.

Pour ce qui est de la guerre ou des activités de guerre, eh bien, c'est une attaque sur un État-nation par un État-nation. Donc, là, je n'ai pas les informations sur ceci, mais ceci arrive. Donc, il y a, dans le monde entier – pas seulement aux États-Unis, mais dans le monde entier –, du personnel militaire qui s'occupe de ces actes guerriers sur l'Internet. Ça peut être une attaque sur, par exemple, une installation militaire, sur un bureau spécifique. Et donc, l'objectif est de déterminer si cette attaque vient d'une personne, si elle est effectuée par un groupe non gouvernemental ou par un gouvernement. Parfois, même souvent, il est difficile de déterminer quelle est la source de l'attaque, quelle est l'origine de l'attaque. Suivant le type d'attaque, on peut penser que c'est un gouvernement, mais parfois, ces gouvernements utilisent des entités qui ne sont pas affiliées à eux pour justement attaquer un gouvernement légitime.

En termes de cyber terrorisme. Donc, c'est une attaque ou un acte terrorisme d'intimidation sur les citoyens d'une nation par des personnes civiles pour personnaliser la guerre. Donc, là, il s'agit de

groupes de civils. Ce n'est pas donc pas nécessairement une attaque sur un gouvernement ou sur un organisme militaire. Cela peut être dirigé contre la population civile, à moins qu'il y ait peut y avoir un accès. Mais dans la plupart des cas, il s'agit d'essayer de cibler un groupe de personnes et en fait, cette – la personne qui fait ces actions est également un groupe de personnes.

Ensuite, en termes de cyber surveillance. Donc, des informations cachées pour la surveillance et la collecte d'informations. Donc, là, ça peut être simplement des *cookies* sur le navigateur, ça peut être simplement des suggestions de produits, ça peut être, vous savez, tout ce qui se passe au niveau de la NSA, donc le gouvernement qui surveille certains canaux, certains serveurs, certains mots-clés qui sont recherchés, ça peut être également moi, chez moi, qui m'assure que mon fils ne sera pas sur un site Web sur lequel je souhaite qu'il ne se rende pas. Donc, ça, c'est tout ce qu'est la cyber surveillance. Et il faut vraiment fournir le contexte par rapport à la surveillance qui se passe; ce que l'on cherche; ce qu'eux cherchent; pourquoi est-ce qu'il y a surveillance de votre dispositif. Et puis, on a l'activisme et le *hacktivism* dont on parlait tout à l'heure, avec un « h ». Ça pourrait être encouragé par les entités commerciales, des entités non commerciales ou simplement des groupes d'individus ou des états. Donc, ça pourrait être orienté vers des sociétés où leur cible – je passe ici au *hacktivism* et j'oublie de parler de l'activisme, mais les hackers, typiquement, ont une cible qu'ils peuvent attaquer en général à cause d'un produit, donc ils vont essayer de faire cette attaque à travers un réseau social, à travers un site Web parce qu'il y a des problèmes connus avec un logiciel, avec

un site Web et donc, ils vont essayer de remplacer ceci par un produit qu'ils sont développé eux-mêmes. Donc, des fois, dans les salles de bavardage, une salle de chat, si vous faites des commentaires ou si vous dirigez la discussion, cela sera fait pour montrer aux autres le pouvoir qu'ils ont sur le groupe.

Lorsqu'on parle de l'activisme, on a des organisations légitimes qui essaient de faire passer un message d'une manière non conventionnelle. Il pourrait très bien s'agir d'un moyen qui devrait être arrêté, peut-être, en travers une campagne de courrier électronique où on utilise ce moyen pour une fin spécifique. Mais beaucoup d'organisations utilisent ces chaînes de courrier électronique pour envoyer ces messages aux individus. Ce n'est pas à ce niveau, en tous cas, au niveau des activismes, ce n'est pas censé être une attaque envers une cible spécifique, envers une société ou une organisation tout simplement pour augmenter la conscientisation, le niveau de sensibilisation sur un sujet. Donc, ce sont des activités qui n'appartiennent pas forcément à la mentalité illégale.

En parallèle avec le *hacktivism*, on a le vandalisme. Tout comme le *hacktivism* dont je parlais tout à l'heure qui prend le contrôle d'un site Web parce qu'il n'est pas d'accord avec l'objectif d'une organisation, d'un site Web et qui [peu clair 0 :21 :31], des fois ça pourrait se faire parce que les hackers veulent devenir connus et veulent montrer au reste du monde, spécialement s'ils vont prendre le contrôle de leur site Web, ce qu'ils peuvent faire. En Californie, on a beaucoup de ce type d'activités de vandalisme qu'on appelle « *tagging* », donc c'est une manière de [peu clair 0 :22 :02] pour que l'on voit qui est la personne à

laquelle il faut faire gaffe. Ces personnes prennent le contrôle des sites Web pour faire passer ce message, pour se faire connaître et pour que tout le monde sache ce dont ils sont capables dans l'ambiance où ils sont connut, bien sûr. Là où on sait qui est chaque hacker.

Je pense déjà avoir dit cela, mais la plupart des activités ne sont pas exclusivement cyber. D'habitude, ce n'est pas quelque chose qui correspond uniquement aux activités criminelles ou délits, mais lorsqu'on voit l'activisme, par exemple, il est rare que l'on soit des activités d'activisme exclusivement sur Internet. D'habitude, l'Internet est un moyen de plus qui est utilisé pour ajouter une autre perspective ou un autre moyen d'atteindre les personnes pour leurs activités.

Lorsqu'on parle d'activités criminelles, on pense généralement aussi au reste des activités criminelles, ce que l'on essaie de faire à travers ce moyen. Donc, l'Internet devient une partie de notre identité, mais les conséquences d'habitude, ou les cibles d'habitude appartiennent au monde du physique, du réel. Donc, lorsqu'on considère les activités, il faut considérer tout à fait ces trois aspects dont on parle et donc, les moyens, les motifs et l'opportunité. Cela fait trois aspects qui vont nous aider à faire la distinction entre les activités, voir si c'était quelque chose d'exclusivement virtuel, quelles sont les conséquences, si c'est quelque chose de criminel ou pas et puis voir si ce n'est que du pourriel ou si c'est en fait un courrier électronique qui avait un but additionnel. Donc, il y a différentes manières de pouvoir faire la distinction entre les activités.

Il faut que l'on confronte ces activités au jour le jour. Donc, il faut que l'on comprenne quelle devrait être notre réponse face à ces activités. Nos réponses doivent être claires parce que des fois, on se fait voler notre identité ou alors, notre sécurité est en fait risquée. Il faut voir si on devrait se rapproche d'une agence d'application de la loi ou pas, voir si c'est quelque chose qui n'aurait pas des effets négatifs sur nos activités ou sur nous. Mais si c'est quelque chose de grave, les forces d'application de la loi vont pouvoir remédier à la situation.

Avant de passer aux questions, je sais qu'il me reste encore du temps, donc je voudrais que l'on pense un peu à pourquoi on parle de ces cyberactivités. Au sein de l'ICANN, on parle d'adresses IP, du système des DNS, et puis il y a les forces d'application de la loi, il y a les intérêts gouvernementaux et il y a aussi cet aspect d'activités criminelles qui n'appartient pas tout à fait à l'ICANN. Donc, pourquoi serait-il d'intérêt pour l'ICANN? Eh bien, cet aspect est discuté au sein d'une petite équipe où on n'est pas beaucoup de personnes, mais cette équipe s'occupe de différents aspects et de plus en plus, on commence à travailler avec les forces et les agences d'application de la loi pour essayer de comprendre l'aspect numérique de tout ce qu'on fait. Donc, le domaine du cyber ou plutôt les activités ne sont pas exclusivement sur Internet. En ce moment, nous travaillons pour aider la communauté technique, les gouvernements et forces d'application de la loi à comprendre non seulement qui entreprend ces activités et pour comprendre quel est le fonctionnement ou le risque du WHOIS, mais plutôt comment gérer ou comment résoudre les potentiels problèmes sur Internet et comment s'adresser à un juge pour lui demander, par

exemple, d'élargir la législation disponible pour qu'il comprenne quel est le risque de ce type d'activités. Il faut, dans le domaine du réel [peu clair 0 :27 :24] des preuves pour pouvoir prendre des mesures avant de pouvoir déposer une plainte. Alors, sur Internet, il faut que l'on comprenne vraiment quelles sont ces preuves dont on pourrait se servir pour aller voir un juge et déposer cette plainte et commencer notre procès. Le [peu clair 0 :27 :49] au-delà de ces aspects à coordonner les activités. [Inaudible 0 :27 :55] sur l'élaboration d'un *bot net*, comme on l'appelle, pour essayer d'assurer que les noms de domaine qui ne sont pas approuvés n'aient pas de mauvais effet sur les bureaux d'enregistrement accrédités.

Alors, on travaille avec les forces d'application de la loi et avec les bureaux d'enregistrement pour comprendre ces risques potentiels, pour voir comment agissent ces personnes qui vont contre leurs intérêts, contre le bien commun et pour qu'ils comprennent comment mieux opérer. Alors, il faut assurer que tous les processus soient correctement suivis, que les bureaux d'enregistrement travaillent correctement dans le cadre établi avec les registres. Et si l'un deux était impliqué dans des activités illégales, il y aurait un tiers qui va coordonner les mesures à appliquer pour pouvoir résoudre cette situation. Donc, on travaille depuis un bon moment sur ces aspects, au moins depuis deux ans. Donc, ça fait deux ans que l'on discute sur comment pouvoir aider à résoudre ces problèmes. Comment on peut trouver les preuves nécessaires pour le faire.

Alors, je vais m'arrêter là et vous passer la parole pour que vous puissiez poser vos questions.

Y'a-t-il des questions?

ALAN GREENBERG : Y'a-t-il des questions? Bien, Alberto veut prendre la parole. Il est sur le canal espagnol, sans doute. Allez-y, Alberto.

ALBERTO SOTO : Oui, Alberto ici. Je m'excuse, je suis enrhumé et donc, ma voix n'est pas vraiment très forte.

Au sein de LACRALO, nous avons une séance de formation dans le cadre de notre programme de formation et on voudrait pouvoir inclure votre présentation dans ce programme que nous avons. Donc, je reprends dès le début votre présentation et je voudrais dire que l'on devrait mieux comprendre ce qu'est le cyber, que l'on devrait discuter davantage de la formation des utilisateurs individuels, qui sont vraiment les cibles de notre programme, mais ils font également partie de notre structure multipartite parce qu'au sein de chaque séminaire Web que nous avons organisé, nous avons toujours expliqué cette différence gouvernementale, des fournisseurs de services Internet et de la société civile. Donc, chaque fois, on avait un représentant de tous les secteurs – ou on essaie en tous cas de le faire, d'avoir des personnes du secteur académique aussi. LACRALO ne voudrait pas établir la différence, on voudrait plutôt générer une participation conjointe et expliquer ce que l'ICANN peut faire pour pouvoir atteindre un public plus large.

Merci.

ALAN GREENBERG : Merci, Alberto. Je ne sais pas si Steve voudrait que l'on entende plusieurs questions et puis que l'on réponde tous ensemble ou faire question par question.

STEVE CONTE : Comme vous voulez, Alan.

ALAN GREENBERG : Si vous voulez, on peut entendre Holly d'abord et puis on répond.

STEVE CONTE : Excellent. Merci.

ALAN GREENBERG : Holly, allez-y,

HOLLY RAICHE : Vous m'entendez? Merci.

Je suis Holly Raiche. Steve, je voulais parler des attaques aux formes d'unités constitutives. Est-ce que vous avez établi la différence entre les différentes attaques? Parce que lorsque vous expliquez les différences et les différentes activités, vous parliez à chaque fois de pouvoir sensibiliser les gouvernements pour qu'ils comprennent les implications de ces attaques et de ces activités. Et il me semble que c'est une

manière excellente de pouvoir sensibiliser des cyberdélits, de la cybercriminalité, mais peut-être que ce serait bien également d'intégrer les autres unités constitutives pour que tout le monde comprenne les impacts de ces activités.

STEVE CONTE : Merci, Holly. Je suis d'accord avec vous. Je pense que je pourrais répondre à votre question et à celle d'Alberto avec la même réponse, en réalité. En tant que société, nous travaillons de près avec le groupe de participations des parties prenantes mondiales puisque c'est eux qui sont à la base, qui travaillent avec la communauté élargie, qui ont les connexions avec les gouvernements et les organisations de chaque région. Donc, nous visons à travailler au sein de l'ICANN avec le groupe de participations multiparties prenantes mondiales pour pouvoir atteindre un public élargi. Alors, par rapport à votre question, Holly, tout à fait. On essaie d'augmenter notre niveau de contact avec les différents secteurs avec la communauté qui appartient à l'ICANN dans le sens large.

Par exemple, pour ce qui est de la ccNSO, nous nous sommes rapprochés d'eux lors de la réunion de Londres, si je ne me trompe et on a discuté avec certains membres de l'ICANN, également, pour essayer d'établir les rapports avec eux et pour essayer de renforcer les rapports.

Maintenant, lors de ma présentation, je n'ai pas demandé quelle était la situation de votre groupe. Parce que lors de la réunion de Los Angeles, on s'est réuni avec votre groupe et on a discuté de la possibilité de

coordonner nos activités avec vous pour pouvoir augmenter le niveau de participation, d'engagement avec votre groupe qui compose l'aspect communautaire de l'ICANN.

Cette formation de sensibilisation de la sécurité qu'on fait, en réalité, n'est pas tellement pertinente pour votre groupe. On sait que vous voyagez autant que nous. Mais au niveau du consommateur, on essaie sans doute de travailler autant qu'eux au niveau gouvernemental. Donc, il y a des organisations qui travaillent pour aider le système et pour assurer, par exemple que les chaînes de courriers électroniques ne sont pas de l'hameçonnage, donc que l'on ait des conversations avec les différentes entités, non seulement avec les gouvernements aussi.

Nous allons probablement organiser une série de séminaires Web de formations. En ce moment, on travaille sur une meilleure compréhension du DNS, et c'est un module qui est vraiment à la base du travail de l'ICANN puisque c'est la mission principale de l'ICANN. Donc, on essaie de donner ces informations de base sur ce qu'est le DNS. Et une fois qu'on aura conclu ce programme, nous allons demander à tous les groupes de nous faire des contributions pour voir quel est l'intérêt des personnes des différents groupes, comme vous, par exemple, et pour assurer que nous travaillons à un niveau correct pour voir que notre attention est mise là où il le fait. Et donc, on suit un nombre de processus en ce moment.

J'ai mis ici un lien sur la salle de bavardage pour que vous voyiez quelles sont les ressources que nous avons sur la sensibilisation de la sécurité.

Donc, si vous avez d'autres idées à nous transmettre, faites-le-nous savoir, s'il vous plaît.

Nous travaillons avec les forces d'application de la loi, comme j'ai dit tout à l'heure, et nous essayons de contacter ces forces et les gouvernements parce qu'on veut commencer dès le début, et trouver des moyens de résolution des problèmes. Et on travaille du bas vers le haut, comme partout dans l'ICANN.

Donc, Holly, Alberto, j'ai répondu à vos questions?

HOLLY RAICHE : En ce qui me concerne – c'est Holly —, moi, je pensais aux activités qui ont lieu, par exemple la question des enfants dans la cybercriminalité. Donc, c'est le type de choses, telles que la coordination – il y a beaucoup d'information qui devrait être disséminée, qui devrait être à disposition. Et donc, l'idée, ce serait d'utiliser l'ALAC pour diffuser ces informations.

STEVE CONTE : Je suis d'accord avec ça. Effectivement, on pourrait regarder le lien. Donc, n'hésitez pas à me contacter parce qu'on pourrait effectivement développer un modèle là-dessus.

HOLLY RAICHE : Oui. Merci.

ALAN GREENBERG : Merci, Steve. Y'a-t-il d'autres questions? Sinon, c'est à moi. Alors, moi, j'ai fait ma première présentation sur le pourriel, je crois, en 2002. Il m'a fallu collecter pendant six mois avant tous les pourriels que j'avais reçus. C'était intéressant. Et j'ai donné ma première présentation sur la cybercriminalité, d'une manière plus générale, il y a à peu près 15 ans, je crois.

Alors, à votre avis, quel a été le plus gros changement? La plus grande évolution? Il y a eu des hauts et des bas, on est passé vraiment de problèmes très graves à des problèmes moins graves, mais qu'est-ce qui a changé?

STEVE CONTE : C'est une excellente question. De mon point de vue en tant que simple personne – et je ne sais ce que considère les forces de la loi, mais en tous cas, ce qu'ils nous disent, c'est que les plus gros changements au cours des dix dernières années, disons, bon, le pourriel, on en est au même point, mais il y a beaucoup plus de gens qui utilisent l'Internet aussi. Mais on voit de plus en plus d'activités d'hameçonnage, de collecte de données, et donc, on essaie de voir un petit peu ce qu'il faut faire pour mieux comprendre, pour mieux saisir ce qui se passe dans ces activités d'hameçonnage. Je sais qu'à Londres, la FDA des États-Unis s'est souciée du problème des produits pharmaceutiques sur Internet, des produits illégaux. Ça, c'est vraiment un vrai problème. Ce n'est pas simplement une perte d'argent ou un vol d'identité, mais c'est une question de vies qui sont mises en danger. Donc, ça, pour moi, c'est un nouvel aspect de cybercriminalité. Donc, en termes de sécurité

publique, les communautés cherchent vraiment à mieux saisir ce qu'il faut faire pour mettre un frein à ceci. Autrement, en dehors de l'hameçonnage…

ALAN GREENBERG : Alors, nous avons demandé à ceux qui ne parlent pas d'éteindre leur micro, s'il vous plaît. Il y a beaucoup de bruits et on n'entend plus rien. Merci beaucoup.

Alors, nous avons Alberto et ensuite, Holly.

ALBERTO SOTO : Au sein de notre organisation et dans les différents pays, nous considérons – en fait, nous parlons aux utilisateurs de l'Internet, nous parlons de tout ce qui est le trafic, la pornographie, la traite des hommes. Donc, nous parlons aux utilisateurs. Lors de notre dernier webinaire, il y a eu une présentation et au cours de cette présentation, on a parlé du GAC et des utilisateurs de l'Internet. Nous avons parlé avec le président du GAC et nous nous sommes mis d'accord sur le fait qu'il fallait qu'il y ait participation à des réunions pour avoir une meilleure relation parce que ceci doit nous être utile. Pourquoi? Parce que dans les pays d'Amérique latine, il n'y a pas de loi là-dessus et il y a très peu d'équipes techniques qui aient vraiment les moyens, les capacités de s'occuper de ce genre de sujets. Et quand je parle de capacité, il y a aussi les équipements, les dispositifs. Tout ceci coûte très cher!

Donc, notre tâche, c'est de nous focaliser sur un travail qui puisse générer, de manière ascendante, l'élaboration de politiques dans les différents pays pour vraiment traiter de ces sujets parce qu'il est possible qu'ils aient des dispositifs, des équipements, mais il est possible qu'ils n'aient pas d'autorisation de conserver les données. Donc, c'est ce qui se produit avec les fournisseurs d'Internet. Donc, il faut déjà faire l'investigation du crime, mais il n'y a pas de données qui sont disponibles. Et ces informations ne sont pas disponibles parce qu'il n'y a pas d'obligations de conserver ces informations, de garde les données. Donc, il y a un problème assez complexe auquel nous sommes confrontés dans la situation actuelle. Merci.

ALAN GREENBERG : Merci, Alberto. Steve, avez-vous des commentaires?

STEVE CONTE : Bien sûr. Avant de passer à Holly, c'est effectivement un commentaire intéressant. Si nous étions tous présents et si je pouvais, en juin, à Buenos Aires, vous demander de lever la main si dans les différentes régions, vous avez ce même problème, je m'imagine que nous verrions la moitié ou la majorité de la salle avec la main levée. Donc, je crois que c'est un point à considérer, c'est un point important et ce n'est pas réservé à vous.

Donc, en termes de politiques, ce que nous avons vu au cours des 15 dernières années, c'est qu'il y a toujours eu deux groupes spécifiques : les décideurs et les développeurs. Donc, les décideurs, en termes de

politiques, et puis la technique. Et donc, je voudrais féliciter Sally Wentworth et l'Internet Society parce qu'ils ont fait un travail extraordinaire pour établir le dialogue entre ces deux groupes. Donc, de plus en plus, on voit des personnes qui s'occupent à la fois de la technologie et de la politique. Et ça, ça va nous aider parce que la politique sur l'Internet ne peut pas être mise en place sans la technologie. Et de nos jours, la technologie ne peut pas évoluer sans qu'il y ait de politiques, non plus.

Donc, l'Internet n'est plus ce qu'il était… Il est devenu – je suis en train de faire des guillemets avec mes doigts – c'est un petit peu comme s'il avait deux corps, deux entités, qui, de plus en plus, deviennent une seule entité. Donc, ceci, nous devons le promouvoir dans toutes les régions pour, justement, atténuer ce genre d'activités. Il nous faut travailler avec les personnes qui sont responsables des politiques et les personnes qui sont responsables de la technologie pour promouvoir des protocoles plus responsables, des applications, des politiques, tout ceci, à mon avis, c'est important pour que nous puissions aller de l'avant.

ALAN GREENBERG : Merci, Steve. Holly?

HOLLY RAICHE : Je vais poser une question difficile. Quels sont les défis, en tant que nouveaux gTLDs…

INTERPRÈTE : Désolée, je n'ai pas bien entendu Holly.

STEVE CONTE : En termes de nouveaux gTLDs, non seulement les IDNs, mais aussi la nouvelle série de TLDs qui vont être lancés, nous voyons un petit peu les tendances en termes de cybercriminalité. Donc, nous faisons beaucoup d'analyses, de recherches pour savoir quels sont les bureaux d'enregistrement qui n'observent pas bien ce qui se passe chez leurs clients, quels sont les secteurs qui sont les plus ciblés. Et donc, nous avons essayé de voir un petit peu que faire au niveau des nouveaux TLDs avec cette approche.

Je n'ai pas de statistiques à vous donner dans l'immédiat, mais c'est ce que nous prenons en considération. Nous travaillons avec les bureaux d'enregistrement, les opérateurs de registres et nous essayons de les aider à atténuer les activités criminelles.

HOLLY RAICHE : Merci. Je pense que ce serait quelque chose – une discussion qu'il faudrait poursuivre à Buenos Aires.

ALAN GREENBERG : Y'a-t-il d'autres questions? Y'a-t-il d'autres commentaires? Nous avons encore un peu de temps.

Apparemment, vous avez répondu à toutes les questions possibles et imaginables.

Avez-vous des commentaires pour conclure?

STEVE CONTE : Je voudrais simplement répéter mon message. Lorsque j'étais à Los Angeles pour la réunion de l'ICANN, que j'ai parlé à l'ALAC, je ne sais plus en quelle capacité, mais je me souviens d'avoir été présent et d'avoir eu vraiment eu les yeux ouverts parce que je n'ai pas suffisamment, par le passé, discuté avec l'ALAC. Je crois que ce qui est important pour moi, c'est d'être plus en plus présent. Donc, n'hésitez surtout pas à communiquer avec moi. Bien sûr, je ne vais pas non plus prendre tout votre temps, donc dites-moi de partir si je prends tout votre temps. Mais je crois que c'est important d'avoir un dialogue entre mon .équipe SSR et votre équipe. Je pense que la relation est importante et j'apprécie beaucoup cette opportunité que vous nous avez donnée de pouvoir discuter avec vous et de pouvoir créer ce dialogue.

ALAN GREENBERG : Merci. Alors, quelques commentaires. De toute évidence — en fait, il y a une autre main qui s'est levée, donc vous n'avez pas tout à fait terminé. Il y a une question dans le chat aussi en plus. De toute façon, nous avons 90 minutes de prévues, donc nous avons encore le temps.

Bon. Si vous venez à nos réunions ALAC, nous n'allons pas vous fermer la porter. Et beaucoup des choses que nous faisons sont focalisées sur les utilisateurs. C'est notre rôle. De manière plus spécifique, c'est non seulement ce qui peut nuire à l'utilisation, mais aussi ce que nous

pouvons faire pour améliorer l'expérience des utilisateurs pour la rendre plus sécurisée et meilleure. Donc, ce que nous faisons, notre travail, c'est justement quelque chose qui concerne la SSR. Pas nécessairement dans ce qui est sous le contrôle de l'ICANN, mais nous nous focalisons là-dessus.

Alors, Olivier. Il me semblait bien que vous ayez une question.

OLIVIER CRÉPIN-LEBLOND : Merci beaucoup, Alan. Olivier au micro. Vous m'entendez?

ALAN GREENBERG : Oui.

OLIVIER CRÉPIN-LEBLOND : Très bien. Merci beaucoup, Steve, pour cette présentation. C'est très intéressant. Ce qui m'intéresse, c'est vraiment cette question des attaques dans l'espace cybernétique, l'*hacktivism*, le piratage, etc. Et bien sûr, l'ICANN est aussi – il y a le problème de l'hameçonnage. Et est-ce qu'on parle en termes de [peu clair 0 :51 :08]? Est-ce qu'on parle d'*hacktivism* ou est-ce que c'est autre chose?

STEVE CONTE : D'accord, Olivier. Donc, l'hameçonnage, d'une manière générale, c'est donc obtenir des informations des utilisateurs. Donc, si vous avez un e-mail qui vous vient avec quelqu'un, eh bien, leur objectif c'est d'obtenir votre mot de passe. À ce moment-là, vous avez été hameçonné,

d'accord? Ils vont prendre vos informations et vos informations vont être utilisées pour une entité qui ne devrait pas les utiliser, par exemple vos informations bancaires.

Alors, maintenant, pour ce qui est du *spear phisphing*, c'est-à-dire de l'hameçonnage ciblé, eh bien, c'est une attaque qui justement vise certaines personnes, certains groupes, certaines organisations afin de compromettre les points d'entrée dans le réseau en lui-même pour rentrer dans l'organisation.

Donc, la SSR ne s'occupe pas dans l'aspect sécurité au jour le jour du protocole Internet, mais il y a eu un hameçonnage ciblé. Nous avons été attaqués. Nous avons été ciblés, nous, en tant qu'organisation, et puis également, certaines personnes dans l'organisation. Nous ne savons pas exactement qui a agi de la sorte, nous ne savons pas quelles étaient leurs motivations. D'ailleurs, l'équipe de sécurité au sein de l'ICANN, au sein de notre propre service et puis en dehors a essayé de savoir première quel a été le compromis et deuxièmement, quelle a été la motivation. Le modèle que je vous ai présenté tout à l'heure : les objectifs, les motivations et les opportunités.

Parfois, il est très difficile de déterminer « qui » et « pourquoi » parce que sur l'Internet, vous pouvez être le mec poilu et faire comme si vous étiez une petite fille. Bon, c'est ça, le problème. L'hameçonnage est très difficile à définir parce qu'on peut se cacher.

Donc, en termes d'hameçonnage ciblé, une fois qu'on a été attaqué, une fois qu'il y a eu compromission des données, eh bien, il faut agir immédiatement. Et bien sûr, l'ICANN l'a fait. L'ICANN a agi

immédiatement, dans les huit à douze heures qui ont suivies. Il y a eu action. Cela s'applique à d'autres organisations. Ce n'est pas forcément uniquement pour l'ICANN. Nous avons mis en place d'autres pare-feu, nous avons mis d'autres processus en place pour sécuriser le réseau. Et l'autre élément, c'est de collecter les données. On espère qu'il y a des données à collecter. Une fois que les données ont été collectées, on essaie de reconstituer le puzzle, l'histoire, pour avoir une image de la personne, qui est-elle, pour pouvoir agir.

ALAN GREENBERG : Merci beaucoup. Ce serait peut-être amusant d'entendre ça : je vais vous parler de ma première expérience d'hameçonnage. Hameçonnage ciblé, je ne sais pas. C'était un télétype de caractères de dix par seconde. Bien sûr, ça n'a pas coûté très cher, mais bon…

Y'a-t-il d'autres questions? Y'a-t-il quelqu'un qui parle sur le chat? Non?

Alors, Steve, vous avez peut-être une autre opportunité d'en terminer avec nous. Vous n'êtes pas obligé de répéter ce que vous avez dit tout à l'heure, mais y'a-t-il encore des questions? Des commentaires?

HOLLY RAICHE : Dev a une question.

ALAN GREENBERG : Dev fait référence à un certain nombre de sessions lors de réunions d'ICANN précédentes et donc, il demande s'il en aura d'autres,

similaires, en Argentine sur la cybersécurité, sur la sécurité publique, donc des ateliers.

STEVE CONTE : Donc, l'atelier sur la sécurité sera constant. Nous allons donc rassembler les forces de l'application de la loi, la communauté ICANN pour parler de ce qui se fait. En général, c'est une session qui est à moitié ouverte et à moitié fermée. Je ne sais pas exactement quand elle aura lieu. Sans doute le jeudi.

Alors, en ce qui concerne la cybersécurité, les événements SSR, à Buenos Aires, je ne sais pas exactement. Je sais que John Crane va s'en occuper. En tous cas, je pourrais vous faire passer les informations. Je ne sais pas si je dois passer par Terry pour vous faire passer le message…?

ALAN GREENBERG : Ou Gisella peut-être…?

STEVE CONTE : Alors, s'il y a des choses qui sont organisées par SSR de manière spécifique. Eh bien, je vous laisserais passer par Gisella pour l'ALAC.

ALAN GREENBERG : Alors, dernier commentaire? Une fois… deux fois… trois fois… c'est terminé.

Merci, tous cas, Steve, pour votre temps. De mon point de vue, j'aimerais vous remercier.

STEVE CONTE : Merci. Et surtout, n'hésitez pas à venir vous présenter à moi à Buenos Aires. J'y serai sur place pendant toute la semaine.

ALAN GREENBERG : On va essayer de ne pas oublier. En tous cas, merci pour votre contribution, du petit poème au début de l'appel. Je ne sais pas si c'est vraiment un poème, mais merci, en tous cas, de votre présente.

STEVE CONTE : Merci.

ALAN GREENBERG : Merci à vous tous d'avoir écouté notre appel.

[FIN DE LA TRANSCRIPTION]