ICANN69 | Réunion générale annuelle virtuelle – Séance sur les politiques d'At-Large : au-delà de Budapest: le Traité de l'ONU sur la cybercriminalité et les abus du DNS
Mardi 20 octobre 2020 – 16h30 à 17h30 CEST

MICHELLE DESMYTER: Nous pouvons lancer l'enregistrement. Bonjour, cette séance va commencer, nous allons lancer l'enregistrement.

Bonjour, bienvenue à cette séance au-delà de Budapest, relative au traité de Budapest sur la cybercriminalité. Cette séance est enregistrée et nous allons appliquer les normes de conduite de l'ICANN.

Pendant cette séance vous pouvez utiliser l'application de Congress Rental, un service d'interprétation simultanée en français et en espagnol sera disponible pour cette séance, via Zoom et la plateforme d'interprétation simultanée à distance de Congress Rental. Les participants sont encouragés à télécharger l'application de Congress Rental Network suivant les instructions dans le chat ou dans le document disponible sur la page web de la réunion.

Si vous souhaitez parler, levez la main dans la salle Zoom. Lorsque vous serez appelé par votre nom notre équipe technique activera votre micro. Dites votre nom pour l'enregistrement, la langue dans laquelle vous allez parler si ce n'est pas l'anglais. Au moment de parler assurez-vous de mettre en mode muet tous les autres dispositifs.

Parlez clairement et à une vitesse raisonnable pour permettre une interprétation exacte de vos propos.

Je vais maintenant donner la parole à Joanna Kulesza. Joanna vous avez la parole.

JOANNA KULESZA: Merci, merci de vous joindre à nous pour cette séance. J'ai plusieurs diapositives, est-ce que vous pouvez les mettre sur l'écran s'il vous plait ?

Nous allons présenter nos intervenants. Le titre ici sera un titre assez controversé : au-delà de Budapest, et nous allons parler du traité contre le cyber délit des Nations Unies. Et nous allons voir quels sont les processus qui existent actuellement qui visent les activités malveillantes en ligne.

Nous avons donc eu une série déjà de séance, nous avons eu plusieurs discussions qui ont eu lieu au sein de l'ICANN sur l'utilisation malveillante du DNS. Et il est clair pour nous tous de quoi nous parlons lorsque nous parlons d'utilisation malveillante du DNS, et At-Large a fait plusieurs formations sur ce thème.

Cette séance est une autre tentative visant à mieux comprendre ce que signifie l'utilisation malveillante du DNS et comment protéger les utilisateurs finaux. Nous essayons de voir quels sont les instruments qui existent pour atteindre cet objectif, et nous allons aussi explorer

les différentes possibilités permettant de lutter contre les utilisations malveillantes du DNS et de combattre ce problème.

Bien, donc première diapositive avec l'ordre du jour et une présentation un peu de notre discussion. Je vais d'abord commencer par récapituler un petit peu les discussions que nous avons eues à At-Large.

Nous avons analysé les différentes tendances politiques qui se focalisent sur les politiques internationales qui pourraient avoir un impact sur la communauté de l'ICANN. Nous allons analyser le travail réalisé par les Nations Unies. Je ferai une petite présentation et je vous dirai où nous en sommes au niveau de la discussion géopolitique.

Ensuite mon collègue d'ALAC et d'EURALO va nous parler de la perspective de l'utilisateur final, Matthias Hubodnik qui va nous parler donc des différentes politiques concernant l'utilisation malveillante du DNS. Et ensuite, je suis heureuse d'accueillir Alexander Seger qui va nous parler de ce sujet.

Donc nous avons une heure, et j'espère que nous aurons aussi le temps de passer à la discussion.

Donc Alexander nous donnera une petite idée de ce qu'il se passe entre les politiques du DNS et les processus internationaux qui existent actuellement et qui essaient de viser ces problèmes et de maintenir les utilisateurs finaux du bon côté.

Bien, nous allons voir un petit peu où nous en sommes concernant cette discussion. Prochaine diapo.

Donc ici, cette diapositive, nous avons discuté de l'utilisation abusive du DNS et il y a eu une série de travaux qui ont été faits dans ce domaine. Ici nous avons une définition de l'utilisation malveillante du DNS, ici vous avez le cadre qui aborde ces questions. Et nous allons aborder toutes ces difficultés, tous ces problèmes, les activités qui sont dangereuses. Donc il s'agit du logiciel malveillant, des réseaux zombies, du hameçonnage, du dévoiement, courrier indésirable ou spam.

Et, prochaine diapo, vous allez aussi voir des définitions plus spécifiques de l'utilisation malveillante du DNS et des actions que l'on attend de la part des bureaux d'enregistrement et des opérateurs de registre.

Ici vous voyez donc qu'il y a un encouragement pour ces bureaux d'enregistrement et opérateurs de registre, pour qu'ils puissent participer davantage et pour qu'ils puissent donc agir pour notre sécurité, la sécurité des utilisateurs finaux.

Je vais maintenant présenter Alexander, ensuite – prochaine diapositive – nous allons parler de la convention de Budapest.

Je sais que tout le monde connait cette convention, mais je suis sûre qu'Alexander pourra nous en donner un petit peu plus de détails.

Je sais que nos collègues et nos partenaires qui n'appartiennent pas à l'ICANN vont pouvoir aussi indiquer à notre communauté l'importance de cette convention pour lutter contre la cybercriminalité.

Il y a des discussions qui ont eu lieu dans le domaine de la géopolitique au sein de l'ICANN. Ici vous voyez donc les points qui ont été discutés auparavant. Nous avons l'ICANN Org qui va nous parler du travail réalisé au sein des Nations Unies.

Les Nations Unies sont très intéressées par le succès de cette convention de Budapest. Et c'est quelque chose qui ne va pas avoir lieu demain, mais lorsqu'on a eu cette discussion de géopolitique, on s'est demandé comment la communauté pourrait participer à ce processus pour que l'utilisateur final soit mieux protégé.

Donc ici, voilà, vous avez les différentes tendances qui existent, vous voulez peut-être y participer. Nous allons essayer de voir comment est-ce que cela est possible et comment se joindre à cette tendance.

Et, la dernière diapositive que j'ai ici, c'est un petit peu une manière de voir la tendance qui existe entre cette géopolitique, et ici vous trouverez ce document sur le site internet de l'ICANN, qui est produit par l'équipe de participation de l'organisation intergouvernementale de l'ICANN. Et donc ici c'est Veni Markosvki qui va participer, va présenter ce document demain pendant une séance beaucoup plus longue.

Donc j'encourage tout le monde à participer aujourd'hui à la réunion pour introduire la réunion de demain.

Bien, en tout cas, Veni va nous présenter ce document et c'est un lien entre un processus actuel et la protection du DNS et la lutte contre l'utilisation malveillante du DNS.

Je crois que j'ai une dernière diapositive. Voilà les questions sur lesquelles nous allons essayer de nous centrer pour répondre aux différentes questions. Donc comment les utilisateurs finaux peuvent aborder ces questions, est-ce qu'il y a un lien entre l'utilisation malveillante du DNS et les règlementations liées à la cybercriminalité, les traités internationaux ? Est-ce qu'il y a un rôle pour la communauté de l'ICANN pour participer à ces discussions au niveau international et comment protéger efficacement les utilisateurs finaux contre l'utilisation malveillante du DNS.

Voilà, je sais que tout cela sont des questions controversées.

Et, maintenant, je vais m'arrêter ici, je vais donner la parole à Matthias qui va aussi présenter un thème plein de controverses.

On me demande de respecter le temps de parole de chacun, donc je donne la parole à Matthias et ensuite je demanderai à Alexander de répondre à ces questions et de nous parler des outils que nous avons pour lutter contre ces problèmes.

Matthias vous avez la parole.

MATTHIAS HUBODNIK: Bonjour à tous, je suis Matthias Hubodnik. Pour ceux qui ne me connaissent pas, je suis un ingénieur, je suis membre du comité

consultatif d'At-Large. Et, comme Joanna l'a dit, je vais essayer de mettre l'accent sur le processus législatif existant actuellement et sur son impact concernant les politiques de lutte contre l'utilisation malveillante du DNS à l'ICANN et qu'en attendre.

Tout cela est basé sur des exemples et je vais être aussi bref et pratique que possible de façon à ce que nous ayons suffisamment de temps pour passer aux questions ensuite.

Prochaine diapositive.

Il s'agit ici de Matt, c'est un utilisateur d'internet. Ici vous voyez WWW.MAT.INFO, c'est son adresse. Et, un jour, ce nom de domaine a reçu un problème et comment résoudre ce problème ?

Prochaine diapositive.

Alors, que peut faire Matt en tant qu'utilisateur final d'internet pour lutter contre cette utilisation malveillante de son nom de domaine ? Il peut aller voir la police, et la police va appliquer la loi locale et les lois liées à la télécommunication qui sont plus ou moins les mêmes que celles qui existent dans les autres systèmes. Ici il s'agit du système légal de loi locale. Ensuite, très souvent on a des problèmes de cybercriminalité qui pourraient être coordonnés par la police locale ou par les forces de l'ordre, comme dans le cas de l'agence européenne de lutte contre ce type de problème. Et, comme je l'ai déjà dit, l'origine, l'enquête se fait en général à travers la législation locale lorsque le suspect habite dans un pays étranger et a besoin

d'une assistance légale. Et donc les demandes sont faites pour que les suspects soient interrogés.

Prochaine diapositive.

Nous allons maintenant avancer un petit peu plus loin. Ici vous voyez donc une image controversée avec donc ce terme de « censuré », et l'utilisateur final va voir cette image sur son site internet. Comme c'est un journaliste, il va par exemple y avoir un événement qui a attiré l'attention et il va voir cette image apparaitre avec une photo, avec des enfants, et cette photo a montré aussi donc différents droits. Il y a eu un débat concernant la liberté d'expression en Norvège après qu'une photo soit diffusée sur un site. Cela a été interdit et annulé.

Donc, il y a une équipe de personnes, des humains, sur Facebook, qui ont décidé de retirer cela du site et que cette photo violait donc les comportements attendus de l'ICANN.

Passons maintenant à la prochaine diapo.

Comme Joanna l'a dit tout à l'heure, voilà donc les cadres différents, les cadres juridiques différents, à différents niveaux, qui sont utilisés. Et je voudrais souligner le cadre de travail du DNS. Et cela donc touche aux opérateurs de registre et aux bureaux d'enregistrement et les principes qu'ils utilisent vis-à-vis du contenu, de l'utilisation malveillante du contenu, donc encore une fois sur tout ce qui est site web.

En particulier ce que je voulais souligner c'est le fait que dans ce papier ou dans ce document que les opérateurs de registre et les bureaux d'enregistrement devraient faire cela dans l'ordre.

Ce qui me surprend plutôt c'est le langage. Vous voyez sur la photo, vous voyez ce qui peut être utilisé pour retirer du contenu lorsqu'il y a de la revente.

Le document aussi souligne qu'un bureau d'enregistrement ou un opérateur de registre peut gérer tout cela, et donc on peut demander au titulaire de registre de retirer le contenu.

Voilà donc des points très intéressants. Je ne veux pas entrer dans une conversation détaillée sur les services, car nous aurons une séance qui va faire référence à ces questions.

Je veux là discuter de la définition. Qu'est-ce que cela veut dire pour les utilisateurs finaux ? Comment est-ce que ça a un impact sur eux ?

J'essaie d'expliquer de façon pratique cette perspective. Quelqu'un peut dire : ho, ça va, je peux contacter mon opérateur ou mon bureau d'enregistrement sans une demande, sans une demande juridique, sans avoir à utiliser la loi.

Mais, d'un autre côté, quel est le cadre que l'on peut utiliser ? Qui décide et qui a l'expertise pour le faire d'une façon indépendante ou techniquement ? Enfin est-ce quelqu'un a l'expertise technique pour le faire ?

Prochaine diapo.

Ce que je voulais dire, je ne suis pas là pour résoudre ce problème, je suis là pour dire qu'il ne faut pas penser à d'autres remèdes, d'autres remèdes additionnels, mais il est crucial d'en parler et de souligner les avantages et les inconvénients. Cela dépend bien sûr de l'opinion de chacun ou de la position de chacun. Comment est-ce qu'on peut garantir les droits de liberté d'expression par exemple ? Comment peut-on aider les utilisateurs finaux de façon réaliste pour qu'ils soient sécurisés ? Est-ce qu'il doit y avoir disons un groupe qui pourrait superviser, qui ferait des révisions ou des examens, est-ce qu'il pourrait y avoir un groupe dédié qui va décider de ce que vont faire les opérateurs de registre ou les bureaux d'enregistrement, et dans quelle capacité ? Comment les preneurs de décision vont respecter les normes ?

Et donc je vais m'arrêter là. Je suis impatient de recevoir vos informations de retour et d'écouter la conversation qui va suivre.

Je passe la parole à Joanna.

JOANNA KULESZA: Merci. À vous Alex.

ALEXANDER SEGER: Oui, très bonne discussion. J'espère que je peux contribuer. Le titre de cette séance était un peu controversé. Donc on a parlé de.. Au-delà de Budapest, moi je dis avec Budapest.

On a parlé de la coopération mondiale sur la cybercriminalité, et cela inclut l'utilisation malveillante du DNS.

Prochaine diapo s'il vous plait.

Si vous observez tout ce qui concerne la cybercriminalité, et là on parle de l'utilisation malveillante du DNS en tant que point de départ, il y a donc une obligation positive de protéger. Les gouvernements ont donc l'obligation de protéger les individus contre la criminalité, y compris par le droit pénal.

La convention de Budapest est un traité de justice pénale. Et donc il y a eu une décision qui a été prise sur ce qu'il s'est produit entre KU et la Finlande. Il y a eu donc des réponses juridiques. Ce n'est pas un instrument… C'est un instrument qui traite de données spécifiques qui était nécessaire. Et, comme Matthias l'a dit quand on a parlé des droits de personnes, la réponse de la justice criminelle est de protéger les personnes contre la criminalité. Mais ses pouvoirs sont limités. Et pour protéger les individus, les personnes, c'est très compliqué.

Il faut aussi garder à l'esprit que la justice pénale ne peut pas protéger tout le monde et répondre à toutes les menaces de sécurité de l'utilisation malveillante du DNS. Cette réponse est une partie importante.

Prochaine diapo.

Maintenant, comme Matthias l'a déjà ou l'a souligné tout à l'heure, il faut faire très attention, il ne faut pas aller contre la liberté sur

l'internet. Donc on parle des informations invalides, et il faut pouvoir donc avoir la liberté de partager des informations.

Les restrictions sont mises en place pour qu'il y ait un flux libre des informations. Il faut que ce soit bien aligné avec les requêtes qui sont mises en place, ou les exigences en place.

[L'idée c'est l'extension du cadre de la convention de Budapest au niveau mondial…]

Et puis il y a des propositions qui flottent ce sens. Je ne dis pas exactement que le traité des Nations Unies traitera directement, mais nous pensons que des idées en ressortiront.

Donc on parle de cybercriminalité et aussi de criminalité de l'information et on parle de la sécurité de l'information. Les gouvernements ont quelque peu le contrôle de leurs informations et savoir quelles sont les informations, quelles sont les informations des individus qui doivent être protégées.

Il y a donc des idées qui n'ont pas de consensus au niveau mondial, il y aura de la fragmentation et des sphères d'influence au lieu d'obtenir une réponse globale à cela. Et c'est ce qu'on attend depuis cette convention de Budapest.

Prochaine diapo s'il vous plait.

Alors, c'est quoi la convention de Budapest ? Il s'agit de lois pénales qui doivent être mises en place pour des infractions spécifiques contre ou au moyen de système informatique. Il doit y avoir des pouvoirs

procéduraux assortis de garanties pour enquêter sur la cybercriminalité, recueillir des preuves électroniques en rapport avec toute infraction, ils doivent aussi s'engager dans une coopération internationale en matière de criminalité et de preuve électronique.

Ce traité a 20 ans, à peu près 20 ans, mais il contient des informations de guidage, ce sont des notes d'orientation du moins. Il y a donc là un protocole sur la coopération renforcée en matière de cybercriminalité. Et, couramment, un protocole est donc en négociation sur la cybercriminalité et sur les preuves électroniques.

À Budapest, cette convention a établi des standards ou des normes communes pour tout ce qui est protection des enfants, etc. Et nous avons aussi le comité de la convention sur la cybercriminalité. Et ensuite nous faisons du renforcement de capacité avec le [CPROC] qui concernait les programmes de coopération technique.

Donc la convention de Budapest c'est tout cela, c'est un mécanisme et pas seulement un traité. Il y a 65 parties du moins d'États membres qui ont adhéré à cette convention de Budapest.

Prochaine diapo s'il vous plait.

Si vous voyez cela par rapport à ce qu'il s'est passé avec la Covid, et que vous parlez de tout ce qui est hameçonnage, logiciel malveillant, rançon-logiciel, réseaux zombie, etc. souvent, en combinaison avec toutes ces dispositions, il y a donc des orientations dans ce sens pour tout ce qui est, encore une fois, toutes ces utilisations malveillantes du DNS et sa relation avec la criminalité.

Les parties ont criminalisé… Pardon… Donc on a découvert des crimes, des cybercrimes qui sont en relation avec la Covid. Nous avons donc des investigations en cours pour fournir des preuves, dans les articles 16 et 17, ensuite il y a dans l'article 19 on parle d'ordre de production, dans l'article 20 et 21 de perquisitions et de saisies. Donc le cadre de travail est en place.

Donc, après cette convention, ce type d'utilisations malveillantes est devenu criminalisé, cela veut dire que maintenant il peut être investigué, donc il peut y avoir des investigations ou des enquêtes à ce sujet.

Vous voyez les 65 parties, nous avons le Pérou, la Colombie, il y a beaucoup d'autres pays qui posent des problèmes. Comme vous le voyez, comme les pays d'Europe par exemple, nous avons aussi trouvé des problèmes au Sri Lanka, au Japon, au Sénégal, au Botswana ; à l'ile Maurice, au Cap Vert, au Canada, le Costa Rica, l'Argentine…

Donc ce n'est pas seulement un instrument européen, c'est un instrument au niveau mondial. Mais en plus de ces États qui sont des États parties, il y a une demande pour que cette convention soit appliquée avec 150 pays qui vont appliquer cela au niveau de leur droit interne. C'est très important de comprendre cela.

Prochaine diapo.

Bien, comme je l'ai dit, il y a un nouveau protocole qui est en cours de réalisation et d'application depuis 2017. On va commencer des

négociations avec une série de choses qui vont être faites et l'objectif est qu'il soit ouvert pour pouvoir être signé à partir de 2021.

Alors, pourquoi est-ce que c'est un nouveau protocole ? C'est très important parce qu'il y a une question de territorialité, de juridiction en ce qui concerne donc l'informatique en nuage, la territorialité du droit. Si on veut avoir des preuves, on peut changer de pays, on ne sait pas où se trouve les coupables et donc on a un problème complexe de territorialité et de juridiction qui fait que, parfois, on ne peut pas avoir d'efficacité, l'entraide judiciaire n'est pas suffisante. On a besoin d'un nouveau protocole et on a commencé à travailler là-dessus il y a 3 ans.

Prochaine diapo.

De manière brève, voyons quels sont les éléments de ce protocole. On ne peut pas aller très loin parce qu'il y a des points qui sont encore en cours de négociation, mais je dirais qu'il y a des dispositions pour plus d'entraide judiciaire, une coopération plus efficace en cas d'urgence, avec un processus juridique qui va continuer. Et il est important aussi que l'on puisse travailler à travers une assistance, une entraide judiciaire mutuelle, de façon à obtenir cette assistance dans le cadre de ce protocole. Mais il y a aussi une autre disposition qui fait que les pays peuvent utiliser leur droit local pour certains contenus, en cas d'urgence, et les divulguer à d'autres parties.

Et c'est très important, c'est une disposition qui est très importante parce qu'elle concerne la coopération.

Ensuite, cette idée selon laquelle les autorités d'un État, d'un pays, peuvent coopérer directement avec un fournisseur de service dans une autre juridiction, dans un autre pays membre.

Aujourd'hui je suis en Roumanie, à Bucarest, et on peut coopérer directement avec des fournisseurs de service en Norvège par exemple ou dans d'autres pays. Et, pour pouvoir faire cela, on a publié une disposition préliminaire qui indique que l'on peut donc coopérer et il y a des protections dans ce sens, des sauvegardes de protection de donnée.

Et puis il y a un point qui est très important et très intéressant pour la communauté de l'ICANN, c'est la possibilité de considérer les bases légales pour demander la divulgation des informations WHOIS pour un bureau d'enregistrement ou un opérateur de registre. Cela a été en cours de négociation, on devrait bientôt avoir un rapport préliminaire là-dessus, et les différentes parties prenantes pourront à ce moment-là y participer.

Il s'agit ici de compléter la base légale pour les mécanismes et les procédures qui existent, les outils qui existent, et qui découlent du processus réalisé par l'ICANN. Et tout cela en cas d'urgence et de coopération accélérée. On va avoir une opération directe avec une divulgation des données WHOIS et des sauvegardes de protection de données, toujours dans ce protocole, en fonction du RGPD, selon la perspective européenne, mais aussi pour que tous les pays, les États parties de ce protocole puissent y participer et l'appliquer. C'est un processus compliqué, parfois frustrant, mais je pense que dans les

prochains mois à venir on va avoir un protocole préliminaire qui sera bientôt disponible, en tout cas je l'espère l'année prochaine.

Dernière diapositive : les conclusions.

Quel que soit ce qui arrive dans d'autres forums, aux Nations Unies ou ailleurs, on pense que la Convention de Budapest avec son protocole futur va rester la norme internationale la plus importante en ce qui concerne la cybercriminalité.

Les délits concernant l'utilisation malveillante du DNS sont couverts par la convention. Les dispositions de coopération internationales et procédurales pour enquêter sur ces utilisations abusives du DNS. Les discussions sont en cours et sur la possibilité d'inclure une base légale pour des demandes ou pour des divulgations d'enregistrement de noms de domaine et d'informations liées à ces enregistrements de nom de domaine à travers toutes les parties prenantes et les pays parties de ce protocole.

Je vous remercie.

JOANNA KULESZA: Merci beaucoup Alex. Je vois qu'il y a beaucoup de questions qui sont en train d'apparaitre dans le chat. Il y a des questions liées au développement de capacité, ça intéresse beaucoup de gens. D'autres concernent certains aspects spécifiques de la convention.

Ce que je voudrais faire maintenant, c'est donner la parole à Hadia. Si Hadia peut prendre la parole nous allons lui donner la parole pour voir

ce qu'elle pense, donner la parole à nos participants et ensuite nous passerons aux questions et nous demanderons à Alexander s'il veut répondre aux questions l'une après l'autre ou à plusieurs questions en même temps.

Et nous allons commencer par Hadia. Hadia, allez-y vous avez la parole.

HADIA ELMINIAWI: Merci Joanna. Ma question porte sur ce qui vient d'être dit et sur la convention de Budapest qui est le seul traité international quand il s'agit de lutter contre le cyberdélit, et il est destiné à protéger la société avec des législations appropriées, mais aussi destiné à mettre en place une coopération internationale. Ma question porte sur cette coopération internationale lorsqu'il s'agit de l'utilisation malveillante du DNS et de la cybercriminalité, comme on peut le voir tout cela entre sous le cadre de la convention. Et, est-ce que l'ICANN a un système pour mettre en place cette coopération au niveau international, ou la règlementer ? Parce qu'il est clair que lorsqu'on parle de l'utilisation malveillante du DNS, on parle de cybercriminalité, il y a une série d'actions qui doivent être mises en place. Et ma question donc porte sur l'ICANN et sur la façon dont l'ICANN peut encourager cette coopération. Et puis si on regarde des questions comme le WHOIS, les données d'enregistrement, ces questions pour lesquelles la communauté travaille déjà ensemble sur ces questions, et c'est penché sur ces problèmes.

JOANNA KULESZA: Alex, peut-être que je peux vous parler du processus d'élaboration de politique accélérée, l'EPDP, qui porte sur les données WHOIS. Et Hadia a beaucoup participé à ce processus et a travaillé pour que l'ICANN évolue dans ce cadre.

Est-ce que Alex vous voulez répondre à cette question spécifique ensuite nous passerons à la longue liste de questions que nous avons concernant le travail du conseil de l'Europe.

Je m'excuse nous avons un petit problème de temps. Donc Alex pourra répondre à vos questions par écrit si nous n'avons pas le temps de répondre à toutes les questions aujourd'hui. Alex est-ce que vous voulez répondre à la question de Hadia d'abord et ensuite nous passerons aux autres questions.

ALEXANDER SEGER: Des organisations comme l'ICANN, les organisations comme les fournisseurs de service, les bureaux d'enregistrement, les opérateurs de registre doivent coopérer bien sûr, coopérer avec la justice. Mais lorsqu'il s'agit des actions de la justice, il faut laisser la justice qui lutte contre cette cybercriminalité agir.

Et à propos de WHOIS et autre, je pense que c'est un bon exemple ici. Il serait bon qu'il y ait un mécanisme efficace, avec des procédures qui permettraient d'accéder à ces informations, à ces données WHOIS, mais les autorités doivent avoir une base bien claire dans leur droit

national, et c'est là que la convention de Budapest joue un rôle important.

Donc c'est un effort de coopération, mais je suis convaincu que l'action du droit pénal doit être soutenue.

JOANNA KULESZA: Merci beaucoup. Matthias je vais vous donner la parole. Donc nous allons prendre le premier commentaire.

Judith Hellerstein a posé cette question : est-ce que vous pouvez nous donner un récapitulatif du travail qui a été fait récemment. Au sein d'At-Large nous avons une communauté AFRALO qui travaille beaucoup dans le domaine du renforcement de compétence, est-ce qu'il y a des membres de cette communauté ici ? Et peut-être qu'on pourrait en tout cas entendre parler du travail que vous faites dans le domaine du renforcement de compétence sur le thème de la cybercriminalité, même pour les pays qui n'ont pas ratifié cette convention.

ALEXANDER SEGER: Oui, d'accord. En 2013, on a décidé d'établir un programme de cybercriminalité spécifique qui a été diffusé dans le monde pour renforcer le droit et la législation nationale. Il y a un bureau qui est situé à Bucarest, qui a commencé à travailler en 2014. Nous avons fait une série de cours de renforcement de capacité, en Afrique, en Asie, en Amérique latine, sur ces thèmes, sur la cybercriminalité. Nous en

sommes maintenant à la deuxième phase et c'est un projet conjoint de l'UE et du Conseil de l'Europe avec un budget de 19 millions d'euros.

Nous avons tellement de demandes que nous nous sommes focalisés sur les pays qui ont signé cette convention de Budapest. Nous avons une série d'activités qui sont proposées. Nous avons travaillé au Nigéria, au Ghana, au Sénégal, à l'ile Maurice, etc., et nous essayons aussi de soutenir d'autres pays au niveau de leur législation locale, comme par exemple la Namibie, et d'autres pays comme le Congo avec lequel nous travaillons, les iles Fidji et beaucoup d'autres pays.

Mais je dirais que nous avons donc une série de formations et nous travaillons avec plus de 40 pays, et je pense que ce serait le total.

JOANNA KULESZA: Oui, je sais que le Conseil de l'Europe a un bureau très efficace, avec des employés qui travaillent de manière très efficace aussi.

Nous avons deux questions. La première question de Stéphanie Perrin qui est un membre de l'ICANN très actif, qui se focalise sur les questions de sécurité et les questions de protection de la vie privée. En ce qui concerne, donc, les protections pourquoi est-ce qu'on ne doit pas rendre cette signature obligatoire ?

Et la deuxième question de Stéphanie en termes de juridictions, est-ce qu'il va y avoir un bureau de supervision des données de WHOIS et est-ce qu'on a besoin de solutions dans le domaine de la protection de

données. Je voudrais savoir si vous avez davantage d'informations puisque la communauté d'At-Large s'intéresse toujours beaucoup à ces questions. Donc est-ce que vous pourriez nous donner votre opinion concernant la cybersécurité et sur ces questions. Merci. Alex.

ALEXANDER SEGER: Je suis heureux d'y répondre et de faire d'autres remarques d'ailleurs. Je pense que sur la deuxième ou troisième diapo j'ai parlé des lois pénales pour la protection. Il faut donc règlementer nos gouvernements, les autorités politiques, pour interférer. Il ne faut pas que la criminalité soit protégée, il faut qu'il y ait un espace pour les opérateurs. Il s'agit de la sécurité nationale.

Le problème que nous avons, après les scandales qu'il y a eu, les révélations qui ont été faites, est que les résultats n'ont pas forcément à faire avec la sécurité nationale.

La convention 108 est la version modernisée. Mais ce n'est pas une coïncidence que les parties non européennes, les parties non européennes, comme l'ile Maurice, le Sénégal, l'Argentine et d'autres pays font partie aussi de la convention 108, c'est très important.

Comme je l'ai dit, nous soutenons la Namibie et d'autres pays dans ce qui est de la législation, mais beaucoup d'autres en ont besoin, au Sri Lanka aussi il y a des besoins, nous travaillons avec eux et dans beaucoup d'autres pays. Donc nous sommes vraiment favorables à cela.

Après la convention de Budapest et ce protocole qui a été mis en place, il est difficile de mettre ces normes en œuvre, pour référencer cela vis-à-vis d'autres normes qui sont déjà en place.

Une des provisions, des sous-provisions essentielles au niveau des autorités de supervision qui sont requises par le protocole sur la supervision des données et qui a été développé pour respecter le WHOIS, donc encore une fois une partie transfère des données à une autre partie, il faut s'assurer que ces données soient protégées d'un côté comme de l'autre.

JOANNA KULESZA: Merci Alex. Il nous reste 12 minutes. Nous avons des questions un peu plus d'ordre général. Olivier Kouami qui pose cette question : quelle est la relation entre la convention de Budapest et la convention de Malabo. Je pense que cette question est aussi pour Alex.

ALEXANDER SEGER: La convention de Malabo, de l'Union Africaine, va au-delà de la convention de Budapest, parce que la convention de Budapest se préoccupe de protection des données et il faut regarder dans ce cas quelle est la relation entre la cybercriminalité comme elle a été traitée par la convention de Budapest et celle de Malabo.

Nous en avons parlé, nous avons analysé cela en beaucoup de détails avec l'Union Africaine, nous voyons cela comme quelque chose qui est complémentaire, parce que la convention de Malabo est limitée à

l'Afrique, et donc elle n'a pas de disposition spécifique au niveau international pour sécuriser donc les preuves électroniques. Elle a été adoptée par les entités gouvernementales. Et ensemble nous pouvons mettre en place des directives qui conviendraient à la convention de Malabo et celle de Budapest.

JOANNA KULESZA: Merci Alan. J'ai encore une question générale qui vient de Siva : est-ce qu'il pourrait y avoir des juridictions croisées et qu'il puisse y avoir un processus qui soit rapide, rapide du moins direct ?

ALEXANDER SEGER: Oui, je ne sais pas ce que ça veut dire.

JOANNA KULESZA: Est-ce qu'on peut donc soutenir ces lois rapidement et efficacement ?

ALEXANDER SEGER: Il y a dans la convention de Budapest un nombre de mesures qui permet donc une action immédiate. Un coup de fil, un courriel, etc. Il y a plusieurs dispositions de cette convention de Budapest qui incluent ce genre d'intervention.

Dans ce protocole qui va venir, il y aura des mesures qui iront un peu plus loin et qui iront directement vers des FAI et d'autres parties pour essayer d'endiguer le problème. Ce sont des sauvegardes qui sont intégrées. Et ce protocole fournira donc un moyen d'exécution plus

rapide pour pouvoir endiguer le problème plus rapidement. Je l'ai mentionné sur l'une de mes diapositives.

S'il y a donc un cas d'urgence, s'il y a une attaque terroriste et là on a besoin d'accès aux données, on doit savoir qui est impliqué, ce qu'il s'est produit et regardez ce qu'il s'est passé à Paris, etc.

Il y a donc deux dispositions qui sont en place, qui peuvent agir rapidement, et qui peuvent avoir accès aux données rapidement. Oui, il y aura donc des moyens qui seront plus efficaces pour agir au niveau de la justice. Et ça c'est très important, pour maintenant et bien sûr pour l'avenir.

JOANNA KULESZA: Une autre question de la part de Judith, qui a posé une question : est-ce que les pays ont besoin de signer tous les protocoles supplémentaires et comment cela fonctionne-t-il ?

ALEXANDER SEGER: Vous ne pouvez pas rejoindre le protocole si vous n'avez pas signé la convention, ça va la main dans la main. Maintenant nous recommandons le deuxième protocole. Le premier protocole de 2003 était lié à du racisme vis-à-vis d'un système informatique. Donc maintenant, dans certains pays, les États-Unis en font partie, la liberté d'expression est tellement protégée, donc ils disent qu'on ne peut pas rejoindre ce protocole, on ne peut pas faire partie de ce protocole.

Donc il y a différentes parties, 65 parties, 30 parties qui ont ratifié la convention de Budapest avec le premier protocole. Pour ce deuxième protocole qui va suivre, il y a quand même des mesures très attrayantes pour beaucoup de pays puisque là on parle de données WHOIS, il y a donc des mesures qui permettront d'être plus sécurisé. Ce deuxième protocole sera donc plus attrayant pour d'autres parties afin qu'ils rejoignent cette convention. Et s'ils ont rejoint le premier protocole, immédiatement ils pourront rejoindre le deuxième protocole.

JOANNA KULESZA: Oui, c'était très clair oui, c'est quelque chose que nous avions dans les commentaires aussi. Donc nous avons parlé de la liste qui devrait utiliser en termes d'actes illégaux en parlant des messages haineux et l'utilisation illégale encore une fois.

Donc il nous reste 5 minutes et ce que j'aimerais qu'on puisse faire puisqu'il nous reste 4 questions, je voudrais demander aux panélistes de répondre sur le chat. On nous a dit que nous serons pénalisés si nous dépassons notre temps imparti. Je ne peux pas me le permettre. Donc je vais trier toutes ces questions et les faire passer aux panélistes qui sont concernés.

Donc je voudrais passer aux questions rapidement et j'espère que je vais pouvoir donc m'en occuper. D'abord, Élisabeth : y aura-t-il au niveau juridique pour les demandes de divulgation des informations

d'enregistrement des noms de domaine à travers les parties pour ce protocole ? Par les parties ? on veut dire par là les gouvernements.

Il y a Siva aussi qui demande si les forces de la loi pourraient venir avec des propositions avant même que les problèmes se produisent. Donc encore une fois on parle de créativité.

Rick aussi : la Commission américaine a vu une augmentation de la fraude en ligne durant la pandémie et il y a donc des problèmes de données à cause du RGPD. C'est la fin de la question.

Ensuite il y a une question de la part de Zakir : merci pour la discussion intéressante, ma question est pour Alex. Puisqu'il y a un débat assez important sur le traité des USA sur la cybercriminalité, donc proposé par la Russie, qui a déjà eu un soutien considérable, est-ce que vous pensez que les deux, que ce soit le traité sur la cybercriminalité des Nations Unies et la convention de Budapest avec son nouveau protocole pourront coexister et collaborer ? Donc je suppose qu'on pourra vous donner des détails là-dessus. Donc il y a la discussion sur la cybercriminalité dont on parle à l'ICANN, il y a aussi une discussion nouvelle qui a été initiée en dehors de l'ICANN.

Il y a une question sur la dernière diapositive : quand il s'agit des requêtes au niveau des données WHOIS, vous avez mentionné la consultation, Alex, des parties prenantes diverses au sein de l'ICANN pour collectionner, confronter, consolider les opinions sur cela. Comment allez-vous le faire et dans quel délai ?

Alex vous avez quelques minutes pour nous donner une information rapide, du moins donc brièvement si vous pouviez analyser tout cela. Merci.

ALEXANDER SEGER: La première question avait pour but de parler des protocoles, l'accès de WHOIS, qui a accès donc. La convention de Budapest donc a des compétences et donc donne la possibilité pour les autorités de la justice de faire des demandes. Ces entités sont très conservatrices. Et là il y a des problèmes de juridiction bien sûr qui doivent être définis au niveau international. Ils sont très créatifs maintenant pour pouvoir justement faire face à cela. Donc avec ce nouveau protocole on va pouvoir avancer.

Si j'ai bien compris de la part des forces de l'ordre, oui, il y a de la collaboration dans ce sens. L'investigation de ces problèmes demande l'accès aux données WHOIS qui sont limitées.

Le traité des Nations Unies, je ne suis pas sûr que ça devrait être appelé comme ça, peut-être que ça devrait être appelé un traité sur l'information. Mais il y a d'autres traités des Nations Unies qui font du travail sur la corruption et d'autres domaines. Ils peuvent bien sûr coexister tous ces traités, mais on ne sait pas encore exactement quel sera le contenu, à savoir s'ils comprendront tous les crimes qui correspondent à tout cela. Je ne sais pas.

Quand il s'agit de la consultation sur les protocoles, qui a été discutée l'année dernière, donc en novembre, à l'époque on ne parlait pas de

WHOIS, on parlait d'autres éléments. Il y avait des représentants de l'ICANN, il y avait d'autres personnes concernées. On doit discuter au sein des parties qui négocient pour savoir si la proposition qui [est liée] à WHOIS est toujours en cours. Nous aurons donc des détails sur ces consultations avec les parties prenantes et nous espérons que la communauté ICANN y participera. Il y aura donc des possibilités pour faires des commentaires, des propositions.

En tout cas on pourra faire une réunion virtuelle avec la possibilité de discuter des différents commentaires reçus et nous montrerons comment on peut tenir compte de ces commentaires.

JOANNA KULESZA: Oui, bien nous sommes sur la fin de notre réunion. J'avais promis à Matthias qu'il allait pouvoir prendre la parole. Matthias allez-y.

MATTHIAS HUBODNIK: Oui, je voudrais d'abord vous remercier pour cette discussion des plus intéressantes. J'espère que nous pourrons répondre à ces questions par la suite.

On nous parle de protection pour protéger les utilisateurs finaux contre l'utilisation malveillante du DNS et, comme je l'ai dit dans ma présentation, nous avons ce cadre applicable aux cas d'abus qui vise, justement, à offrir un cadre de protection.

Donc différents efforts sont réalisés, comme je l'ai déjà dit, pour remédier à ces problèmes. On coordonne encore la partie légale en

fonction des pays où cela a lieu. Et le problème est que nous avons encore besoin de solutions additionnelles, et pour cela toutes les parties prenantes concernées doivent participer.

JOANNA KULESZA: Je crois que c'est une très bonne conclusion. Merci beaucoup Alex d'avoir participé à cette conférence et d'avoir expliqué à la communauté comment le Conseil a travaillé sur cette convention pour mieux protéger les utilisateurs finaux.

Je vais m'arrêter ici. Je remercie tous les participants à cette discussion, les intervenants et le public. Nous allons continuer à travailler sur l'utilisation malveillante du DNS. Je vous remercie, je remercie nos employés, je remercie les interprètes et le service technique. Merci à tous.

Au revoir.

**[FIN DE LA TRANSCRIPTION]**