COPENHAGUE – Presentaciones de NextGen
Lunes, 13 de marzo de 2017 – 11:00 a 15:00 CET
ICANN58 | Copenhague, Dinamarca

DEBORAH ESCALERA: NextGen, por favor ingresen. Tomen asiento. Queremos empezar en horario. Por favor cuando vean la señal, esta señal significa que les queda 1 minuto. Yo les voy a hacer esta señal que significa que les queda 1 minuto. Ustedes ya saben que tienen 10 minutos. Son 15 ustedes, así que nos va a llevar bastante tiempo. Les vamos a avisar 1 minuto antes. Si se pasan 1 o 2 minutos no es el fin del mundo, pero bueno tranquilos.

Voy a dar los nombres. [Incomprensible]. Carolina Matamoros o [incomprensible] Matamoros. Ferrari. No sé cómo decir tu apellido. Oh, [incomprensible] es el apellido. Sí, ya sé que es [incomprensible], pero ¿qué quieres que diga: que te llame Ferrari o [incomprensible]? ¿Cómo pronuncio tu apellido? A ver, acércate. Es un apellido muy largo.

Bueno, Sara Dushi. ¿Sara? ¿Te llamo Sara? Jacqueline [incomprensible]. ¿O Jackie? Te voy a llamar Jackie. Katharin Tai, Krishna Kumar. Luã, ¿quieres que diga todo tu apellido?

LUÃ FERGUS: No. está bien.

DEBORAH ESCALERA: Matthias. ¿Digo todo tu nombre completo? ¿Nertil Berdufi? ¿Pronuncié bien tu apellido?

NERTIL BERDUFI: Es Berdufi. Un poco difícil.

DEBORAH ESCALERA: Olga, ¿cómo se pronuncia tu apellido? ¿Kyryluk? Peter Chon. ¿Chon?

Valerie Filnovych. Yousra, ¿cómo se pronuncia tu apellido? Yousra, ¿cómo se pronuncia tu apellido? Usa el micrófono, por favor, que no escuchamos.

YOUSRA HSINA: Hsina.

DEBORAH ESCALERA: Bueno, quiero recordarles que lo que ustedes digan se va a estar grabando, así que cuando se presenten hablen lentamente por favor, preséntense para que todo el mundo sepa de dónde vienen porque tenemos intérpretes que van a estar traduciendo.

Están sentados allí al fondo del salón. Ahora con esto empezamos porque ya estamos un poquito atrasados.

Gracias a todos los que van a participar en esta sesión sobre las presentaciones de NextGen. En primer lugar le vamos a dar la palabra a Abderrahman Ali. A ver si ponemos su presentación en pantalla.

ABDERRAHMAN AIT-ALI: Hola a todos. Hoy voy a hablar sobre cadenas de bloques. Me voy a parar por allí. No funciona.

Bien. Está funcionando.

En primer lugar voy a explicar lo que son las cadenas de bloques, algunas de sus características. Les voy a hablar un poco de su historia. No es una historia muy larga. Y les voy a mencionar algunas de sus aplicaciones. Una idea es un proyecto en el que estuve trabajando y es una idea que podría desarrollar la ICANN. Después voy a dar algunas conclusiones.

Bien. ¿Qué es la cadena de bloques? Es básicamente ledger público de par a par, peer to peer, que se utiliza para hacer una transacción. Es un mayor publico. Se hace una transacción que se registra en un mayor, en un libro contable. Se utiliza para estas herramientas criptográficas. La idea es tener una lista encadenada de registros o pedidos. Aquí tenemos algunas de las

características de las cadenas de bloques, que son muy interesantes a nivel de los servicios de internet. Uno de ellos es la apertura. Esto está abierto. Todo el mundo puede abrirlo y hacer un aporte al libro mayor.

La descentralización es una característica muy importante. Nadie controla este libro mayor. Es descentralizado. La seguridad es también muy importante. Este libro mayor, el sistema de almacenamiento y de verificación utilizan la criptografía. También la flexibilidad. Es un sistema distribuido, así que tenemos un proceso de replicación en todo momento. Hay otras características como inmutabilidad. Lo que está en el libro mayor, lo que se registró no se puede modificar.

Consenso. Esto tiene que ver con la confianza, como los bitcoins. Y trazabilidad son bloques encadenados, donde se puede hacer un seguimiento de todas las transacciones. Acá tenemos un ejemplo. El bitcoin, que es un ejemplo de las cadenas de bloques. Es una criptomoneda. Está basada en cadenas de bloques. Esto es solamente una aplicación de las muchas que puede haber. Aquí tenemos un poco la historia. Todo esto empezó a principios de los 90. No es una tecnología muy antigua. Empezó con un trabajo de investigación relacionado con la criptografía. Después hubo un mecanismo, un concepto, que fue introducido por Nick [incomprensible]. Es solamente un concepto. Se llama bitgold (bit oro). La ejecución

de este concepto fue llevada a cabo por [incomprensible]. Se transformó en los bitcoins.

Después hubo otra ola de aplicaciones, que llamamos cadenas de bloques 2.0, que va más allá de las criptomonedas en las aplicaciones financieras. Después voy a hablar de algunas de estas aplicaciones. Esto es como un espectro de las diferentes aplicaciones de cadenas de bloques. Es como una canasta que todos los días presenta nuevas aplicaciones y que incluye las monedas digitales. Todo empezó con las monedas digitales. Ahora pasamos a contratos inteligentes, seguridad, los registros, y hay muchas aplicaciones. Imagine usted cualquier tipo de aplicación que puede utilizar este concepto y ahí ya tenemos la aplicación.

La aplicación más común se ve en el sector financiero. Tenemos las criptomonedas. Como ya dije antes, la bitcoin. Tenemos otra criptomoneda, que es [incomprensible]. Empezó siendo una criptomoneda, pero ahora esto pasó a contratos inteligentes, que es una forma de utilizar protocolos informáticos para llevar a cabo transacciones y contratos. Un producto muy famoso es el proyecto [incomprensible]. Están trabajando en contratos inteligentes, viendo cómo aplicar las cadenas de bloques a los contratos. También hay financiamiento, que es un poco el proyecto en el que yo estoy trabajando.

Este es un mapa de las diferentes empresas y proyectos que están desarrollando aplicaciones financieras. Hay muchas empresas porque hay mucho potencial, muchos incentivos financieros.

La internet de las cosas. Es otra aplicación, otra área de aplicaciones. Otra área donde se pueden utilizar las cadenas de bloques. Una aplicación importante que va a cambiar de alguna manera la internet o los servicios de internet en el futuro es la identidad digital. Hay muchos productos que se están desarrollando aquí para utilizar las cadenas de bloque para definir a las personas a nivel digital. También hay muchos proyectos que se están desarrollando en el área de la seguridad del internet de las cosas para reducir las vulnerabilidades.

Hay otras aplicaciones. Una de ellas es una aplicación en la que nosotros pensamos y que la ICANN podría utilizar. Ayer participamos de las sesiones de DNSSEC y una de las formas de mejorar más la seguridad del sistema de DNS sería utilizar una escritura de sistemas distribuidos con cadenas de bloques. Esta es una aplicación de interés para la ICANN.

Otra aplicación interesante es un proyecto en el que estoy trabajando, que tiene que ver con ONG, financiamiento, con unir a las ONG con los financiadores. Es utilizar las cadenas de bloques como un sistema de transacciones descentralizado, de

modo que las ONG y los filántropos o los entes de financiamiento pueden intercambiar dinero sin necesidad de recurrir a un tercero o una autoridad central, como los bancos. Es un proyecto, y todos pueden visitar el sitio web que figura aquí para encontrar más información.

Hay muchas comunidades que están trabajando en estas aplicaciones de cadenas de bloques y diferentes proyectos e iniciativas. Dos de ellas son la cumbre de cadenas de bloques [incomprensible] o el grupo de interés especial en cadenas de bloques de la ISOC (internet society). Si les interesan estas aplicaciones, pueden participar de estos dos grupos. En algunos de estos dos grupos o en los dos, si les interesa.

Estas serian las conclusiones. La cadena de bloques es una tecnología muy nueva. Empezó a desarrollarse a principios de los 90 y tiene muchas características interesantes que todos buscamos en un servicio de internet. Tiene una amplia gama de aplicaciones, pero hay muchos temas y asuntos que es de esperar que nuestras comunidades encaren para resolver. Muchos de estos temas tienen que ver con las normativas, la privacidad, la integración, la escalabilidad. Y hay muchos nuevos temas y problemas que van surgiendo a medida que avanzamos. Y eso es todo. Muchas gracias.

DEBORAH ESCALERA: Bueno, les pedimos que las preguntas que tengan los NextGen las guarden para el final de la sesión, pero si hay alguna pregunta del público la pueden hacer ahora.

ORADOR DESCONOCIDO: Hola. Quisiera saber si puede explicarnos un poco más de qué manera la cadenas de bloques pueden ayudar a la seguridad del DNSSEC y a todo el sistema de seguridad en general, todo el sistema de DNS.

ABDERRAHMAN AIT-ALI: DNSSEC. Como vieron en esta diapositiva de las características de las cadenas de bloques, hay una que tiene que ver con la flexibilidad. El hecho de que es un sistema distribuido eso aumenta la flexibilidad del sistema de DNS. Pero hay un problema aquí con la escalabilidad que habría que resolver. Yo creo que una de las aplicaciones que impulsará las investigaciones y el desarrollo en términos de la escalabilidad de las aplicaciones de cadenas de bloques sería el uso de estas cadenas de bloques para el DNS.

DEBORAH ESCALERA: ¿Hay alguna otra pregunta? ¿No? entonces ahora le damos la palabra a Carolina Matamoros.

CAROLINA MATAMOROS: Buenas tardes a todos. Soy Carolina Matamoros. Voy a hablar sobre la perspectiva de defensa de seguridad y la necesidad de tener una internet segura versus la necesidad de tener una internet abierta. Para esto, voy a hablar sobre esta triple intersección que incluye defensa y seguridad, pero es defensa y seguridad desde un punto de vista más amplio. Desde el punto de vista de lo que son la defensa y la seguridad y no solamente la seguridad como la vemos siempre.

Empecemos entonces con esta introducción de lo que significan defensa y seguridad. Tiene que ver con los estados y los individuos. Cómo protegerlos. El concepto de protección es muy importante aquí. Más importante de lo que todos pensamos. También tenemos que pensar en la soberanía de los estados. Cómo defenderla y protegerla, y especialmente cómo hacerlo en todos los dominios. Todos los dominios deben estar protegidos. Esa es la perspectiva que tiene cada país, cada nación. Además también desde el punto de vista de la seguridad, especialmente aquí en Europa, es el concepto de la seguridad humana. Cómo protegemos a los individuos de todos los posibles peligros. Cómo podemos permitirles que se sientan libres, plenamente libres y protegidos. Eso es lo que significa seguridad.

Para hacer esto, tenemos las fuerzas armadas, la policía. Y estos organismos son los que aplican la ley y los que en teoría podrían garantizar estos derechos. Están allí para protegernos, en teoría por lo menos. Una vez más no debería dedicarle tanto tiempo a esto. La internet está abierta, tiene una plataforma, es abierta, nos permite innovar, crear, conectarnos. Todos estamos aquí por todo lo que se puede hacer con internet y cómo nos puede afectar en todos los niveles.

Vamos a gobernanza. Gobernanza es la posibilidad de gobernar algo correctamente. Un estado, una persona, toda una organización. Entonces puede ser una gobernanza local, nacional, global, pero exige que alguien ejerza la gobernanza, y alguien que sea gobernado.

Volvamos a la intersección. Hablemos de la intersección entre seguridad y gobernanza. Para que esto funcione debemos saber a quién estamos gobernando, protegiendo. En general esto se define de maneras diferentes, según las constituciones o tratados. Hay que definir a quién estamos defendiendo, según las diferentes legislaciones. También es importante saber que no hay una fuerza global de defensa de seguridad. Simplemente hay coordinación entre los estados. Los estados se coordinan entre sí para brindar seguridad a nivel global, pero es un proceso muy difícil basado en la coordinación y el consenso, y

que es bastante difícil de lograr. Entonces debemos saber que no hay gobernanza sin seguridad y defensa.

La defensa y seguridad y gobernanza dependen de todo esto. Entonces ¿en qué medida se puede aplicar cualquier tipo de defensa si depende de la coordinación a nivel global? ¿Podemos defender algo? es muy difícil. Entonces cuando hablamos sobre gobernanza de internet tenemos muchas cosas que son difíciles, empezando con la legislación nacional. La legislación de los diferentes países no esta alineada con la de otros países. Cada país tiene su propio abordaje, lo que está permitido y lo que no esta permitido, lo que es un delito y lo que no es un delito.

Entre nosotros estamos de acuerdo en que la internet debe ser abierta, neutral e interoperable, pero es difícil por varios motivos. En primer lugar, porque es abierta, libre. Cada persona puede decir lo que quiera. Nadie es responsable por lo que dice o hace en su dominio en el ciberespacio. Esto lleva a diferentes problemas. Podemos decir ahora que estamos en la era de la desinformación porque hay tanta información falsa, que es muy difícil manejarse porque no sabemos qué es cierto y qué no lo es. Entonces no está muy claro a quién están dirigidas las políticas relacionadas con internet.

Entonces ahora hablemos de defensa, seguridad e internet. Aquí el primer tema es que no sabemos quién es el que efectuó el

ciberataque. Como mucho podemos identificar la dirección de IP, incluso eso puede ser complejo. Entonces es muy difícil saber quién hizo algo. También es muy difícil identificar el ataque. Podemos atacar a una identidad. Ustedes pueden robar mi información, mi cuenta bancaria, pero también pueden hackear el sistema de trenes en Alemania. Según lo que estén atacando, cambia el nivel de dificultad para enfrentar esto desde el punto de vista de un país. Si se ataca a un estado, tiene que ver con la defensa nacional y la soberanía. Entonces es un tema que preocupa a todos los países porque todo el mundo está amenazado. No hay medidas de defensa de seguridad que nos permitan estar totalmente protegidos en este dominio.

Es muy interesante lo que estoy mencionando. Estoy hablando de un dominio. Piensen entonces: tierra, aire, mar, espacio. Estos son los elementos básicos del sector de defensa, pero internet es otro sector. También tenemos derechos allí, que deben ser protegidos, como deben ser protegidos los países, pero la jurisdicción, la competencia no están claras. Entonces, ¿cómo nos podemos defender en esas condiciones? Es muy difícil.

Fíjense que hay diferentes tipos de tratados. Un tratado es el realizado en Múnich en el área de defensa. Pueden ver todos los representantes de diferentes países. La ciberguerra es una prioridad. Es la forma más fácil de atacar a otro país. Un país

quizás ni se entere de que otro país lo está atacando. Entonces una prioridad para todos los estados deberían ser los ciberataques.

¿Qué tenemos aquí? Esto tiene consecuencias muy negativas para la apertura de la internet. Los países están preocupados por su propia defensa, pero si no tienen un buen sistema de defensa les preocupará la apertura de la internet. Si no resolvemos esto, la internet va a estar fragmentada. Veo movimientos en los diferentes países con respecto a esto. Hay diferentes países en diferentes niveles. En China, Corea del Norte, Venezuela, incluso Alemania, a veces no se puede descargar algo porque en algunos países es ilegal. Entonces todos los países de alguna manera están tratando de encontrar la forma de defenderse. Es algo que nosotros aquí debemos tener en cuenta; que nos debe preocupar.

Para resumir entonces, en primer lugar, los países quizás estén interesados en fragmentar la internet para proteger su propios países, su propia población civil. En segundo lugar, no hay una aplicación global y creíble de las leyes de la legislación. Esto dificulta la coordinación de los estados porque, aunque estamos de acuerdo en que esto es un problema, no podemos estar de acuerdo en cómo resolverlo. En tercer lugar, la gobernanza global de la internet está más bien a nivel de asesoramiento. Podemos hacer recomendaciones, pero allí se acaba la cosa.

Son solamente recomendaciones y seguimos viviendo con esta amenaza para la internet. Lo que quiero valorar con esto es darles una idea de la urgencia. Aquí en la ICANN debemos hacer algo al respecto.

Entonces para resumir, mientras que no sepamos cuáles son las jurisdicciones y las competencias y cuál es la población que se ve afectada por cada ataque, la defensa en el dominio del ciberespacio no es una verdadera defensa. Mientras que no sea real, estamos bajo la amenaza. Se está amenazando la transparencia, apertura e interoperabilidad de la internet.

Estas son algunas opciones; cosas que podemos hacer. Por ejemplo, tenemos que poder diferenciar la ficción de la realidad, como en una biblioteca. En una biblioteca tenemos una sección sobre historia y de novelas. También el anonimato de los usuarios. Si un usuario [incomprensible] se va a comportar de manera diferente que si pudiera actuar de forma anónima, como los delincuentes. Debe haber una forma de poder aplicar las normativas, la legislación a nivel global. Con esto termino. Muchas gracias.

DEBORAH ESCALERA: Gracias, Carolina. ¿Hay alguna pregunta del público?

ORADOR DESCONOCIDO: Hola. ¿Cree usted que en esas estrategias para la defensa y la seguridad, la ciberpaz podría ser una estrategia posible para ayudar a las comunicaciones entre los países, etc.?

CAROLINA MATAMOROS: Cuando usted habla de ciberpaz, ¿habla de paz en general? Sí. Esto tiene que ver con la confianza que les otorgamos a los civiles. Podemos estar seguros de que todo el mundo va a actuar de forma pacífica, simplemente porque acordamos hacerlo así. No es probable, pero puede ser un principio, como el principio legal que establece que una persona es inocente hasta que se pruebe lo contrario. Sí podemos decir que vamos a actuar de forma pacifica, pero necesitamos medidas que garanticen que cuando alguien no se alinea con esta confianza y nos ataca, podemos llevarlos a los tribunales para contrarrestar su ataque. Incluso aunque tengamos un principio de paz que guie la internet, deben tomarse medidas para poder demandar y enfrentar cualquier tipo de ataque.

Entonces incluso con este principio, incluso si se aplica este principio, todo lo que mencioné es un tema que nos debe preocupar. ¿Hay alguna otra pregunta?

ORADOR DESCONOCIDO: Usted dijo que una forma de lograr un equilibrio sería poner fin al anonimato de los usuarios de internet. ¿Cómo jugaría esto con el tema de la privacidad?

CAROLINA MATAMOROS: Hay diferentes formas de encararlo porque la privacidad es un tema que preocupa a todos los usuarios de internet y según el país a algunos les preocupa más o menos. Entonces la forma de encarar esto varía de país a país. Podemos decir: "Usted puede hacer esto en forma voluntaria, revelar su identidad". Y también se podría hacer en diferentes tipos de dominios. Quizás uno no quiera ser anónimo si se contacta con su cuenta bancaria porque todos los que entren en un dominio de un banco van a hacer una transacción, por lo menos en teoría. Entonces mientras que todas las personas que entren en el dominio del banco estén identificadas, uno se siente seguro. Pero si quieren visitar por ejemplo Wikipedia, ahí uno puede actuar de forma anónima.

Quizás en ciertos sitios se pueda actuar de forma anónima y en otros, no. pero la preocupación respecto a la privacidad, tiene más que ver con la confianza que se tiene en los gobiernos, como por ejemplo quién va a utilizar esta información. Si yo doy mi identificación personal a alguien, ¿la va a usar para algo? bueno, depende de la frecuencia con la que esto pase, pero

mientras la información esté allí disponible esto es una amenaza. Desde el punto de vista realista, yo diría que hoy no hay privacidad tampoco. Entonces si uno comunica su identidad porque uno confía en su gobierno (confía en que el gobierno nos va a proteger) quizás podamos ganar más privacidad a través de otras entidades, pero por supuesto es un debate que debemos llevar adelante porque hay ciertas contradicciones aquí y estoy de acuerdo con lo que usted mencionó.

DEBORAH ESCALERA: Un segundito, que resuelvo algunas dificultades técnicas, y luego va a continuar Chawana.

Nuestro próximo orador es Chawana Huangsutomachai.

CHAWANA HUANGSUTOMACHAI: Señoras y señores, espero que me presten atención durante unos 10 minutos o menos. ¿Hay algún danés por acá? ¿No? ¿Sí? Ah. Hola.

[HABLA EN DANÉS]

Buenos días, señores y señoras. Mi nombre es Chawana Huangsutomachai. Pueden llamarme Ferrari, que es mi sobrenombre. Provengo de la universidad de [incomprensible], de Holanda.

Hoy vamos a hablar sobre este tema. Vamos a tener la versión 6 de IP (IPv6). A mí se me ha ocurrido una idea. Es una idea muy fantasiosa. ¿Qué pasaría si tuviéramos una dirección IP personal? Una dirección IP estática para todos. Como si fueran números de identificación para todos en todo el mundo. Tipear una dirección IP y ahí aparecemos nosotros. Aparece una persona. Entonces sí, tal como dijeron los oradores anteriores, hay una parte esencial de la internet que es la anonimidad, el anonimato.

La falta del anonimato. Algunos dicen que el anonimato en el mundo de internet existe. Nadie sabe si uno es un perro, con todo respeto. Básicamente eso significa que nadie sabe quiénes somos. Ahora, si la dirección de IP representa a una persona, ahí dejaremos de perder el anonimato. ¿Qué ocurre en el contexto legal? Debo decir una cosa. Esto es algo muy subjetivo. Si es bueno o malo depende de cómo se lo mire.

Efecto sobre el gobierno. La vigilancia será más fácil porque en general la dirección de IP se recopila a través de los ISP. Pero es posible que los gobiernos tengan una base de datos que digan: “Esta persona tiene esta dirección IP”. Entonces si quieren identificar a alguien va a ser mucho más sencillo. Entonces aplicación de la ley, investigación, especialmente el área de los delitos cibernéticos. Voy a explicar esto brevemente. Si alguien comete un delito cibernético, los gobiernos, los organismos de

aplicación de la ley, van a trabajar en primer lugar con la dirección IP porque en general no saben quién está detrás de una dirección IP, pero ahora quizás sí lo sepan. Si tenemos una dirección IP personal, esto va a sortear algunas dificultades. Va a ser más fácil. Pero hay algunas cosas buenas, creo yo. Esto mejoraría la protección de los ciudadanos frente a procedimientos ilegales porque si saben quiénes somos, si saben dónde estamos. Entonces podemos decir: “Yo estoy acá. No te metas conmigo”.

Tema de protección de datos. Vamos a hablar acerca de la protección de datos. La dirección IP se convierte en datos personales, y los datos personales significan datos que pueden identificar personas. Suena… Especialmente en la era de la internet de las cosas. Ahora tenemos teléfonos inteligentes, tenemos relojes inteligentes, y quizás pronto vamos a tener también zapatos recargables. Sería posible obtener datos a través de la conexión de internet. Con un solo número de identificación tendríamos todo aquello que conectamos a internet, pero también hay algo que se gana y algo que se pierde. Esto podría afectar a la privacidad online. Debido a los números de identificación centralizaría toda la información de una persona en un lugar. Por lo tanto, para cumplir con la protección de los datos esto sería más fácil, pero se necesita una implementación adicional.

La internet en paz. Personalmente creo que internet es bueno, pero detrás de la pantalla, detrás del teclado, hay carne. Hay personas. Si todos saben quiénes somos porque nos identificamos porque la gente sabe cuál es nuestra dirección IP, en ese caso pensaríamos varias veces antes de hacer clic en enter porque acá viene el ciberbulling y otras cosas malas que ocurren debido al anonimato. Esto se evitaría, pero además esto puede tener un efecto de amedrentar a la gente.

¿Qué ocurre con la libertad de expresión? Nuevas oportunidades. Me gustan los monos. Ignórenlo. Nuevas oportunidades y dificultades. El tema es el conflicto de interés. La dirección de IP podría estar por encima de cualquier otro número. Piensen en sus números de teléfono o quizás los números de identificación de los ciudadanos. En Tailandia tenemos un número de identificación de 13 dígitos. Esto podría estar por encima de todos esos números. Podría convertirse en nuevas oportunidades de negocios, pero ¿qué pensarían las empresas de telefonía? Esto generaría por supuesto conflictos de interés. Muchas gracias por su atención.

DEBORAH ESCALERA: ¿Hay alguna pregunta del público?

ORADOR DESCONOCIDO: Estoy de acuerdo con las dificultades que señaló en términos de anonimato. Lo que me preocupa es cómo se implementaría esto porque todos los proveedores de internet dependen de la flexibilidad de las direcciones IP para poder configurar nuevas conexiones. Entonces tener una sola dirección IP por persona seria una gran carga, algo en lo que tendríamos que pensar, pero además tendríamos que coordinar toda esta información en una base de datos central. Todas estas empresas van a estar en conflicto entre sí con respecto a cuál es la información correcta. Quizás tengamos varias direcciones IP iguales, considerando la cantidad de personas.

Entonces me parece que eso sería demasiado difícil. ¿Cómo se podría lograr esto?

CHAWANA HUANGSUTOMACHAI: Estoy de acuerdo con usted. Es una idea que surge de la imaginación, pero ¿quién sabe? Las causas parecen imposibles hasta que finalmente ocurre, así que solo quiero decir que la implementación sería terrible para la gente técnica. Les pido disculpas a los técnicos. Pero es una posibilidad, y no pensé acerca de cómo implementarlo. Sin duda sería un conflicto de intereses.

DEBORAH ESCALERA: Gracias, Chawana. El próximo orador es Clement Genty.

CLEMENT GENTY: Hola a todos. Soy francés. Soy Clement Genty. Soy ingeniero, nada que ver con la contabilidad, la ley, la diplomacia. No. simplemente quiero hablar acerca de las políticas de nombres.

Como habrán visto, soy francés, así que voy a hablar acerca de Francia. Sí. Aquí tenemos un avión fantástico. Es un avión francés. Ahora es un avión estadounidense. ¿Cuál es el tema? Quizás habrán observado que en la cola del avión tenemos un código de identificación. De hecho, en 1944, en Chicago, tuvo lugar una convención para crear la convención de aviación civil internacional.

Hablemos acerca de los amateurs de la radio. En 1927 se creó el código de telecomunicaciones, como observarán aquí. No puedo ir para atrás. Aquí. En 1927 lanzamos este código, y podrán verlo en esta tarjeta de radioclub. W significa EEUU. La F, para Francia. Cuando los científicos crearon el sistema de nombres de dominio, tuvieron la misma idea. Por ejemplo, para el ccTLD de Francia los científicos de [incomprensible], un laboratorio francés, crearon una política de nombres con subdominios. Por ejemplo, arriba tenemos la gendarmería que depende del ministerio del Interior. Sabemos que es un sitio gubernamental porque tenemos .gov.fr. Luego para la escuela

francesa del ejército depende también del ministerio de Defensa y del gobierno de Francia, etc.

EEUU, lo mismo. Jon Postel, que fue el administrador de .us, creó también esto. Pueden ver acá [incomprensible], la escuela que está en California, en EEUU. Después tenemos la ciudad de [incomprensible], en California, y también en EEUU. Después trataron de lanzar el kids.us pero no funcionó lamentablemente. Acá tenemos un collage fantástico en California, en la ciudad de [incomprensible]. Observen que pueden leer el nombre de dominio y confiar en el nombre de dominio. Ustedes saben qué es [incomprensible], universidad, estado, California, EEUU. Acá tenemos la policía de Nueva York. Tenemos police, la ciudad de Nueva York, en el estado de Nueva York, en EEUU, pero el registro se dio cuenta de que podía ganar mucho dinero delegando todos estos subdominios.

Ganaron mucho dinero. Utilizaron esta herramienta de identificación de nombres de dominio. Ahora podemos ser todo. Yo puedo ser un registro de nombre de dominio. Puedo registrar Clement abogado punto Estados Unidos. Nada está prohibido. Las empresas trataron de crear barras de navegación para ayudar al usuario final a confiar en la información que está en internet, pero no funciona. No funciona. Eso es un hecho.

Luego creamos la seguridad SSL. Se puede utilizar Paypal en un sitio web, pero a la izquierda vemos el sitio web de Paypal, que tiene seguridad SSL. A la derecha vemos summary support .com, que tiene seguridad SSL. Observarán que el dominio que está a la derecha también tiene SSL, pero el primer nivel de SSL. Hay tres niveles de SSL.

Entonces no podemos confiar en la información que está en internet. Esa es la realidad. Hoy en día no podemos decir: “Ah, yo conozco el sitio web del gobierno francés”. No podemos decir: “Este es un sitio web real”. A mí personalmente eso me preocupa porque soy francés. En mayo tendremos elecciones presidenciales, y cuando vi lo que pasó en otros países por noticias falsas me preocupo. Entonces este es el tema. No hay nada presente para ganar confianza en internet.

Doy clases en la universidad y le pedí a los estudiantes que me digan qué piensan ellos. Cuál es la forma, qué es lo que les ayuda a ellos a tener confianza en una página web en internet. La adopción es un tema político. Cuando uno tipea “adopción” en EEUU, uno sabe que los jóvenes buscan información médica a través de Google. Hay muchas páginas web, pero hay algunas páginas web administradas por asociaciones.

Yo pedí a los estudiantes, 137 estudiantes, que hicieran un ranking de estos cuatro dominios, en una escala de 1 a 3. Tres es

confío en ese dominio y cero es no confío en este dominio. Pueden ver .gov, .fr son los subdominios en los que más confían (.fr, .org, .net, en ese orden). Entonces lo que quise crear y lo que quiero mostrarles es una herramienta para los usuarios franceses. Digo franceses porque yo utilice un ccTLD que no se utiliza. Como saben, Francia está en el exterior. En Sudamérica hay ccTLD para distintos territorios y países, la Antártida, etc. Nosotros tenemos dos ccTLD. El primero es [incomprensible] acá, el oeste de México. Después tenemos el ccTLD para Francia metropolitana, que es .fx. Y quiero utilizar este ccTLD para mostrarles un ejemplo de internet.

Vamos a crear un espacio de confianza con subdominios para distintas autoridades. Les pedimos a las autoridades… Por ejemplo la asociación de abogados, la profesión de los abogados es manejada por la asociación de abogados en Francia. Sugiero que el CNB, la asociación de abogados, debería administrar el dominio .fx para mejorar la confianza. Lo mismo con respecto a los aeropuertos, a los médicos. En Francia, las embajadas utilizan [incomprensible] punto Francia punto el país, pero cualquiera puede registrar un nombre de dominio .org. Podrán ver fácilmente que Francia registró estos dominios a través de las embajadas y así surgen muchas noticias falsas en internet.

Acá tenemos entonces… ¿cómo puedo explicarlo? No se puede utilizar. Es decir, a veces se utiliza subdominios de acuerdo con una certificación. Quizás no se acordarán. Esto pasó hace 300 años. Se pensó que podríamos dividir la información a través de la memoria, la razón y la imaginación. Entonces yo traté de crear un TLD francés con acreditación de registrador. Acá lo tenemos. Ese es el punto. No se puede confiar en nada de lo que está en internet. Tenemos que encontrar otra forma de ayudar a la gente a acceder a la información. Muchas gracias.

DEBORAH ESCALERA: Muchas gracias. Una vez más los miembros de NextGen, si tienen preguntas, guárdenlas para el final. Ahora quisiera saber si algún miembro del público tiene alguna pregunta.

ORADOR DESCONOCIDO: Tengo una pregunta con respecto a la generación de confianza. En su trabajo, usted consideró otro proyecto llevado a cabo por el investigador y desarrollador de los paquetes [incomprensible] francés. Esto podría utilizarse para estos fines, por parte de cualquiera que no confíe en Francia, por ejemplo.

CLEMENT GENTY: Sí. [Incomprensible] es el inventor de la raíz abierta. Él creó una alternativa europea para Arpanet hace varias décadas. Gracias.

DEBORAH ESCALERA: Sara, un momento. Estamos teniendo dificultades con la computadora nuevamente.

La próxima oradora se llama Sara Dushi.

SARA DUSHI: Buenos días. Soy de Albania. Estoy haciendo un máster en Legislación, Ciencia y Tecnología en Polonia.

DEBORAH ESCALERA: Perdón, Sara. Odio interrumpirte, pero tenemos que cambiar de computadora. Les pido disculpas a todos los asistentes. Un minuto, por favor.

A los miembros del público: a las 12:30 vamos a hacer una pausa para almorzar y vamos a seguir con las presentaciones a la 1 pm. Tenemos varias presentaciones, así que la pausa para el almuerzo va a ser muy breve.

Les pido disculpas. La oradora, Sara Dushi.

SARA DUSHI: Estoy haciendo una investigación en abuso sexual y explotación sexual de niños a través de internet. Quisiera empezar mi presentación con esta frase de 1995: así como las computadoras

han empezado a revolucionar la vida social, también van a revolucionar el delito y las anomalías, especialmente las conductas sexuales anómalas. De hecho esto ya está pasando. Vemos que ya en esa época el ciberdelito empezó a desarrollarse.

Estos son algunos hechos en los últimos dos años. Se aplican a los últimos dos años. En este momento hay 3.400 millones usuarios de web, pero hoy, según dijo Goran, ya tenemos 3.900 millones de usuarios de internet. En 2016, la IWF identificó más de 68.000 páginas web con imágenes de abuso sexual infantil. Esto representa un aumento de 417 años en los últimos dos años. El 69% de los niños en estas imágenes tienen 10 años o menos. La mayoría de estos son niñas. Según los investigadores, lo que los niños perciben como conductas de riesgo en línea, como compartir información personal con extraños o encontrarse con estos extraños, para los jóvenes eso son conductas normales en el espacio informático.

Estas son las formas de abuso sexual en línea. Es abuso sexual infantil. En el pasado esto se daba pocas veces y a través de imágenes que no se transmitían a nivel global. Hoy en día con internet todo es más sencillo. Es un problema global. Hay persecución sexual, invitación u ofrecimiento de servicios sexuales y explotación sexual. Todo esto toma diferentes

formas: prostitución infantil, tráfico de niños con fines sexuales, turismo sexual infantil, etc.

Vamos a empezar con la descripción del problema en el mundo real. En 2007 hubo un caso en el Reino Unido donde se encontraron imágenes de abuso sexual de niñas del sudeste asiático, pero no se pudo identificar al abusador. Había un sospechoso porque era una persona que viaja con frecuencia al sudeste asiático, pero no pudieron demostrar. Esto no fue suficiente para probar y demostrar la persona que había cometido ese delito porque en las imágenes solo se veía la mano de la persona y a los niños de los que se estaba abusando. Se pidió entonces ayuda a un centro de investigación, que con técnicas muy especiales, midiendo los patrones de la piel, métodos que utilizan los forenses, entonces pudieron evaluar el patrón de piel del sospechoso que demostró ser el mismo patrón de piel de la mano que aparece en esas fotos. Esto demostró la conexión entre las imágenes online, que viajaban por internet, y el abuso real que se estaba dando. Las imágenes eran reales y se estaba abusando de estos niños en realidad.

También se demostró que a fin de investigar este tipo de delitos, las autoridades de aplicación de la ley no pueden hacer todo por sí mismas. Necesitan de energía especializada y cooperación de diferentes partes interesadas. También demuestra la escala internacional del problema porque los delincuentes en general

tratan de buscar países donde no haya una legislación muy rígida con respecto al ciberdelito. En este caso una persona de Reino Unido fue al sudeste asiático para cometer estos delitos. También es necesario que diferentes instituciones cooperen entre sí.

Aquí vemos otro ejemplo de 2015, donde [incomprensible], que es una empresa muy conocida de Hong Kong, que ofrece tecnología educativa que es utilizada por niños. Aquí hubo una violación de datos. Puso en peligro los datos de las cuentas de 6.400.000 niños. De estas cuentas se pudieron tomar fotos de los niños, y se pueden relacionar las fotos de los niños con sus nombres y sus direcciones.

Estas son estadísticas globales. Aquí vemos que las imágenes de abuso infantil en general están alojadas en América del Norte y Europa. Aquí vemos la cantidad de dominios que alojan contenido sobre abuso infantil por año. El mayor nivel lo tuvimos en 2007. Aunque el número cayó, vemos que la tendencia es creciente. En 2015 hubo 1.900 dominios con imágenes de abuso sexual infantil.

Mis preguntas de investigación fueron las siguientes. ¿Cuáles son las medidas legales más efectivas para frenar el abuso sexual infantil en [incomprensible]? ¿Cuál es el alcance y la naturaleza de las capacidades internacionales necesarias para

implementar y evitar el abuso infantil y la explotación sexual de niños? A fin de responder estas preguntas, voy a avanzar por cuatro direcciones para identificar las causas de delitos, su prevención e identificación de los mismos y la respuesta.

Metodología. La metodología que estoy utilizando hasta el momento es un análisis de las normas internacionales, análisis del derecho constitudinario y entrevistas cualitativas a gobiernos, comunidad, utilidades de aplicación de la ley. Los puntos críticos que he detectado hasta ahora es que no hay una definición única y uniforme de niño y abuso sexual infantil, contenido con material sobre abuso sexual infantil. No hay una definición estándar de abuso sexual infantil.

Todos sabemos que la tecnología avanza mucho más rápidamente que las normativas y que la legislación. Además es un delito sin fronteras. Esto causa muchos problemas de jurisdicción y competencia. Hay problemas en la comunicación de diferentes países y muy pocas veces estos delitos se denuncian. Muchas veces los niños no los denuncian. Esto solo se encuentra en forma ocasional. En la mayoría de los países no existe un departamento de investigaciones especial dedicado al abuso sexual en línea. En general esto cae bajo la órbita del departamento de ciberdelitos, delitos informáticos, y el personal no tiene tanta experiencia en la investigación de los delitos sexuales infantiles, el abuso sexual infantil.

Además realmente es necesario definir a nivel universal la edad en que se puede dar el consentimiento para participar en actividades sexuales. Esto es un problema porque se trata de un delito que no tiene fronteras. Entonces quizás se puede considerar que el niño sea mayor. Quizás el niño sea considerado mayor en un país, y por lo tanto no se puede demandar a la persona que cometió este delito. También necesitamos un abordaje de múltiples partes interesadas.

Mis conclusiones hasta el momento son las siguientes. Es necesario contar con nuevas investigaciones para el proceso de investigaciones. Una de estas nuevas tecnologías fue presentada en los últimos años en los EEUU por [incomprensible]. Tiene una tecnología spotlight, que utilizan la mayoría de los países para investigar estos delitos. De esta manera es más fácil detectar las imágenes de abuso infantil. Es necesario la cooperación de todas las partes interesadas para identificar el abuso sexual infantil en línea. Yo creo que no debería existir la posibilidad de que algún país no acepte las definiciones internacionales o regionales en cuanto al abuso infantil.

La cantidad y el número de recursos humanos para la investigación de este tipo de delitos son realmente reducidos. También sugiero que es necesario crear un comisionado

regional e internacional para proteger los derechos del niño en línea. Muchas gracias.

DEBORAH ESCALERA: Gracias, Sara. ¿Hay alguna pregunta del público?

Bueno, entonces vamos a hacer una breve pausa para el almuerzo y continuamos con nuestra sesión a las 12:40. Muchas gracias.

NextGen, nosotros vamos a almorzar aquí, así que vamos a ir a buscar nuestro almuerzo y continuamos trabajando.

NextGen, por favor prepárense porque vamos a comenzar enseguida.

Quiero recordarles a todos que por favor bajen el volumen de computadoras y teléfonos durante estas presentaciones y durante toda la semana. Aquellos que usan computadoras para las presentaciones hoy, como Jackie, avísenme y [incomprensible]. Pero de lo contrario por favor tienen que tener las computadoras y los teléfonos apagados durante las sesiones. Si las usan para tomar notas no hay problemas. Otra razón por la cual les dimos los anotadores es para que no usen las computadoras.

Seguramente el público va a volver, pero por una cuestión de tiempo y como tenemos tantas presentaciones, vamos a continuar. La próxima oradora es Jackie Eggernschwiler.

JACQUELINE EGGENSCHWILER: Hola a todos. Es muy difícil volver después del almuerzo. Lo sé. Ya lo vemos. Tal como dijeron, yo soy Jackie Eggernschwiler. Soy investigadora en la universidad de Oxford. El tema de mi presentación es el ciberespacio y la reglamentación y regulación correspondiente.

Voy a hablar acerca de un proyecto sobre este tema. Se centra básicamente en la responsabilidad. Una palabra que ya hemos escuchado varias veces en estos dos días. El modelo de múltiples partes interesadas y el modelo multisectorial son otras palabras que escuchamos varias veces y que volveremos a escuchar en esta presentación.

Voy a darles un poco de información acerca de lo que motivó este proyecto para comenzar. Lo que está ocurriendo en el espacio del que estamos hablando, en este ecosistema de la tecnología digital y en este entorno, son diferentes partes interesadas, distintas esferas de regulación. Además, por supuesto, distintas áreas. No hablamos solamente de la administración del DNS. Hablamos también de la privacidad, temas relacionados con la protección de datos, delitos

cibernéticos. Hablamos acerca de cómo manejar, por ejemplo, una dirección IP digital para todos.

Tal como dijo Chawana, hay muchos temas que surgen aquí. Esto modela. Genera modelos de estructuras de responsabilidad. Considerando la multitud de actores y las áreas de las que estamos hablando, los distintos temas y también, por supuesto, los distintos foros involucrados en este entorno regulatorio, no podemos decir fácilmente: este organismo es responsable de eso y este otro organismo es responsable de lo otro. Vemos estructuras en conflicto que están surgiendo.

Una de las preguntas que guiaron este proyecto fue la siguiente. Desde la perspectiva conceptual, ¿cuáles son los desafíos en relación con la responsabilidad en el área de la gobernanza de internet o del ciberespacio? En segundo lugar, considerando los diferentes actores que interactúan en la importancia de los actores que conforman este entorno, ¿qué clase de responsabilidad surge en este contexto? ¿Es una sola clase de responsabilidad? ¿Son múltiples clases de responsabilidad? En ese caso, ¿cuáles son?

Con respecto a la primera pregunta, parte de la respuesta a la que llegué como parte de este proyecto es la siguiente. Los desafíos que enfrenta este entorno básicamente surgen del concepto básico propiamente dicho. El hecho de que hay

muchas manos que contribuyen a este entorno, vemos una gran cantidad de distintas áreas problemática y vemos un grado híbrido de organizaciones institucionales.

Hablemos primero acerca del problema de muchas manos. Como dijimos, no hay una sola parte interesada (digamos, los gobiernos). Es el sector privado, las personas individuales, las unidades constitutivas, las organizaciones de la sociedad civil. Es difícil tratar de identificar quién es responsable de qué, considerando el grado de complejidad.

La gran cantidad de áreas diferentes. Estas áreas pueden converger si pensamos en los nombres y números, por ejemplo. Pueden surgir temas repentinamente en relación con IP. Ahí una vez más tenemos que preguntarnos cómo podemos manejar esto, cómo podemos resolver esto y quién es responsable de esto.

El grado híbrido de organización institucional. Esto se refiere a una situación en la que tenemos diferentes instituciones y cada vez hay una mayor cantidad de instituciones involucradas en la regulación del ciberespacio. Pero a veces solamente tienen una naturaleza transitoria. Surgen, desaparecen, vuelven a surgir ocasionalmente. Entonces nos enfrentamos con este desafío también.

Con respecto a la segunda pregunta, considerando la prevalencia de estos diferentes actores, ¿qué clase de estructuras de responsabilidad observamos? Yo sostengo que vemos tres clases de estructuras que no son excluyentes, que pueden fusionarse, interactuar, incluso pueden formar nuevas estructuras. Pero estas son las clases típicas de estructuras. La responsabilidad jerárquica, que está relacionada con una situación por ejemplo de responsabilidad clásica, donde se siguen líneas estrictas y verticales de mano, de arriba hacia abajo. El que está arriba tiene la responsabilidad individual de lo que ocurre por debajo de ese nivel. Esa clase de estructura podría surgir por ejemplo en áreas relacionadas con la ciberseguridad, en donde hay personas que son responsables de la falta de implementación de cláusulas en torno a la seguridad.

También vemos un tipo de responsabilidad relacionada con el sector privado corporativo. Esto aparece a través del velo del nivel individual y corporativo. Considerando las prevalencias de estos grandes actores de internet de los que escuchamos hablar y de los que hablamos varias veces, piensen en los grandes: Google, Amazon, Microsoft. Todos los Microsoft de este mundo. Esta es una clase de responsabilidad importante porque por lo menos conceptualmente estas empresas tienen responsabilidad. Ya hemos visto cuáles han sido los grados de responsabilidad de este entorno.

Y finalmente podríamos decir el más importante es el grado de responsabilidad colectiva, considerando el hecho de que las partes interesadas contribuyen a políticas, a resultados de políticas, a resultados técnicos. Si no pueden ser responsables de forma individual, porque no es una única entidad la que decide, entonces necesitamos contar con una clase de instrumento que nos permita hacer una comunidad. Por ejemplo, si es responsable. Esto nos lleva a la idea de que todos aquellos que contribuyen a un resultado, ya sea una política o un resultado técnico, debe ser responsable.

La responsabilidad en este sentido en realidad es un concepto relacional porque se refiere a la obligación de un actor de ser responsable de contactarse con otro actor. El proyecto no proporcionó ninguna respuesta, en cuanto a cómo responder los temas que acabo de plantearles, simplemente queríamos ver cuáles eran las diferentes posibilidades. No hice ninguna recomendación. Pero en términos generales podemos decir que la gobernanza en el ciberespacio les presenta a los investigadores y a los profesionales una serie de relaciones de responsabilidad de distintas clases, de distinto diseño. Lo fascinante es que la responsabilidad, de hecho, se ve afectada por los elementos constitucionales y fundamentales de este concepto del ciberespacio.

Una vez más, las distintas múltiples partes interesadas, las distintas cuestiones, las distintas áreas de políticas que surgen, lo que podría ser necesario y lo que la ICANN ha hecho muy bien, y por lo que deberíamos aplaudirla, es la nueva clase o la repetición levemente diferente de estructuras de responsabilidad. Estas estructuras deben ser lo más transparentes y responsables posibles para que todos veamos cuál es el proceso que hay que seguir para determinar la responsabilidad.

Esta fue la conclusión de este proyecto. Con todo gusto voy a responder cualquier pregunta del público y también de ustedes después. Muchas gracias.

DEBORAH ESCALERA: Muchas gracias, Jackie. ¿Alguien tiene alguna pregunta? ¿Algún miembro del público tiene alguna pregunta?

Hay una pregunta del público.

ORADOR DESCONOCIDO: Soy [incomprensible] de Pakistán. Soy embajador NextGen de sus embajadores. Tengo una serie de comentarios.

En primer lugar, a la gente de NextGen, felicitaciones. Realmente estoy orgulloso de que hayan llegado a ser embajadores en solo

un año. En segundo lugar, Deborah y Janice, muchas gracias por todo lo que hacen por nosotros. Yo soy NextGen. Vine aquí solamente para agradecerles a ustedes dos y a todos los demás. Muchas gracias por todo.

Ahora, por supuesto, lo más importante. A la gente de NextGen que está aquí, saben que en la ICANN todo se transcribe. Entonces cuando toman la palabra, primero tienen que decir su nombre y de qué organización son. Por ejemplo, ustedes dicen: "Yo soy Carolina de México, de NextGen, y esta es mi pregunta". No tomen directamente el micrófono y digan: "Esta es mi pregunta". Los programas NextGen y de becarios son dos programas diferentes. Muchas personas de NextGen dicen: "Yo soy de NextGen y soy del programa de becarios". No pueden ser de los dos.

Y finalmente, lo más importante es que por favor vuelvan. Este no es el fin de su travesía. Es solo el principio. Una vez que uno es un NextGen, uno es un NextGen para siempre. Yo estoy aquí para ayudarles, y ustedes van a estar aquí en la próxima reunión. Muchas gracias.

DEBORAH ESCALERA: Muchas gracias.

Estamos teniendo algunos problemas técnicos, así que vamos a continuar con las presentaciones en un par de minutos.

La próxima oradora es Katharin Tai. ¿Katharin?

KATHARIN TAI: Buen día. Yo soy Katharin Tai. Estudio Relaciones Internacionales en la universidad de Oxford y mi tesis tiene como tema la cibersoberanía como relato en la política exterior de China. Todo el proyecto tiene que ver con qué es la cibersoberanía. Pensé que en primer lugar tenía sentido hablar un poco de mis antecedentes, de las relaciones internacionales como disciplina y de lo que esta disciplina busca ser.

Mi estudio de grado estuvo centrado en política de Asia, la sociedad y la historia de Asia. Y mi doctorado está centrado en las relaciones internacionales. Las relaciones internacionales ocupan menos del tema de lo que debería hacerse para lograr ciertos objetivos. No están todos centrados estos estudios en las políticas, sino más bien están centrados en la teoría y en tratar de desarrollar conceptos que nos ayuden a entender el mundo y entender lo que está pasando a nivel de política.

El objetivo de esta presentación es darles una descripción general de la cibersoberanía, qué es o dónde hay un problema para la política internacional como disciplina. Podemos tener

algunas herramientas para conceptualizar este concepto de ciberespacio. Esto es interesante porque Carolina en su presentación habló de los estados. Cuando uno piensa en jurisdicción, piensa en territorio de un país. Voy a tratar de avanzar en esto.

¿Qué es la cibersoberanía y cuáles son los desafíos que esto nos presenta? En primer lugar, esto ha sido importante para los gobiernos de China en relación con la gobernanza de internet desde mediados de 2014, que fue cuando el gobierno de China creó un pequeño grupo que se ocupaba de los temas de ciberseguridad y donde se creó la administración del ciberespacio de China, que es una entidad dentro del gobierno dedicada únicamente a responder estas preguntas del ciberespacio a diferentes niveles.

En general, tiene un foco muy interno, pero también se ocupa de estos temas de gobernanza de internet a nivel internacional. La ciberseguridad ha sido central en el discurso de este organismo durante muchos años, pero no se entiende muy bien qué significa. Por eso, esto es importante para el discurso, la narrativa del gobierno en China y se utiliza y menciona muchas veces en las sedes políticas internacionales de China. Decimos siempre: “Bueno, esto es lo que dice China. Basta. Pasamos a otro tema”. Pero nadie realmente trató de analizar qué significa esto como concepto, como palabra.

En segundo lugar, también nos obliga a responder la pregunta de qué es un estado en el ciberespacio y cómo nosotros podemos conceptualizar esto. Yo sé que especialmente en la ICANN mucha gente dice: "Bueno, el futuro tiene que ver con múltiples partes interesadas. No necesitamos a los estados". Pero para nosotros como disciplina las relaciones internacionales se centran mucho en los estados como actores y los estados seguirán siendo importantes y seguirán actuando en el ciberespacio. La pregunta para nosotros es: ¿Cómo conceptualizamos la soberanía en el ciberespacio? Para responder esta pregunta es importante responder otra pregunta antes. ¿Qué es la cibersoberanía? Existe el supuesto de que el ciberespacio socava el estado. La gente dice: "El ciberespacio va más allá de las fronteras, y como cruza las fronteras puede socavar el poder de un estado".

Aquí tenemos el supuesto de que el estado está relacionado con un territorio y que no se puede separar de un territorio. Una vez que es difícil definir el territorio, el estado y su soberanía, su poder está socavado y desaparecen. También hay que ver de dónde viene la soberanía. Esto se inició como un conjunto de derechos. No estaba tan asociado con un estado como entidad, sino estaba asociado por ejemplo con un rey, el soberano. El soberano no era el pueblo inicialmente. Este concepto con el tiempo se transformó en algo que se les daba a las personas. No

había una persona que quera soberana, sino que el pueblo era el soberano.

En el siglo XV esto estaba más relacionado con nuestra idea de territorio. Entonces en lugar de tener una entidad abstracta, que era soberana, la gente empezó a pensar en esto como que esta entidad era soberana con referencia a un territorio determinado. Podemos pensar en esto como un círculo en el mapa. Trazamos líneas y alguien es soberano con respecto a todo lo que está dentro de esos límites. Esta es una idea que fue desarrollada a fines del siglo XIX en América del Norte, durante la época de la descolonización. Muchos estados querían ser los dueños de su territorio. En América Latina los países querían ser independientes de la colonización, con derecho al autogobierno y con esto obtuvieron el derecho a manejar su propio territorio. O sea, no es la soberanía. Es soberanía y autogobierno en un territorio para un cierto grupo. Entonces la soberanía, que antes tenía que ver con los derechos de una entidad, ahora está relacionada con esta idea de territorio.

Hay un académico que lo describió de esta manera. El estado territorial ha colonizado nuestra imaginación, así que no podemos pensar en un estado como algo diferente de estas líneas trazadas en un mapa. Pensamos en un estado como líneas en un mapa bidimensional. Esto acarreó una serie de problemas. Por ejemplo, si pensamos en el ciberespacio es a veces difícil

decir dónde está algo en los mapas. Y si pensamos en dos dimensiones esto ya no sirve. Un problema especial es el tema de la autoridad, la competencia, que tiene que ver con el tema de responsabilidad porque si tenemos un mapa y trazamos una línea, cruzando un circulo podemos decir: “Una mitad del circulo es mía. La otra mitad es tuya”. No puede ser de los dos al mismo tiempo. Ese es el tema de la bidimensionalidad. Pero en el ciberespacio esta exclusividad no se puede aplicar. Repentinamente ya no podemos pensar más en el espacio como algo que divide. No podemos dividir espacio entre partes claramente identificadas que pertenecen a diferentes estados, donde estos estados tienen autoridad y nadie más la tiene en ese mismo estado.

DEBORAH ESCALERA: ¿Puedes hablar por favor un poco más despacio para las intérpretes?

KATHARIN TAI: Ahora quiero hablar sobre dos abordajes a la teoría de la soberanía, que podrían ayudarnos o podrían darnos una idea de cómo podemos enfrentar este tema del ciberespacio. Por un lado, la idea mencionada por Stephen [incomprensible], que dijo: “La soberanía no es una cosa que uno puede tener. No es como una torta entera”. Es algo que puede dividirse en partes.

Algunas partes tienen que ver con control sobre las cosas que están en un territorio, pero algunas partes de la soberanía tienen que ver con autoridad, facultades. Tenemos parte de la soberanía que consiste en ser reconocidos como un estado legitimo por otros estados. Esto no puede darse sin control. Por lo tanto, este académico dice: “Si la cosa es así, los estados pueden ser soberanos de diferentes maneras”. Algunos estados son soberanos en cuanto a la forma en que son reconocidos, y esta es una parte de la soberanía que puede faltar en los estados. Pero esto no significa que la soberanía no existe en estos otros estados.

Es un abordaje importante cuando hablamos del ciberespacio porque el hecho de que la parte territorial y espacial de la soberanía exista, pero quizás ya no se apliquen. Esto no significa que la soberanía esté socavada o no sea válida cuando pensamos en la soberanía como un conjunto de muchos aspectos.

En segundo lugar, y algo muy interesante, es algo que ha surgido, que ha sido desarrollado por los que estudian la globalización. Quizás hayan escuchado hablar de Anne Marie Slaughter. Ella trabaja en redes internacionales de profesionales. Para ella, la globalización ha cambiado a la soberanía. La soberanía no son atributos, diciendo: “Un estado tiene esto. Tiene un territorio. Tiene una autoridad”. Ella dice:

"Los estados deben poder proteger a sus ciudadanos. Y si por ejemplo la capacidad de participar en organizaciones internacionales sirve a este propósito, esto significa que la soberanía está presente". Entonces la soberanía es importante, básica, y no tanto ya un atributo que ya existe de por sí.

Ahora, para hacer el círculo y volver a China, decimos que esto es algo que está muy presente en el relato del gobierno, en cuanto a cómo entienden la cibersoberanía. Ellos dicen que la cibersoberanía es muy importante porque básicamente tiene por objetivo ayudar al desarrollo económico, y ese es el objetivo al que queremos llegar. Y sabemos que así es cómo existe la soberanía. Muchas gracias.

DEBORAH ESCALERA: Gracias, Katharin. ¿Hay alguna pregunta del público?

El próximo orador es Krishna Kumar. Un segundo, Krishna.

Adelante.

No se está viendo toda la diapositiva.

KRISHNA KUMAR: Soy Krishna Kumar, como ya saben. Pero antes de comenzar mi presentación siéntanse libres de agregarme en LinkedIn, Twitter, Facebook. Utilizo el mismo nombre en todas partes.

¿Yo hice eso?

Voy a hablar acerca del análisis institucional de la transición de la IANA. Tiene que ver con cómo los economistas enfrentan una determinada situación. Voy a explicar el concepto de gobernanza, que es un tema que me interesa.

¿Qué es la gobernanza? La gobernanza es todos los modos de coordinar la acción social en la sociedad humana. Así de simple. Tenemos múltiples actores que proporcionan la gobernanza. Puede ser los gobiernos, la jerarquía, las redes y los mercados. Lo que necesitamos tener en cuenta aquí es que el gobierno es uno de los actores que proporciona servicios y gobernanza. Y no es el único. Muchos gobiernos tratan de no entender esto de la forma correcta porque también afecta la autonomía y la soberanía. Ahí tenemos un problema.

El otro tema que hace que la gobernanza sea esencial son las instituciones. ¿Qué son las instituciones? Las instituciones son las reglas que nosotros, como seres humanos, utilizamos cuando interactuamos con otras personas y otras organizaciones. Para que cualquier sistema de gobernanza funcione, las instituciones desempeñan un papel clave. Mi estudio trata acerca de cómo la ICANN como institución evolucionó para enfrentar los desafíos de gobernanza.

En mi estudio me basé mucho en [incomprensible]. Durante mucho tiempo, los economistas entendían las cosas de una forma muy simple. Para ellos estaban simplemente los mercados y el gobierno que ofrecían bienes públicos y privados a las personas, que consideraban racionales. Esto no siempre es así porque como seres humanos nos conocemos muy bien. Somos seres complejos y existe esta necesidad inherente de entender los sistemas complejos. Esto es lo que hace este marco también.

[Incomprensible] dijo: "Los seres humanos que estudiamos tienen estructuras motivacionales complejas y establecen diversas organizaciones privadas con fines de lucro, gubernamentales, institucionales de la comunidad, que operan en las distintas escalas para generar soluciones productivas e innovadoras, así como resultados destructivos y perversos".

Tenemos un sistema policéntrico. ¿Cómo funciona? En un sistema policéntrico analizamos múltiples centros de toma de decisiones y los analizamos en función de si funcionan de forma independiente o interdependiente, cuáles son los mecanismos contractuales, cómo cooperan, qué jurisdicciones rigen y cómo esto lleva a patrones de interacción predecibles. Para calificarlos llegaron a este marco de desarrollo y análisis institucional. Primero tenemos las categorías, que son las características biofísicas, [incomprensible] de la comunidad y

las reglas en uso. Se trata de definir cuál es el problema. En el caso de la transición de la IANA e internet, internet sería la característica biofísica del estudio. Los atributos de la comunidad son qué hace que esta comunidad pueda trabajar conjuntamente, por qué trabajan juntos, cómo interactúan y qué es lo que ponen sobre la mesa cuando negocian, y las reglas que usan. Todas las unidades constitutivas, todas las partes interesadas, tienen sus propia serie de reglas que utilizan cuando interactúan con los demás.

En el área de la acción tenemos situaciones de acción en la transición de la IANA en este caso. Voy a hacer un seguimiento de los patrones de interacción y el resultado principal. ¿Por qué la transición de la IANA? Yo creo que es uno de los mejores de estudios de casos. Simplemente porque muchas personas de todo el mundo se reúnen con gran esfuerzo, en términos de la cantidad de horas que trabajan (más de 800), 33.000 intercambios de email o más, 600 llamadas y reuniones. ¿Qué hace que esto sea tan especial? Tenemos gente de todo el mundo que creció con distintos sistemas de valores, pero luego deciden reunirse para trabajar bajo el techo de la ICANN y deciden adherirse al sistema de valores de la ICANN porque creen que la internet debe permanecer abierta y debe ser global. Esto es lo que lo hace especial.

Como dije, voy a analizar las variables exógenas y también la situación de acciones en términos de participantes, posición, resultados, cómo se controla la información, básicamente las interacciones que tienen lugar, y también los actores individuales en términos de su nivel de conocimiento, la selección, los recursos que traen a la mesa. ¿Por qué es necesario realizar este estudio? Porque la ICANN es especial. La ICANN es especial, pero no es perfecta. Lo que la hace especial es que sigue siendo funcional, lo que no ocurre con otras organizaciones gubernamentales. El concepto de múltiples partes interesadas es algo que los distintos gobiernos han tratado de implementar desde la década de los 90. Lo han intentado con las conferencias climáticas y otros problemas globales, pero nunca se ha logrado. Esto tuvo lugar en 1998 a través de la ICANN. Yo creo que la ICANN es un sistema que evoluciona constantemente. Como dije, no es perfecto, pero es funcional y eso es lo que lo hace especial.

Es necesario llevar a cabo este estudio porque nos ayuda a entender la complejidad de los sistemas de gobernanza. Nos ayuda a entender los esfuerzos realizados en el pasado. Y dentro de muchos años van a cambiar todos los sistemas de valores y vamos a poder volver a este estudio y ver qué es lo que cambió y qué es lo que está pasando. Muchas gracias.

DEBORAH ESCALERA: Muchas gracias, Krishna. ¿Alguien tiene alguna pregunta?

Muchas gracias. La próxima oradora es Lua Fergus Oliveira da Cruz.

LUÃ FERGUS: Hola. Lua Oliveira da Cruz. Para aquellos que no me conocen, soy Lua. Estudio Derecho en Brasil, pero en este momento estoy viviendo en Lisboa. Estudio en la universidad de Lisboa y voy a hablar hoy sobre la juventud y la gobernanza de internet. Es un tema interesante. He estado estudiando este tema desde hace dos años, cuando empecé a participar en una asociación llamada "Observatorio de la juventud", que es una organización dentro de ISOC. Somos un grupo de interés, un grupo especial de interés. Trabajamos en relación con la juventud.

En este discurso de Obama, dijo que el futuro pertenece a los jóvenes educados y con imaginación para crear. Esta es la fuente de poder en este siglo. Todo el mundo puede estar de acuerdo en esto. Los jóvenes son los que van a ser los próximos líderes y los que van a hacerse cargo del mundo.

Pero ¿qué pasa hoy en día? ¿Realmente nos permiten decir algo respecto de dar forma al futuro en el que vamos a vivir? Los jefes, las personas con las que nos relacionamos, ¿nos permiten opinar? ¿Sí? ¿No? ¿Quizás? Voy a tratar de hablar de algunos

desafíos y oportunidades para que la juventud participe en los debates sobre gobernanza de internet. En 2015 los participantes de un programa de juventud dijeron que tenemos dos problemas importantes, en cuanto a participar en la gobernanza de internet, que tienen que ver con las limitaciones de idioma y el aspecto económico. Dado que las limitaciones del idioma es un tema muy importante, me voy a centrar en el segundo elemento: el elemento económico.

La primera pregunta es cómo podemos pedir más auspicios y más cantidad de iniciativas para el desarrollo de capacidades. Esto se está hablando mucho en el tema de gobernanza de internet dentro de la ISOC, dentro de la ICANN, etc. Voy a mostrarles ahora cuáles son las oportunidades que ya existen para que los jóvenes participen en la gobernanza de internet. Tenemos el programa NextGen por ejemplo. En América Latina también tenemos el governance prime, que es un curso auspiciado por la ICANN, donde durante un mes los jóvenes van a la universidad y aprenden los elementos básicos de gobernanza de internet, la ICANN y todo lo que tiene que ver con internet.

ISOC también tiene estos dos programas. El youth at IGF program lo desarrolló junto con el CGI, que es el comité directivo de internet de Brasil. Tenemos aquí a [incomprensible], que también ayudó a crear este programa. Este programa reúne

muchas personas. Tiene un programa de desarrollo de capacidades que dura dos meses. Es muy intenso. Yo participé estos dos años. Primero fui alumno, y el segundo año fui tutor. Después los jóvenes que participan en este primer programa crearon un observatorio de la juventud para hacer participar a diferentes personas de América Latina (y ahora, de todo el mundo) en estos debates para asistir a los foros, participar de talleres de desarrollo de capacidades. Esta es la organización para la que yo trabajo en este momento.

También tenemos la escuela de gobernanza de internet, la south school of internet governance, la [incomprensible] en Brasil. Tenemos la escuela de gobernanza de internet de Brasil. Estas son las principales oportunidades que existen hoy en día para que los jóvenes puedan participar en las decisiones relacionadas con la gobernanza de internet. Pero ¿todas estas acciones son suficientes? Porque parece que estuviéramos viviendo en una burbuja de gobernanza de internet. Siempre somos los mismos jóvenes, las mismas personas, haciendo este trabajo y creo que debemos llegar a otros lugares: a las universidades, al sector privado, que se ve afectado por la internet pero que no está participando de lo que pasa en la internet. No tienen problemas específicos con internet, pero utilizan la internet para sus negocios por ejemplo.

También tenemos una pregunta respecto del elemento económico que es: ¿Qué influencia desempeñan los financiadores? Porque en la mayoría de los debates sobre gobernanza de internet en el proceso de múltiples partes interesadas, los financiadores y los intereses económicos no se tienen en cuenta porque siempre decimos: "Ah, tenemos que tener una persona de África, una de Asia, una de América Latina y tener un equilibrio de géneros". Pero ¿quién les paga a todas estas personas? ¿Quién les paga para que puedan participar de estos debates y discusiones? Por eso muchas veces no se quiere incorporar a los jóvenes en estas discusiones y me pregunto por qué. Es una pregunta que les dejo para que ustedes piensen.

Tengo aquí este extracto de Luca [incomprensible] que dice: "Debería considerarse que la participación de las partes interesadas para el desarrollo de políticas quizás este motivado por la perspectiva del lograr un resultado de maximizar su propia utilidad. Es decir, en su propio interés o por la intención de hacerlo [incomprensible] para lograr un resultado que maximice los intereses del financiador".

La academia, el mundo de los negocios y otros actores tienen puntos de vista diferentes o divergentes, pero todos los que reciben financiamiento pueden participar de estos debates y foros de discusión para expresar su perspectiva. Entonces hay otros grupos que quedan excluidos de estos debates. Este es

otro elemento que quiero destacar porque cada vez que vamos al sitio web de IGF o de la ICANN nos dice: “Esto es un espacio abierto. Usted puede venir, participar, hacerse oír”. Pero como jóvenes tenemos este problema económico. No podemos viajar por todo el mundo y participar de estos debates. Sí, por supuesto, tenemos la participación remota, pero no es tan interesante hoy en día. No se hace tan bien, aunque sí que estamos trabajando todos para mejorar esto.

¿En qué medida lo jóvenes que participan en la gobernanza de internet prestan atención a los intereses de los financiadores? ¿Cuáles son los intereses que deben promoverse para ayudar a la juventud? Otro tema que quisiera mencionar es la representatividad y la legitimidad. Tenemos seis temas representativos donde las personas eligen a otras personas para que representen sus intereses. En el modelo de múltiples partes interesadas todo esto es voluntario. Uno puede venir aquí y decir: “Bueno, yo soy de la sociedad civil o del mundo académico”. Y todo el mundo piensa que nuestra opinión es la opinión de toda la sociedad civil sobre este tema o la del mundo académico sobre ese tema. Entonces tenemos una representación simbólica informal. Y muy pocos miembros que forman parte de una parte interesada tienen recursos para participar en un evento de gobernanza de internet.

Entonces se está desarrollando una elite global de gobernanza de internet, que no incluye a grupos de base, movimientos sociales, grupos de sociedad civil, etc. en cuanto a la legitimidad, que mencioné antes, tenemos este problema. ¿Podemos decir que nosotros somos la voz de los jóvenes? ¿Representamos a todos los jóvenes interconectados? ¿Tenemos legitimidad para hablar en su nombre? Porque es algo que está pasando en muchos foros, en el IGF, incluso en las reuniones de IGF nacionales o regionales. ¿Qué pasa ahora? Queremos que nos escuchen. ¿Cómo lo hacemos? Bueno, queremos que nos escuchen, queremos participar. Y cuando logramos un puesto alrededor de la mesa, ¿qué es lo que pasa? Quiero mencionar estos tres puntos, estos tres aspectos, que tiene que ver con mi experiencia pasada.

Necesitamos más espacio en los debates. Nos han dado espacio, pero necesitamos más espacio. Debemos diversificar el repertorio de la juventud. Los jóvenes siempre decimos: "Queremos decir esto", "Queremos decir lo otro". Bueno, tenemos que decir lo que queremos decir. También tenemos que centrarnos en la calidad antes que en la cantidad. Si tenemos 20 jóvenes hablando todo el tiempo, pero sin nada que decir o sin tener los conocimientos adecuados esto puede hacer que sean menos respetados en última instancia. Por lo tanto es importante mejorar la calidad. Muchas gracias.

DEBORAH ESCALERA: Gracias, Lua. Les pido disculpas por el formato de las diapositivas. Tenemos algunos problemas con esta computadora. Estamos tratando de formatearlas mejor.

¿Hay alguna pregunta para Lua?

FRANK: Hola. Soy Frank [incomprensible], de un registrador. Usted mencionó el impacto económico, cómo afecta al aspecto económico su capacidad de participar. ¿Nos puede explicar cómo le podríamos ayudar? Usted dijo que la participación remota que se ofrece en ICANN, incluso en reuniones del tipo de la IGG y las listas de correo electrónico, le permiten participar, pero no como usted quisiera.

LUÃ FERGUS: Estamos hablando de la IETF, donde solo trabajan a través de listas de correo electrónico. Estoy hablando de los eventos y la participación de los jóvenes. Vemos que los jóvenes no participan como participantes remotos. Tenemos que hacerlos participar más también a través de la participación remota, pero también viniendo a estos eventos. Necesitamos ambos elementos: listas de correo electrónico, participación remota.

Para venir aquí y ver los rostros de las personas con las que están hablando, para relacionarse y participar mejor.

En mi experiencia, los jóvenes no tienen los medios económicos para venir a estas reuniones y solo participarían de listas de correo electrónico o a través de la web, con participación remota, lo que no es justo.

FRANK: Creo que a veces se establecen centros regionales en los diferentes países y los jóvenes podrían participar allí en reuniones presenciales.

LUÃ FERGUS: Sí, en Brasil tenemos un centro regional. Organizó un evento de ISOC. Entonces se reunió la comunidad para hablar de los temas en este centro regional, en esta oficina regional. Tratamos de darles opciones a las personas para que puedan participar de forma presencial para que estén lejos de estas reuniones, como la de la ICANN.

¿Hay alguna otra pregunta del público?

JANICE DOUMA LANGE: Quisiera decirles que nosotros ofrecemos a través del grupo global de participación de partes interesadas. Tenemos aquí el

equipo de la Para. Danielle Think se ocupa de Brasil. Rodrigo Salcedo y Albert Daniels, en el Caribe. Y con muchísimo gusto vamos a ayudarles a organizar un evento, ayudarles con material de difusión externa, porque teniendo en cuenta la persona que hizo la pregunta y usted es muy bueno tener reuniones presenciales, pero las reuniones presenciales no tienen necesariamente que tener lugar en un evento como el de la ICANN. Porque en esas reuniones hay acceso remoto y hay webinars o seminarios web. Pero entiendo lo que usted está diciendo. Lo que está haciendo es emitiendo un llamado a la acción, hablando de una plataforma que responda a los jóvenes para que participen y se sientan parte de lo que pasa y para invitarlos a participar en los debates.

Respeto lo que usted dice y creo que la persona del público que hizo la pregunta trataba de mostrarle a usted que hay muchas opciones. Solo tenemos que concentrarnos en los jóvenes y lo que hace falta para que ellos participen en un debate. No siempre va a ser financiamiento para los viajes, para que vengan a las reuniones, pero sí pueden ser puede ser apoyo del personal de la ICANN y de otras entidades de internet que ayudarán a lograr esta participación. Así que hable con Deborah para que ella le presente a Rodrigo y hable sobre cómo podemos nosotros ayudarles a ustedes a incorporar este recurso tan valioso: los jóvenes. Y los jóvenes son los que tienen entre 18 y 30 y pico

años. ¿Qué son los recursos que necesitamos? Es un buen comentario y quedamos abiertos a seguir hablando del tema. Gracias.

DEBORAH ESCALERA: ¿Hay alguna otra pregunta?

Muy bien. Espero que ahora las diapositivas empiecen a funcionar mejor. El próximo orador es Matthias Hudobnik.

MATTHAIS HUBOBNIK: ¿Funciona?

DEBORAH ESCALERA: Si apuntan de esta forma, sí. Hay que apuntar hacia la computadora.

Matthias, hay que apuntar a la computadora.

MATTHAIS HUBOBNIK: No funciona.

Ahora funciona perfecto.

Hola a todos. Soy Matthias. Soy de Austria. Estoy estudiando Derecho. Voy a hablar acerca de la regulación del entorno digital. Voy a examinar de qué manera los diferentes conceptos,

como el ciberlibertarianismo, el ciberpaterlanismo, el ciberconmutarianismo afectan al espacio cibernético.

En primer lugar, veamos qué es el ciberespacio. El ciberespacio o espacio cibernético puede compararse con internet. Internet puede definirse como una red de computadoras interconectadas. Entonces la pregunta es: ¿Es una clase de lugar? ¿Un espacio virtual que consta de todos los datos e información? ¿O es una clase de medio? Hay un muy buen artículo escrito por [incomprensible] que examina este tema. Podemos analizar este tema desde la perspectiva de los jóvenes. Internet como mundo virtual y espacio cibernético. Y también podemos verlo desde el punto de vista de internet como una red física. Depende entonces de los distintos puntos de vista.

Esto me lleva a la próxima pregunta. ¿Debería regularse el ciberespacio? La pregunta también es: ¿Puede regularse? Si vemos el ciberespacio como medio, hay una definición de [incomprensible] que establece que el ciberespacio es una clase de medio nuevo. Por lo tanto, no puede compararse con la televisión o con el teléfono o con los medios uno a uno o uno a muchos. Es un medio muchos a muchos. El ciberespacio también tiene una definición de [incomprensible], quien lo define como un espacio público. El argumento aquí es que los viejos tiempos de los medios, como la transmisión publica, la

radiodifusión, no encajan en este espacio, ya que es una nueva área con distintas características.

La próxima pregunta entonces también es: ¿Qué significa regulación? En cierta forma, regulación significa monitorear o controlar un proceso o una serie de conductas de acuerdo con determinados requerimientos, protocolos o normas. Hay dos aspectos que puede regularse. Por un lado, el contenido. Por el otro lado, el proceso. En muchos [incomprensible] tenemos ambas regulaciones.

La última pregunta es: ¿Quién debería ser responsable de la regulación? ¿El gobierno? ¿Las organizaciones privadas? ¿Los usuarios propiamente dichos? El primer concepto entonces se estableció a fines de la década de los 90. Quizás algunos de ustedes conozcan a John Berry [incomprensible], un ciberlibertario. El punto original era que el ciberespacio no puede regularse. Hay dos muy buenos trabajos. Uno, realizado por John Berry [incomprensible], y otro, por David Post y David Johnson. Las tesis claves de estos trabajos son que el espacio cibernético no puede regularse porque el derecho está restringido por las fronteras. Internet no tiene fronteras. Por lo tanto, el derecho no puede ser eficaz en el ciberespacio.

Necesitamos alguna clase de regulación. En respuesta este punto de vista surgió también un punto de vista paternalista de

distintos científicos. Algunos, de Harvard. Por ejemplo, Joe [incomprensible], Lawrence [incomprensible] Goldsmith establecen que el entorno digital consta de un código. Por lo tanto, es difícil regular este entorno. Un ejemplo muy conocido es el concepto de las cuatro modalidades de la regulación: derechos, normas sociales, mercado y arquitectura.

[Incomprensible] establece que es un caso hipotético. Les voy a dar un ejemplo acerca de regular el tabaquismo. Entonces primero establecemos una ley que prohíbe fumar por debajo de los 18 años. Las normas sociales significan que nadie puede fumar en lugares privados sin pedir permiso al dueño. El mercado sería la regulación del precio o de los impuestos. Y la arquitectura, por supuesto es la modalidad más fuerte. Significa manipular directamente los niveles de nicotina de los cigarrillos, por ejemplo.

Luego, finalmente pero no por ello menos importante, tenemos el concepto del comunitarianismo de la red de un profesor de derecho, varias profesiones, la mayoría del Reino Unido, como Andrew Murray y Colin Scott. Ellos sostienen que el control proviene de la comunidad. Esto significa que en la mayor parte de los regímenes de regulación las comunidades son vistas como un entorno regulado, y esto es un problema. Él establece en este concepto que el usuarios es un punto activo. La idea de este investigador es hacer una especie de regulación simbiótica.

Esto significa que la regulación no debe estar impuesta sobre los usuarios interactivos. Es necesario utilizar la comunidad para establecer la regulación.

Un buen ejemplo de este caso es un servicio de música, como Spotify. Ya que muchas personas utilizan este servicio y no descargan música ilegal, el porcentaje de privacidad en el Reino Unido bajó significativamente. Porque si le damos al público lo que necesita, deja de recurrir a servicios ilegales, o por lo menos los usa menos.

El último argumento de Andrew Murray. También sostiene que algunos de los puntos por supuesto tienen más autoridad que otros. Por ejemplo, tenemos aquellos que controlan el acceso o tenemos las grandes empresas, como Facebook, Google o Yahoo. Ellos tienen mucha influencia en la sociedad de internet. B y C son más chicos. B sería los sitios web gubernamentales, y C sería por ejemplo sitios de noticias o algo similar.

Finalmente, a modo de resumen, Andrew Murray y Colin Scott critican la teoría de [incomprensible] por el hecho de que la modalidad regulatoria no capta la verdadera esencia de la modalidad regulatoria. El problema también es que no captura la gran influencia de la comunidad. Esto no es útil en términos prácticos porque es necesario regular internet. Lo vemos frente

a todos los problemas que enfrentamos y todos los delitos que tienen lugar.

Finalmente, también tenemos un buen caso CDB versus newsgroup, newspaper. Este fue un caso acerca de la publicación de información en redes sociales o una orden judicial contra CDB, contra un jugador de futbol. Mientras tuvo lugar la orden judicial, mucha gente decía: “Esto no es cierto”. Hubo muchos comentarios al respecto. La orden judicial no se implementó porque el caso no se pudo sostener. Fue un buen ejemplo de la participación de la comunidad. También tuvo lugar el efecto Streisand, y los tribunales no pudieron iniciar una sentencia porque mucha gente consideró que esto ya no era útil.

Muchas gracias. Con todo gusto voy a responder preguntas.

DEBORAH ESCALERA: Muchas gracias, Matthias. ¿Alguien tiene alguna pregunta?

Muy bien. El próximo orador es Nertil Berdufi.

Esperemos un minuto mientras se cargan las diapositivas.

NERTIL BERDUFI: Buenas tardes. Soy Nertil Berdufi, de Albania. En estos momentos estoy trabajando como profesor en derecho penal, en la universidad de [incomprensible]. Voy a hablar hoy sobre el

tema de la investigación de ciberdelitos en Albania. Esto se relaciona con la agenda la Unión Europea y la convención del Consejo de Europa.

Empecé esta presentación con una foto que muestra las armas que hemos utilizado hasta ahora. Esto fue tomado de la revista de la OTAN de 2013. Pueden ver muy bien que en 1913 las armas eran las armas tradicionales. En 2013 cambió esto. Ahora la guerra se hace por medio electrónicos, utilizando elementos electrónicos, presionando un botón. Pueden ver que después, abajo, tenemos la ciberseguridad con la tecla intro. Esto apareció en la revista de la OTAN. Además el director de la CIA en 2011 habló sobre un nuevo Pearl Harbor, que podía ser muy bien un ciberataque. Esto demuestra el tipo de problemas que tenemos en relación con el ciberdelito hoy en día.

El fenómeno del ciberdelito. Como sabemos, los ciberdelitos son uno de los principales desafíos hoy en día. Los ciberdelitos son una actividad delictiva que incluye infraestructuras, tecnología de la información, acceso ilegal, intercepción ilegal, intercepción de datos, fraude y falsificación electrónicos. Estos están en las convenciones internacionales y también en la legislación de Albania. Como hemos visto, desde el año 2000 al año 2016 el uso de internet aumentó en 918,3%. Es decir, que podemos decir que hay aproximadamente 4.000 millones de

personas participando en la internet. Esta mañana dijeron que eran 3.900 millones que están en línea hoy en día.

Se pueden cometer casi todos los delitos utilizando computadores. Es necesario un análisis de la situación actual en Albania relacionado con las normas legales, los mecanismos de investigación y para demandar a los culpables de delitos cibernéticos. Es lo que vamos a hacer en esta presentación. Acá tenemos tres pilares principales: seguridad de la información de la red, autoridades de aplicación de la ley y defensa. Pueden ver que en cada nivel encontramos problemas y agendas diferentes. En la Unión Europea tenemos la red, las autoridades competentes. A nivel nacional en los diferentes países de la Unión Europea, tenemos los centros nacionales, los equipos de respuesta ante emergencia informática. También tenemos en Europa a Europol, [incomprensible] y C-Pol. A nivel nacional tenemos unidades nacionales de ciberdelito.

La defensa es otro de los problemas que tenemos en relación con los ciberdelitos y la Unión Europea ha hecho algunas cosas. Aquí ha creado un organismo de defensa europeo, que actúa muy bien en este campo. También en los países individuales ha introducido cambios y se han creado autoridades de defensa nacional y de seguridad. Es muy importante e interesante ver aquí que la industria y el sector académico también

desempeñan un rol importante para definir y crear legislación para luchar contra el ciberdelito.

Aquí tenemos un gráfico. Podemos ver que en Albania, cuando empezamos a llevar estadísticas sobre el ciberdelito en el 2008, antes de este año no era un delito. Los delitos informáticos no eran un delito porque no estaban definidos en nuestra legislación. Una vez que ratificamos la convención europea sobre ciberdelito introdujimos los cambios en el Código Penal en nuestro país. Unos pocos años después tuvimos los primeros casos donde se llevó adelante el juicio y se condenó a los culpables. Nos estamos preparando para ser parte de la Unión Europea. Por lo tanto, cada vez más se atacan estos ciberdelitos. En nuestro Código Penal, ¿cuál es la evidencia penal? Una notificación sobre los hechos y las circunstancias importantes para el delito penal, que se obtienen de fuentes o a través de herramientas establecidas en el derecho procesal penal, según las reglas establecidas en este derecho procesal penal y que se utilizan para probar o no que se ha cometido un delito. Esto es lo que está establecido en nuestro Código Penal.

El problema de la jurisdicción. Katharin ya habló sobre esto. Es un problema importante para nosotros. La jurisdicción en lo que tiene que ver con el ciberdelito. No voy a repetir lo que ya dijo Katharin antes porque lo explicó en detalle.

Evidencia o pruebas electrónicas. ¿Qué es lo que vamos a utilizar como evidencia para probar estos delitos? Sistemas informáticos, dispositivos manuales, teléfonos electrónicos, PDA, computadoras, multimedia, GPS, periféricos, etc. Todo esto se puede utilizar como evidencia electrónica. En Albania, en 2009, la policía estatal con el apoyo de la oficina de delitos y drogas de las Naciones Unidas redactó una guía para la investigación de ciberdelitos y la evidencia informática para demostrar este tipo de delitos. Este producto es un manual confidencial porque es muy importante para que la policía y las estructuras adecuadas puedan obtener las pruebas necesarias.

En el 2014 se creó la primera unidad de investigación de ciberdelitos, que después se amplió incluyendo policías, especialistas del departamento de policía y otros funcionarios. Entonces tenemos una estructura especial y se crearon 18 oficinas digitales de fiscalías. Teníamos allí personas responsables que podían ocuparse y estaban muy bien preparadas para investigar o participar de las unidades de investigación de delitos cibernéticos. También se creó una fuerza de trabajo dentro de la policía. Ese año (estamos hablando de 2014) se registraron 180 delitos en el área de los delitos informáticos. Se descubrió a 76 culpables. Estamos hablando de delitos cibernéticos. Hay una gran cantidad de

casos, sin embargo, que no fueron resueltos. Esto es un problema importante para nuestro país.

También hice lo siguiente. Entrevisté a cuatro de las personas más importantes que luchan contra los delitos cibernéticos en Albania y al presidente de la unidad de delitos informáticos en la oficina del fiscal, donde se dijo que encontraron una forma más fácil de intercambiar información a nivel internacional para identificar a los culpables de delitos cibernéticos. Tiene que haber algo más fácil que los exhortos. Se encontró una solución a través de Facebook, por ejemplo. Entonces las diferentes autoridades pueden trabajar juntas y obtener información dentro de dos semanas. Esto es muy importante porque en nuestro país hay muchos delitos que son cometidos utilizando Facebook, por ejemplo.

¿Cuáles son los desafíos que enfrentamos? Los ISP no tienen la posibilidad de almacenar la información mínima requerida por ley. La tecnología moderna y los equipos modernos tienen equipos y tecnología modernos, pero faltan recursos humanos. Es un problema. La preparación de los recursos humanos no es buena. También faltan expertos para la inspección y protección de las pruebas y evidencias digitales, así como para la presentación de evidencia en los tribunales. No hay una buena cooperación con los ISP. Falta predisposición para cooperar con los ISP. [Incomprensible] es la autoridad nacional que dijimos

antes. Cada país debe tener un [incomprensible]. Nosotros tenemos el [incomprensible], pero esta institución no opera correctamente. No tiene nada y no han actuado hasta ahora.

También tenemos otros desafíos aquí, en esta diapositiva. Según el experto en política de seguridad, el mayor desafío es la identificación de la infraestructura fundamental y la adopción de una estrategia nacional de seguridad cibernética. Esto se aplica a Albania. Hoy por hoy no tenemos la infraestructura crítica. Además, incluso a través de la capacitación sobre la investigación de los ciberdelitos, a pesar de que están este tipo de capacitaciones, siempre son organizadas por organizaciones externas, como FBI, [incomprensible], [incomprensible], la COE. Ninguna de estas capacitaciones ha sido organizada por el gobierno de Albania.

Las personas que han sido capacitadas no quedan en sus cargos por mucho tiempo. Esto se traduce en un costo económico y en la falta de expertos en la materia. ¿Cuál es el problema? Quizás una persona se prepare bien, obtenga un doctorado en el tema, se capacite en el exterior, se convierta en un experto. Y después de esto viene a Albania, trabaja en el mismo cargo que tenía y después de un año o dos deja su posición, su puesto, se va al exterior, se va al sector privado para ganar un sueldo más alto, por ejemplo.

Las conclusiones son las siguientes. La legislación de Albania está en línea con los estándares europeos y las convenciones internacionales. Albania ha firmado y ratificado todas las convenciones internacionales relacionadas con los delitos cibernéticos. Todavía debe actualizarse la legislación para que sea correctamente utilizada en los tribunales penales. Hemos hecho la ratificación, pero no incorporamos estos tratados en el Código Penal o el código de procedimiento penal. Además también es básico obtener una implementación efectiva. Una vez que hemos implementado o redactado la legislación, necesitamos a las personas que se encarguen de implementarla. Esto es todo. Muchas gracias.

DEBORAH ESCALERA: Gracias, Nertil. ¿Hay alguna pregunta para Nertil?

NERTIL BERDUFI: Gracias.

DEBORAH ESCALERA: La próxima presentadora es Olga Kyrliuk.

OLGA KYRLIUK: Hola. Este tema ya fue estudiado por Jackie, Katharin, Krishna y Matthias, pero yo quisiera analizar en mayor detalle los

procesos globales de gobernanza de internet y su institucionalización para tratar de entender en qué punto estamos ahora.

DEBORAH ESCALERA: Quiero pedirte por favor que hables más lentamente por los intérpretes.

OLGA KYRLIUK: Voy a entrar en mayor detalle acerca de los procesos globales de la institucionalización de la gobernanza de internet para entender en qué punto estamos ahora. ¿Estamos en el punto de la cooperación o nos estamos acercando rápidamente a los umbrales de la Guerra Fría?

¿No funciona? Sí. Yo soy Olga. Soy de Ucrania. Estoy acá porque tuve la suerte de ser seleccionada como NextGen fellow. ¿Por qué elegí este tema? Bueno, sí, no es NextGen fellow, sino NextGen. La razón por la que elegí este tema es porque siempre me interesó este proceso, cómo ocurre la gobernanza de internet. Además se ha convertido en parte de mi tesis y también cubre parte del tema de mi investigación. En caso de que les interese seguir con este tema pueden contactarme en Facebook, en LinkedIn o tienen mi dirección de email también aquí.

Volviendo al tema, quisiera comenzar con una cita de una persona que todos ustedes conocen muy bien. Lo conocemos como el padre de internet. Él dijo que, independientemente de lo que hagamos, cualquier país del mundo tendrá la posibilidad de establecer sus propias reglas internamente. Cualquier país del mundo puede desconectarse. No es una cuestión técnica. No es una cuestión de que esté bien o mal. No es una cuestión de que la gobernanza de internet esté bien o no. es algo nuestro. Lo que me gusta mucho no es si nos guste o no. la gobernanza de internet ya está acá. No es una cuestión de que la aceptemos o no. se está desarrollando. Está recorriendo su propio camino. Lo único que podemos hacer es incorporarnos a este proceso y tratar de entender cuál es la mejor formar de regir estos procesos, cuál es la mejor forma de tratar de reunir la mayor cantidad posible de personas para que participen en este proceso.

Durante mucho tiempo, la norma era que los estados eran los únicos que tenían el poder para establecer las normas para relaciones internacionales. Eran los únicos. Los más poderosos. Pero las cosas están cambiando. Ahora la mayoría de las partes interesadas se están involucrando y hay oportunidades para que sus voces sean escuchadas. Tratemos de ver un ejemplo muy visual, que explica qué es la gobernanza de internet. Yo muchas veces pienso que es como el mecanismo de una bicicleta. Para

que este mecanismo funcione, necesitamos tener dos ruedas y las dos deben funcionar. Si solo una rueda puede funcionar, y la otra no, todo el mecanismo de la bicicleta va a dejar de funcionar. Si pensamos que una de las ruedas es el excepcionalismo de internet… ¿Por qué excepcionalismo? Porque internet es una estructura única, singular, de naturaleza global, transnacional, que no tiene fronteras.

Estoy tratando de hablar despacio. No sé cómo hablo tan rápido.

Por eso, internet es tan excepcional. Por eso, requiere una regulación especial, un mecanismo especial para abordarla y regirla. Uno de estos mecanismos que por el momento parecería ser el más adecuado y el más eficiente es el modelo multisectorial. Esto significa que cada una de las partes interesadas involucradas en internet debe poder hacer escuchar su voz. Significa que todas las partes interesadas deben poder participar en decisiones que los afecten. Todos deben tener el derecho de participar en este proceso de gobernanza global.

En este momento, los dos modelos básicos con los que contamos son el modelo multilateral y el modelo multisectorial de la gobernanza de internet. Voy a comenzar con el modelo multilateral, dado que es el que está basado en la participación de los estados. Es algo que se conoce desde hace mucho tiempo

y que históricamente es el único modelo reconocido por los procesos globales de gobernanza. Para empezar, tenemos la UIT. Es la organización que en este momento está tratando de participar en el proceso de gobernanza de internet. La UIT no tiene tantas oportunidades de ser la única parte interesada que participe en el proceso de gobernanza de internet. La UIT está tratando de influir sobre el ecosistema de internet, organizando las conferencias plenipotenciarias, hablando acerca de la gobernanza de internet, tratando de ampliar la noción utilizada por organización como estas para tratar de participar en todo este proceso de la gobernanza de internet.

En segundo lugar, tenemos a UNESCO, conocida por sus programas de educación. La UNESCO trata de que internet sea lo más multilingüe posible, de que el contenido introducido esté en la mayor cantidad de idiomas posibles para que todo el mundo pueda entender qué clase de información se transmite a través de internet. En este sentido, trabajan muy bien porque IDN permite que el contenido esté en los idiomas locales.

En segundo lugar, tenemos la OMPI, la organización mundial de la propiedad intelectual, que se conecta con internet a través de los tratados de internet. Luego tenemos otros organismos que no son tan conocidos y de los que no se habla tanto como la alianza de gobierno abierto, la coalición de libertad online (freedom online coalition), que incluye 73 países del mundo. El

segundo incluye 30 países. Ellos están tratando de que la operación de los estados sea más transparente, más responsable, tenga una mayor rendición de cuentas. Y están tratando de que los estados ayuden a la gente a ejercer sus derechos, tanto online como offline.

Y mi preferido es la conferencia mundial de internet, también conocida como la cumbre de [incomprensible]. Es una iniciativa china, que ya tuvo lugar durante tres años consecutivos. Es interesante porque China está tratando de decir que tiene su propia voz en los procesos de gobernanza de internet. Están tratando de trabajar en este ecosistema regional y están tratando de impulsar la agenda, en cuanto a que la ciberseguridad y la cibersoberanía son temas que siempre llevan un papel muy importante en el ecosistema de la gobernanza de internet. Pero el punto es que la seguridad y la privacidad no son temas mutuamente excluyentes. Deberían complementarse porque cuando hablamos de la seguridad esto no significa que con la seguridad viene la vigilancia, el control por parte del estado. Cuando hablamos de privacidad no significa… Cuando hablamos de libre flujo de información no significa que cualquiera pueda hacer lo que quiera. Tiene que haber algunos límites para que nuestros derechos no afecten a los derechos de otras personas.

Y así llegamos al próximo modelo, que es totalmente diferente de este, y está basado en la participación de todas las partes interesadas. Lo llamamos el modelo multisectorial o de múltiples partes interesadas. Este modelo comenzó en 2003 durante la cumbre mundial de la sociedad de la información. Si bien surgió como iniciativa de la UIT, esta cumbre se convirtió en la primera reunión global en la que todas las partes interesadas tuvieron la oportunidad de hablar acerca de los temas de la gobernanza de internet. Por otra parte, tenemos el IGF y la versión europea es EuroDIG. Hay una iniciativa muy interesante que es NetMundial, que tuvo lugar en Brasil. Algunos tenían el temor de que fuera a remplazar al IGF, pero no fue así. Se convirtió en una iniciativa de una clase en particular. Nuestro preferido es la ICANN, que probablemente sea el futuro de la gobernanza de internet. Probablemente sea la organización que tiene un potencial enorme para regir todos estos procesos.

Esto es lo que pasó hace no tanto tiempo. La transición de la IANA, cuando esta función fue transferida de la NTIA a la comunidad de múltiples partes interesadas. Ahí llegamos a la conclusión de que necesitamos contar con reglas de transparencia y de responsabilidad que determinen cómo debería funcionar este sistema en el futuro y qué debemos hacer al respecto. Otra razón por la cual elegí este tema fue que por el momento hay un llamado abierto para el equipo de revisión de

transparencia y responsabilidad de la ICANN. No sé en qué medida podemos participar todos nosotros en este proceso, pero es una oportunidad y quisiera poder participar.

Para terminar, dado que no nos queda más tiempo, en esta diapositiva pueden ver al doctor Strange, el superhéroe. Nosotros tenemos que elegir. ¿Queremos un espacio sin fronteras o un espacio limitado por fronteras? Podemos subirnos y abordar los cambios o resistirnos a los cambios. Este es el modelo multisectorial que espera la participación de todas las personas para que todas las voces sean escuchadas. Muchas gracias.

DEBORAH ESCALERA: ¿Alguien tiene alguna pregunta para Olga?

El próximo orador es Peter Chon. Por favor, hable lento para las intérpretes.

PETER CHON: Buenas tardes a todos. Soy Peter Chon. Estoy estudiando en la universidad de Cambridge. En este momento estudio Ciencias Informáticas y Políticas Tecnologías. Pero hoy voy a hablar del trabajo que hice cuando trabajé como becario en Google. Me centré en el desarrollo de tecnología de la información en la zona de Asia Pacífico. Analicé especialmente el tema de la tarifa

cero. Para aquellos que no conozcan esto de la tarifa cero, es una práctica llevada a cabo por los operadores móviles. Ofrecen datos de forma gratuita, pero estos datos son limitados. Estamos hablando de datos móviles.

Esta característica (tarifa cero) se puede utilizar con diferentes objetivos, pero en un mercado competitivo en el Sur Global en especial se utiliza para brindar acceso al desarrollo. Estamos pensando en esta estadística. La infraestructura de red existe para brindar servicios al 70% de la población global, para conectar a un 70% de las personas del mundo a internet. Sin embargo, solo el 45% de la población mundial está en línea de forma activa. Las investigaciones han demostrado que está el tema del costo. Y aunque algunas personas pueden pagar el costo de estar online, las personas piensan que [incomprensible] sea relevante para mí. Entonces ¿para qué voy a estar en línea si no hay nada interesante para mí?

Aquí entra la idea de tarifa cero. Es contenido gratuito para aquellas personas que no pueden accederlo, pero también para atraer a aquellas personas que piensan que no tienen ningún beneficio para ellos acceder a internet. Tenemos una versión de Facebook, que es free basics, que ofrece acceso a personas en muchas partes del mundo. Y tenemos Wikipedia free. Este debate está centrado en la idea de un muro que rodea un jardín. Si las personas están online por primera vez, quizás entiendan

que solamente pueden acceder a un contenido limitado y quizás no estén tratando de entrar a todo lo demás que ofrecemos desde la ICANN, como el contenido de la internet abierta. Esto ha sido un debate sobre la neutralidad de la red que está teniendo lugar en muchas partes del mundo. Muchos de ustedes sabrán que en India el ente regulador definió que la tasa cero era ilegal ya en el 2016. Pero gran parte de este debate está basado en supuestos empíricos y hay muy poca investigación que lo respalde.

Una pregunta clave sería: cuando las personas se conectan con free basics, ¿realmente se mantienen dentro de este jardín cerrado totalmente o acceden a otro contenido? Mis investigaciones se centraron en Myanmar. En los últimos años se liberalizó el mercado en 2012. Esto cambió el mercado en Myanmar. Las tarjetas sim pasaron de tener un alto costo a tener un costo muy, muy accesible. Entonces esta métrica aumentó la penetración al 90%. Learn Asia hizo una encuesta en todo el país y utilizaron una cifra más conservadora, 83%. Pero esta diferencia entre red y personas que acceden y uso de internet sigue dándose todavía en Myanmar. Vamos a ver que solo el 40% de aquellos que tienen acceso se están conectado a internet.

Entonces aquí tenemos tarifa cero como una opción que los operadores de telecomunicaciones han estado analizando para

utilizar en Myanmar. En 2016 se lanzaron dos ofertas. Facebook free basics es el que ya todos conocen seguramente. Debería explicarles qué es free basics. Free basics es Facebook sin imágenes y sin video, disponible en forma gratuita. Messenger, disponible en forma gratuita. Y después una serie de contenido específico para el país. Wikipedia quizás ofrezca en esos países información sobre noticias del país, información sobre un estudio de otros organismos internacionales. Eso es free basics.

[Incomprensible], que es otro operador en Myanmar, lanzó un mes después, para competir con lo que ofrecía MPT, y su promoción era diferente. En cuanto a la estructura ofrecían Facebook en forma gratuita con todo el contenido. La gente podía mirar videos, ver imágenes, por un total de 150 megas por día. También ofrecían texto de forma gratuita en Viber. Esto lo hicieron para ampliar el mercado y crear un mercado competitivo.

Yo analicé cómo se utilizan estos servicios. Me centré en la región de [incomprensible]. Organicé ocho grupos motivacionales (ocho en zonas urbanas y dos en zonas rurales). Y participaron 63 usuarios. Aquellas personas que entrevistamos utilizaban datos de internet. Así que estos hallazgos no se aplican a la totalidad del país. Son resultados cualitativos, que no deben aplicarse al resto del país. También hicimos algunas

otras entrevistas específicas para entender el mercado de internet en Myanmar y cómo poder ampliarlo.

Voy a hablar de los hallazgos principales. Solo voy a poder cubrir tres, pero les invito a leer el informe si les interesa obtener información adicional. En primer lugar, a pesar de que Facebook ofrece free basics a personas en todo el mundo como herramienta para que acceda a internet por primera vez, la forma en que se comercializa en la práctica no está alineada con este objetivo tan loable. En Myanmar, aquellas personas que entrevistamos no sabían que Facebook free basics era algo más que Facebook. Quizás esto se deba a la forma en que se comercializaba. MPT vendía esto como Facebook en forma gratuita y punto. Yo diría entonces que si se permite la tarifa cero es importante que en los diferentes países se analice cómo se comercializa. Esto debe analizarse en detalle.

Otro hallazgo importante son las opciones de diseño en cuanto a cómo armar la promoción y cómo ha de ser la interfaz del usuario. Sirve para ayudar a las personas a utilizar las ofertas. Las dos ofertas. Facebook free basics y MPT, que tenían un contenido limitado de videos, se utilizaron de manera diferente. Básicamente con MPT free basics, como no había contenido de video ni de fotos, las personas se sentían presionadas a ir de un lado a otro en modo pago, en modo gratuito, en modo pago, en modo gratuito. A veces algunas personas dicen: “Facebook sin

las imágenes es como comerse un poco de curry sin la salsa del curry". Faltaba algo. Además las velocidades eran muy lentas. Entonces las personas dejaron de usar la promoción. Esto limitaba el uso a muy pocos casos: a las personas que ya no tenían crédito y querían seguir utilizando Facebook antes de ir a comprar más crédito. Entonces usaban la versión gratuita de forma temporaria. Esta limitación de contenido llevó a que las personas entendieran muy bien cuando utilizaban una promoción de tarifa cero, en comparación con el momento que utilizaban la internet pagada, por así decirlo.

Esto era parecido a lo que pasa con [incomprensible] free. Los que utilizaban [incomprensible] usaban la promoción. En amplia medida el uso de datos aumentó mientras las personas tenían la promoción. Algunas personas vieron por primera vez el video con esta promoción gratuita. Muchos aumentaron su consumo, pagaron por este consumo aumentado. O sea que fue un efecto cascada, pero este efecto estaba limitado a Facebook. Las personas utilizaban más datos, pero estaba dentro de este jardín cercado. Además, había una tendencia a confundir estos datos [incomprensible], que solo servían para Facebook con datos gratuitos en forma general. No estaba muy claro cuáles eran los límites de estos datos gratuitos que recibían.

Entonces esto tenía que ver con el diseño de la interfaz de usuario y también en cuanto a la aplicación general de esta

promoción y el debate sobre si las personas querían o no este tema de tarifa cero. Pero en las entrevistas se vio claramente que la mayoría de los participantes sí salían de estos jardines cercados. Visitaban contenido que no estaba dentro de la tarifa cero. Entraban a google o a [incomprensible], o una aplicación de mensajería muy utilizada en Myanmar. Salían de estos jardines cercados de alguna manera. Es un hallazgo importante para destacar que a pesar de que utilizan mucho Facebook y estas promociones, los usuarios de hecho también salen de este jardín cercado, de esta zona limitada.

Finalmente, pero no por ello menos importante, este último hallazgo es el más importante para la ICANN es esta idea de que los que se conectan en general tienden a utilizar más aplicaciones que navegadores. La mayoría de los entrevistados utilizaban un navegador para acceder a internet, pero los que utilizaban el celular utilizaban básicamente aplicaciones.

Esto es importante para la ICANN por dos motivos. En los últimos días se habló mucho sobre centrarnos en el usuario final, quién es el usuario final y cómo la ICANN puede incorporar mejor al usuario final en este modelo de múltiples partes interesadas. Cuando se utilizan cada vez más las aplicaciones yo diría que estamos separando o alejando un poco más al usuario final, dos pasos más. Lo estamos alejando de la misión de la ICANN. Cuando un usuario se centra solamente en una

aplicación, eso ya no es tan importante para la ICANN. El CEO esta mañana habló de aumentar la diversidad, llegar mejor a los usuarios finales que se conectan por primera vez. Esto es un desafío importante porque utilizan aplicaciones. Sigue siendo importante para estos usuarios finales que utilizan aplicaciones y no navegadores.

En segundo lugar, esto podría ayudar a cambiar la definición de lo que es un usuario final. Si pensamos en los que se conectan a través de aplicaciones, quizás la ICANN puede decir fácilmente: "Un usuario final es aquel que crea las aplicaciones o aquel que registra el dominio". Pero olvidémonos de las personas que utilizan los dominios o utilizan las aplicaciones. Yo me temo que esto es una solución simple que quizás nos obliguen a buscar o utilizan.

Con esto termino. Si les interesa ver el informe, por favor visiten mi dirección de Twitter y allí lo van a encontrar. Muchas gracias.

DEBORAH ESCALERA: Gracias, Peter. ¿Hay alguna pregunta para Peter?

La próxima oradora es Valerie Filnovych.

VALERIE FILNOVYCH: ¿Puedo comenzar? Soy Valerie Filnovych. Soy de Ucrania. Estudio Derecho y doy clases en la universidad. Doy clases sobre el derecho de propiedad intelectual. Esta presentación tiene por título "Problemas de la regulación nacional de los nombres de dominio en Ucrania". Si tengo tiempo suficiente, voy a hablar también acerca de la violación de los derechos de autor en Ucrania.

Nombres de dominio. En primer lugar, la regulación nacional de la delegación de nombres de dominio en Ucrania. Debería subrayar que no hay una legislación específica que rija la transferencia de nombres de dominio y la delegación de derechos. Esta transferencia es solo una concesión de derechos de nombres de dominios. Estos derechos surgen a través de los acuerdos relevantes entre el dueño potencial y el registrador.

El próximo problema es el siguiente. Miren esta imagen. Es un formulario que debe completarse para la registración de un nombre de dominio en Ucrania. Quisiera hablar acerca de este sistema. En primer lugar, si necesitamos registrar un nombre de dominio en el dominio nacional punto ua. Necesitamos en primer lugar una marca comercial antes de registrar el dominio porque si no tenemos una marca comercial para el dominio que necesitamos no lo vamos a obtener.

Pero si queremos registrar un dominio de un nivel inferior punto [incomprensible] punto ua, por ejemplo, el proceso de registración es muy simple, muy laxo. Solo necesitamos cuatro pasos para obtener un nuevo dominio. En primer lugar, necesitamos un nombre y apellido, aun cuando sea falso, porque nadie va a verificar la documentación. En segundo lugar, un número de teléfono celular en caso de que se olviden la contraseña y la quieran recuperar. Luego, una dirección de correo electrónico (eso está claro), y finalmente hay que aceptar los términos del acuerdo de servicio.

Entonces esta situación se da frente a la registración y crea otros problemas. En primer lugar, cualquier puede registrar fácilmente un nuevo dominio. Puede también colocar contenido ilegal en este sitio web, que está bajo este dominio. La prueba de la identidad de una persona que puede ser alguien que cometa un delito demostrar la identidad será algo muy difícil porque no sabemos quién es el titular de este dominio.

El próximo punto. La política UDRP aún no rige en Ucrania. Si la administración de nuestro dominio público punto ua aceptó que esta política se constituyera en la política principal para la resolución de conflictos, pero esta propuesta no recibió el apoyo necesario. Por lo tanto, los derechos solo pueden defenderse por medio de un proceso judicial tradicional. Si lo comparamos con el UDRP, este último es más económico, más rápido, y por

supuesto más conveniente para la gente, para las partes. Además, no nos olvidemos del nivel de corrupción que existe en los tribunales de Ucrania.

Entonces hay algunas cosas que deben hacerse en relación con los problemas que acabo de mencionar. En primer lugar, es necesario contar un procedimiento más estricto para la registración de dominios. Por supuesto, debería consistir de la verificación obligatoria de los datos personales del titular del dominio. Por ejemplo, en Rusia es necesario escanear el documento de identidad (digamos, el pasaporte) para obtener un nombre de dominio. Además, en Rusia la regla establece que el nombre de dominio no debe contener texto abusivo. De lo contrario, la registración no será aceptada.

Como dije, nosotros no tenemos la legislación adecuada en este campo en Ucrania. Pero tenemos algunas reglas temporarias creadas por organizaciones no gubernamentales. Estas reglas temporarias hablan acerca de la registración de dominios, pero estas reglas tienen expresiones. Simplemente establecen que hay ciertas expresiones que no son aceptadas en los nombre de dominio. Hay una lista de expresiones que no son aceptadas. Es necesario crear un registro uniforme que incluya todos los titulares de nombres de dominios en Ucrania con el ccTLD de Ucrania punto ua y también a nivel regional. Además, se debería

desarrollar una reglamentación especial que establezca reglas y normativas para la registración de un nombre de dominio.

¿Tengo tiempo suficiente? Voy a hablar entonces acerca de la violación de los derechos de autor en internet. Por supuesto, en Ucrania. Quiero subrayar la demostración de la violación de derechos de autor en internet. El decreto de la plenaria de la corte suprema económica de Ucrania contiene una lista de evidencias posibles de violación de derechos de autor en internet, que son páginas web impresas, audios, vídeos y certificados.

Páginas impresas. No todas las páginas impresas pueden constituir una evidencia. Las páginas web impresas pueden constituir una evidencia si fueron observadas por una institución o una persona autorizada dentro de la jurisdicción y si fueron selladas.

Vídeo y audio. Vídeo y audio que contenga el proceso de investigación a través del sitio web, llevado a cabo por cualquier persona interesada en un formato electrónico o en otro tipo de material. Esto es lo que se presenta a tribunales. Este material debe indicar el momento, las condiciones del establecimiento de estos registros y los datos acerca de la persona que creó estos registros. Y luego, un certificado recibido a través de proveedores de red y servicios de búsqueda.

Es necesario hacer todo esto. Entonces, ¿qué se puede hacer para defender los derechos de autor en internet? En primer lugar, nuestra lista de objetos de derechos de autor en la legislación de los derechos de autor en Ucrania debe actualizarse, incorporando la idea del sitio web. Nuestro código civil debería incorporar la lista de guías o pautas específicas en relación con las responsabilidades de la violación de los derechos de propiedad intelectual a través de internet, de intermediarios de información, titulares y usuarios en sitios web.

El siguiente. Se debe desarrollar un conjunto común de contratos modelo para la creación de sitios web, para la provisión de servicios de hosting y la implementación de recursos en el servidor, el registro de nombres de dominio para poder crear un sistema unificado de protección de derechos de autor mediante estos contratos. También es necesario que los proveedores sean responsables de supervisar todo luego de que los archivos sean subidos por los usuarios porque los usuarios son aquellos que violan los derechos de autor en internet con frecuencia.

Y finalmente, debería haber algunas cláusulas de la ley SOPA y [incomprensible] en relación con el intercambio de datos sobre amenazas cibernéticas entre los gobiernos y las organizaciones comerciales.

Muchísimas gracias por su atención. Y con todo gusto voy a responder las preguntas que puedan tener.

DEBORAH ESCALERA: Muchas gracias. Me encantó la foto del final. ¿Hay una pregunta?

ORADOR DESCONOCIDO: Soy [incomprensible]. Los últimos puntos acerca de la protección del derecho de autor, ¿son sugerencias suyas? ¿Son sus sugerencias, sus ideas, o es la idea general?

VALERIE FILNOVYCH: Hice algunas sugerencias en la última diapositiva.

ORADOR DESCONOCIDO: El hecho de que los proveedores de hosting deban monitorear el contenido es un tema muy controvertido. ¿No le parece?

VALERIE FILNOVYCH: Sí, pero como les digo a mis alumnos cuando doy clase sobre propiedad intelectual… Les digo que hay que poner marcas de agua en las imágenes que ponen en internet, que deben realizar acuerdos con los titulares de los sitios web para que la información que está en el sitio web no se vea amenazada, por así decirlo. Entonces, marcas de agua, programas informáticos

para los sitios web porque todos los sitios web tienen programas informáticos, acuerdos de licencias con los usuarios para que no hagan determinadas cosas…

ORADOR DESCONOCIDO: Entonces podría ser una tercera empresa, Facebook, etc. que se utiliza para subir fotos, y luego el proveedor de hosting debería escanear y ver todas esas imágenes para ver si violan los derechos de autor. ¿Cómo se tomaría una decisión? ¿Cuál sería el criterio?

Bueno, no importa. Es una pregunta complicada. No hay problema.

VALERIE FILNOVYCH: Estoy tratando de entender su pregunta.

DEBORAH ESCALERA: Bueno, creo que Valerie va a tener que pensar esa pregunta. Si quiere puede enviarla por email y la podemos responder fuera de línea. Gracias, Valerie. ¿Alguna otra pregunta?

La ultima oradora, y no por ello menos importante, es Yousra Hsina.

YOUSRA HSINA: Voy a hablar sobre los proveedores de servicios de internet y la privacidad en línea.

DEBORAH ESCALERA: Por favor, utilice el micrófono y hable lentamente.

YOUSRA HSINA: Voy a hablar sobre los proveedores de servicios de internet y la privacidad en línea. Todos sabemos que las redes sociales y los sitios web que visitamos recogen información sobre nosotros y que la utilizan para publicidad. Sin embargo, pocas veces nos damos cuenta de que nuestro proveedor de servicios de internet también puede recabar información sobre nosotros.

El hecho es que podemos elegir registrarnos y utilizar una red social o utilizar un sitio web o no, pero una vez que celebramos un contrato con una ISP es una diferencia. Los servicios que presentan los ISP son diferentes porque cuando celebramos un contrato con mi ISP no hay forma de dar marcha atrás. El usuario tiene un poco de flexibilidad. Puede cambiar de idea. Muy poca flexibilidad, de hecho. Y no puede evitar entrar a la red. Piénsenlo de esta manera. Su ISP maneja todo el tráfico de red que sale o llega a ustedes. O sea sabe exactamente cómo es su tráfico de internet, los sitios web que visita, las aplicaciones que utiliza, etc. Sin embargo, no podemos negar que hoy en día

los ISP están levemente limitados por algunos desarrollos tecnológicos. Por ejemplo, las VPN, los protocolos de encriptado y la multiplicidad de dispositivos. Obviamente en la actualidad nadie tiene solamente un dispositivo. Todos tenemos varios.

Voy a hablar ahora de las redes virtuales privadas. Cuando utilizamos VPN o redes virtuales privadas, los usuarios y sus computadoras crean una señal encriptada que es enviada al servidor VPN. Según la confirmación de la red privada virtual se puede mandar tráfico de internet al servidor VPN. Pero además, a pesar de que las VPN existen en el mercado desde hace muchos años, no se utilizan muy ampliamente. Además no pueden brindar una protección completa al usuario.

En cuanto a los protocolos de encriptado, el encriptado todavía no se utiliza ampliamente porque si comparamos el tráfico de internet que está encriptado con el tráfico de internet que no está encriptado podrán ver que el tráfico no encriptado es mucho mayor que el tráfico que sí está encriptado. La parte del tráfico que no está encriptado representa de alguna manera el tema de privacidad que preocupa al usuario final.

Les voy a hablar de las tres categorías de investigación que se han investigado, que son salud, compras e investigación. Las estadísticas han demostrado que más del 85% de los principales 50 sitios que visitamos todavía no han adoptado el encriptado o

protocolos de encriptado para la navegación por la web. Entonces las ISP pueden ver toda la información que demuestra cuando estamos buscando investigación sobre tema de salud, cuando analizamos temas financieros o simplemente cuando estamos comprando productos.

Otro punto que tiene que ver con esto es que aunque incluso con https el ISP puede tener información sobre el usuario. ¿Por qué? Porque incluso con https los ISP pueden ver los dominios que está visitando el usuario. Esto puede revelar muchísima información. Como dije antes, incluso con los sitios web encriptados, los ISP pueden acceder a mucha información confidencial sobre clientes. Hay un grupo de investigación en temas informáticos que halló que las ISP pueden acceder a una gran cantidad de contenido sobre los usuarios (contenido encriptado, para ser precisa) sin debilitarlo y sin violarlo. Simplemente analizando las características de los paquetes, el horario en que se mandan, su tamaño, incluso su destino. Los ISP podrían obtener mucha información sobre los hábitos de los clientes de este modo. Esto permitiría identificar, por ejemplo, las veces que visitan páginas web. También podrían obtener otro tipo de información sobre los contenidos.

También voy a hablar sobre las normativas, especialmente hablando de los EEUU. Los usuarios de internet en EEUU el año pasado vieron que la FCC adoptó la regla de privacidad para la

banda ancha. Esto fue el año pasado. Esta regla establece que los ISP antes de compartir información sensible sobre los clientes deben obtener la autorización del cliente para compartir esta información. La regla establece que los ISP deben proteger esta información sensible o privada de los usuarios y que deben especificar cuáles son los pasos técnicos que van a seguir para proteger esta información. Este iba a ser un ejemplo exitoso, pero no lo es lamentablemente porque la normativa debía de haberse implementado hace dos semanas. Pero en realidad se presentaron muchas quejas diciendo que los ISP y otras empresas que están online también tienen acceso a la información de los usuarios.

La pregunta que se presenta es la siguiente. ¿Las normativas de privacidad de los gobiernos deben proteger a los datos de los usuarios de internet [incomprensible] que realizan todas las empresas o solamente deben protegerlos de algunas empresas? La respuesta es a) por supuesto. El problema que se surgió, lo que se cuestionó, en este caso es que otras empresas en línea, como los motores de búsqueda o sitios web o los sistemas operativos, no estaban obligados a cumplir con esta normativa. Esta normativa solo se aplicaba a los ISP. Se consideró una forma de discriminación contra los ISP. Por tanto, esto no se adoptó. Porque la manera en que invaden la privacidad las

organizaciones que no son ISP es tan importante como la manera en que la invaden los ISP.

¿Qué buscan los consumidores? Todavía hay mucho por hacer para regular los ISP y obviamente esto va a llevar tiempo. Hay mucha controversia sobre el tema. Voy a terminar mi presentación recordándoles qué buscan los consumidores. Los consumidores quieren que haya uniformidad, simplicidad, transparencia y que no haya conflicto entre las diferentes normativas. Muchas gracias.

DEBORAH ESCALERA: Gracias, Yousra. ¿Hay alguna pregunta para Yousra?

Con esto terminamos las presentaciones. Para los miembros del público, queremos agradecerles por estar aquí hoy con nosotros. Yo sé que terminamos un poquito más temprano de lo esperado, pero ahora vamos a tomar las preguntas que tengan los miembros del grupo de NextGen.

ORADOR DESCONOCIDO: Quisiera hacer unos comentarios generales respecto a las diferentes presentaciones. Voy a tratar de ser rápida. En primer lugar, son comentarios respecto a todas las presentaciones. Quisiera decirles a los 15 de ustedes: muchas gracias por sus esfuerzos, por su trabajo. Ha sido una sesión muy interesante.

Aprendí sobre diferentes temas, sobre los cuales sabía muy poco. Tecnología de cadenas de bloques, por ejemplo, y cómo se utiliza la tarifa cero en la práctica, etc. Esto fue muy interesante.

También quiero hacer una pequeña corrección o quiero decir algo respecto a algo que se dijo porque conozco el tema. Es la diapositiva sobre el modelo de múltiples partes interesadas y los modelos multilaterales. Quisiera agregar que yo trabajé en la UNESCO. La UNESCO es un organismo multilateral, pero ha apoyado el modelo de múltiples partes interesadas para la gobernanza de internet, así que quizás podríamos pasar eso a la parte positiva de la diapositiva. Bueno, era una broma solamente.

Un comentario más general. Tiene que ver con mi trabajo, que es promover la libertad de expresión. Creo que varias de las presentaciones mencionaron ideas fantásticas. Es importante tener nuevas ideas, nuevas perspectivas. Con respecto a algunos temas, hay consecuencias en materia de derechos humanos que todavía no fueron tan consideradas. Por ejemplo, qué significaría para la privacidad y la libertad de expresión no permitir el anonimato o que una persona tenga su dirección IP para siempre o cuando se puede bajar de un sitio web y hay una violación de los derechos de autor. Algunos de estos temas los

invito a pensar qué consecuencias tiene esto para los derechos humanos.

Hay una sesión hoy a las 3:15 con los comisionados de protección de datos de Europa. También el redactor especial en Naciones Unidas en privacidad. Va a ser una sesión muy importante. En términos más generales, creo que sugeriría que puedan aportar su experiencia, sus ideas y sus procedimientos y que también debemos estar abiertos a otras perspectivas. Si tienen experiencia en propiedad intelectual, derechos humanos o seguridad, comuníquense con los que están del otro lado. Estén abiertos a escuchar sus opiniones porque creo que aquí funciona muy bien el modelo de múltiples partes interesadas. Las personas se reúnen, se entienden y llegan a un acuerdo.

En cuanto a la participación de los jóvenes, este tema se mencionó y fue un tema muy importante. Se planteó muchas preguntas válidas y críticas. Yo creo que se puede hacer mucho a partir de la participación remota, pero también es importante que tengan lugar las reuniones presenciales. Hay un trabajo sobre trabajo en redes, donde se habla de la importancia de las interacciones personales. Esto crea las bases para un trabajo posterior a través de teleconferencia, correos electrónicos, etc.

Realmente estoy totalmente a favor del programa NextGen y creo que es una iniciativa importante y muy sólida. Y como nos

dijo el CEO ayer: “Los jóvenes son el futuro de internet. El futuro de la gobernanza de internet. Y la ICANN los necesita”. Quiero felicitarlos por todos sus esfuerzos. Gracias.

DEBORAH ESCALERA: Andrea, ¿tenía alguna pregunta?

ANDREA: ¿Los NextGen por favor pueden quedarse aquí? Porque quiero tocar algunos temas específicos con ustedes.

¿Alguien tiene alguna pregunta para los que presentaron? Si no, vamos uno por uno a ver quién tiene alguna pregunta.

ORADOR DESCONOCIDO: ¿Sería posible que recibamos las presentaciones de todos los demás presentadores?

Perfecto.

DEBORAH ESCALERA: ¿Ningún fellow tiene alguna pregunta para los demás fellows?

CAROLINA MATAMOROS: Gracias por este espacio para hacer preguntas.

En primer lugar, quiero hablar acerca del tema de la pornografía infantil del que habló [incomprensible]. El punto de vista de la fiscalía. Quisiera saber qué ocurre cuando se comete el delito y cuando el usuario consume estos productos. Porque si establezco un paralelo con el abuso de sustancias, en general se castigan ambas cosas: la producción y la comercialización de productos, como también el uso. Entonces quiero saber en este caso qué ocurre con la pornografía infantil.

ORADOR DESCONOCIDO: Estoy acá.

Depende de la legislación de cada país, pero básicamente se penaliza la producción y el uso. ¿Responde esto su pregunta?

DEBORAH ESCALERA: Adelante. Por favor, diga su nombre porque creo que seguimos registrando.

PETER CHON: Soy Peter Chon. Tengo una pregunta para Abderrahman con respecto a la tecnología de cadenas de bloques. Yo no soy experto en este tema, pero quisiera saber lo siguiente. Al parecer, la cadena de bloques ayudaría a confiar y a verificar la transacción, pero hace algo para resolver el tema que me parece

central con respecto al financiamiento de las ONG. Es decir, una vez que llega el dinero, una vez que finalizó la transacción, ¿cómo podemos tener la confianza y la verificación necesarias para en qué se van a usar esos fondos?

Quisiera saber si la tecnología de cadena de bloques continúa en la cadena, una vez que la ONG tiene los fondos. ¿La tecnología de cadena de bloques puede asegurar que se utilice los fondos, tal como dijeron que se iban a utilizar? Es decir, ¿puede asegurar que se cumplan las obligaciones contractuales, una vez que finalizó la transferencia?

ABDERRAHMAN AIT-ALI: Gracias, Peter. Es una muy buena pregunta. Lo que se hace básicamente es lo siguiente. Por un lado se utiliza la cadena de bloques como herramienta para contratos inteligentes. También hay otras funcionalidades que agregamos a la herramienta. La herramienta está en una etapa inicial de desarrollo. Por tanto, todavía estamos haciendo [incomprensible] y haciendo distintas pruebas, trabajando con prototipos. Y tenemos una ONG que está trabajando con refugiados en Siria, en la frontera con Turquía.

Lo primero que hacemos es usar [incomprensible], la cadena de bloques [incomprensible]. Es decir, no usamos nuestra propia cadena de bloques o nuestro software porque ya hay muchas

API para [incomprensible]. Entonces usamos eso, y luego las ONG básicamente obtienen fondos de diferentes fuentes de financiamiento. Hay distintas etapas de financiamiento. Nosotros lanzamos el primer nivel de financiamiento. Cuando se logra, nos detenemos. Y cuando la ONG recibe los fondos, una vez que está en el campo hay un proceso para seguir a la ONG en términos de sus actividades. Entonces en el prototipo o la interfaz hay un formulario con el flujo y luego pasamos al próximo nivel de financiamiento. Así continúa hasta que se obtiene la financiación total para todo el proyecto.

Así es cómo hacemos el seguimiento. Por supuesto, el prototipo está abierto para sumarle funcionalidades adicionales y nos basamos en los comentarios que recibimos de las ONG y también de los organismos de financiación. En función de esto, vamos agregando cada vez más funcionalidades. Pero básicamente así es cómo funciona el prototipo hoy.

OLGA KYRYIUK: Olga Kyryiuk, de Ucrania. Gracias por los comentarios.

No quise decir que lo que la UNESCO hace está mal. El punto era mostrar la diferencia principal entre estos dos modelos. El modelo multilateral está basado en las organizaciones que inicialmente incluían estados. Ahora tratan de involucrar a otras partes interesadas. La tendencia multisectorial es la que está

ocurriendo ahora, pero simplemente quise mencionar aquello que fue lo más importante durante mucho tiempo y ahora están tratando de involucrar también a otros. Pero al igual que el modelo multisectorial, inicialmente se creó con estas partes interesadas representadas.

CLEMENT GENTY: Tengo una pregunta para Valeria. Perdón. Soy Clement Genty, de Francia. Tengo una pregunta acerca del uso de nombres de dominio para la población. Veo que en punto ua hay un sistema especial y está la idea de tener un acuerdo de derechos de autor, etc. Recuerdo la creación y la delegación de dominios siempre fue un problema desde el 85 cuando se inventaron. Hace tres años, si recuerdo, la ICANN lanzó un programa de nuevos gTLD, y en dos años tendremos cada vez más gTLD. Ahora tenemos unos 3.000 gTLD. Será útil en 2017 desarrollar dominios de alto nivel con código de país, ccTLD. O sea, ¿tiene sentido desarrollar ccTLD cuando sabemos que podemos crear un nombre de dominio con un link, con un vínculo a un tema y no a un país?

VALERIE FILNOVYCH: Como dije, la política de UDRP será suficiente para la resolución de nombres de dominio en Ucrania. Pero la propuesta de la administración de nombres de dominio punto ua no se aprobó.

Por lo tanto, quizás deberían volver a presentar este proyecto preliminar al gobierno para que sea aprobado.

DEBORAH ESCALERA: ¿Alguna otra pregunta o comentario, Peter?

JACQUELINE EGGENSCHWILER: Perdón. Tenemos un problema de coordinación.

Tengo una pregunta para Carolina acerca de este triángulo interesante que nos mostró. Es una pregunta de muy alto nivel. Quisiera saber si estaba pensando en algún mecanismo de coordinación posible que pudiera resolver este tema de la defensa, seguridad, internet, por otro lado, y la gobernanza sería el tercer componente. Gracias.

CAROLINA MATAMOROS: Tiene razón con respecto a la pregunta de alto nivel porque actualmente cualquiera podría hacer esto. Yo lo planteé y lo traje aquí a la ICANN porque creo que acá está la oportunidad de tomar ese espacio. Algunas organizaciones se preocupan por la seguridad de internet, por la seguridad de los estados, pero no se ocupan de ese triángulo. Entonces tenemos seguridad, tenemos el comité asesor de seguridad y estabilidad que en teoría considera esto, pero solamente brindan asesoramiento.

Es muy difícil hacerlo, pero yo creo que podrían hacer algo al respecto. Aquí los dominios y los nombres están y es la forma en la cual fue desarrollada internet. Algunas organizaciones como estas que pueden hacer algo al respecto. Y quería hacer un comentario acerca de lo que usted dijo acerca de la protección de los derechos. De hecho es una pregunta para que pensemos. Todos tenemos diferentes responsabilidades. Las diferentes agencias tienen diferentes responsabilidades. Por ejemplo, aquí en la ICANN yo pregunté cuál es el principal tema de seguridad, qué es lo que están protegiendo, y eso no está claro. Protegen internet, protegen a los usuarios, protegen derechos humanos.

En ciertos casos, esas cosas se contradicen. Entonces estas entidades, especialmente el comité asesor de seguridad y estabilidad, necesitan aclarar qué es lo que quieren proteger para realmente ser efectivos. Esto es algo que debe comenzar, que debe hacerse. Creo que se trata de esto, pero sigue siendo una pregunta amplia sin una respuesta cerrada.

ORADORA DESCONOCIDA: Quisiera hacer un comentario breve. Es importante recordar que la misión de la ICANN tiene un alcance limitado. Se ocupa de nombres de dominios, nombres y números. El IETF se ocupa de otros temas. Quizás DNSSEC se ocupe más de estos temas. Pero hay diferentes preocupaciones en torno a la seguridad del DNS

como sistema versus la seguridad en términos de la protección de los ciudadanos. Simplemente quería recordarles a todos que la ICANN se ocupa del sistema de nombres de dominio y no va más allá de eso.

CAROLINA MATAMOROS: Está claro. Simplemente que de acuerdo con la misión el objetivo es mantener una internet abierta e interconectada. Entonces el equipo asesor de seguridad debería tener por objetivo algo relacionado con esto. Sé que no es su foco. Sé que es mucho más técnico, pero es un espacio que está faltando en este momento. Tal como dije al principio, nadie está prestando atención a esa parte. Eso pone en riesgo internet.

Es simplemente una pregunta abierta.

ANDREA: También hay que tener en cuenta que hay muchas organizaciones que se ocupan de la gobernanza de internet y de la seguridad. No es solamente la responsabilidad de la ICANN trabajar en ese tema. Cuando hablamos acerca de la protección tenemos que tomar en cuenta todas las partes interesadas, especialmente las instituciones que desempeñan esta función de protección de derechos.

PETER CHON: Tengo una pregunta para Chawana. Me gustó mucho su presentación. Aunque no necesariamente estoy de acuerdo con la idea que presentó, me generó muchas preguntas. Me hizo pensar. Así que quisiera plantear otra pregunta.

Si a cada individuo en el mundo le damos su dirección IP personal, tenemos que pensar qué ocurriría en el contexto internacional y la interoperabilidad global. Me imagino que esto facilitaría el seguimiento de toda persona a través de toda organización gubernamental del mundo. Esto podría por supuesto conducir a un punto donde un país en particular quiera proteger a sus ciudadanos porque considera que su misión es proteger a sus ciudadanos. Por lo tanto se retire de la ICANN y de internet global. Y quizás esto podría conducir a una fractura de internet. Ese sería un escenario un poco pesimista en el que quizás podríamos pensar.

ANDREA: Tenemos que cerrar en 1 minuto porque va a comenzar otra sesión.

CHAWANA HUANGSUNTOMACHAI: Gracias, Peter, por sus comentarios. Es un comentario interesante, de hecho.

Para hacer esto, para que esto ocurra, creo que tenemos que trabajar un poco más. Tenemos que ver quién es el dueño de la base de datos. Quizás determinados estados no tengan una base de datos con direcciones de IP para identificación de los ciudadanos de otros países. Debe funcionar de esa forma, creo yo. Pero creo que es necesario seguir conversando y hablando sobre ese tema. Gracias.

DEBORAH ESCALERA: Muchas gracias a todos por su presentación. Creo que todos hicieron un excelente trabajo. Un aplauso.

[FIN DE LA TRANSCRIPCIÓN]