MARRAKECH – Presentaciones de NextGen Parte 2
Miércoles, 26 de junio de 2019 – 09:30 a 11:45 WET
ICANN65 | Marrakech, Marruecos

CYNTHIA JADE MAKORY: Esto es un desafío porque las empresas también se ven afectadas. Si pierden sus secretos comerciales, esto es muy perjudicial para la empresa en sí. Según el gobierno del Reino Unido, se estima que aproximadamente 34 países tienen equipos de ciberespionaje que están bien financiados. Hay muchos países en el mundo donde esto ocurre. El mundo está establecido con una dinámica muy hegemónica. Tenemos países más fuertes, países que tienen capacidades que otros no tienen. Qué deben hacer los otros países. Esta es mi recomendación en cuanto a lo que se puede hacer y lo que los distintos países pueden apuntar. Tenemos una situación en la que ya sabemos qué es lo que ocurre. Estamos esperando quizá que el orden internacional lo resuelva. Todos los países son responsables de asegurar esto. Por eso tenemos que lograr que nuestra Internet sea segura. Se debe generar capacidad. Esto permite que un país entienda de dónde proviene la amenaza y que pueda responder adecuadamente. Por eso generar capacidad es muy importante. Si generamos una capacidad también tratamos de generar estructuras que bloqueen algunos de estos ataques que podrían afectar la infraestructura crítica de un país y, poco a poco,

nuestros sistemas van a ir pasando a esta plataforma que se llama Cyber. Está todo interconectado y no está limitado a Internet.

Por este hecho de estar conectado significa que si alguien puede hackear un sistema, atacarlo, ataca una infraestructura que es muy vulnerable y la investigación debe enfatizar y permitir que un país entienda cuál es la razón por la cual estos actos están ocurriendo. También permite que los usuarios estén en el centro. El estado tiene una obligación para con sus ciudadanos. Debe haber herramientas defensivas porque no se trata solo de identificar el problema sino también tratar de generar herramientas que efectivamente le den al país la posibilidad de protegerse de estas amenazas específicas. Hay una necesidad también de evolucionar y esto requiere que uno se adapte a las técnicas y, por lo tanto, pueda anticipar las amenazas.

Les voy a hacer una pregunta. ¿Cómo trata el ciberespionaje el país donde ustedes viven? ¿Cuáles son las regulaciones nacionales, regionales e internacionales que se pueden establecer en respuesta al ciberespionaje? Quisiera ahora mostrarles esta cita que me parece muy importante. El ciberpoder es ahora un hecho fundamental de la vida global dado que ya está aquí.

¿Qué están haciendo entonces los distintos países? ¿Cómo están tomando los países esto en consideración cuando generan distintas políticas? ¿Están los ciudadanos en el centro de todo esto en términos de ciberespionaje y de ciberprotección? Este es el final de mi presentación.

DEBORAH ESCALERA: Muchas gracias, Jade. Quisiera saber ahora si hay alguna pregunta.

ORADOR DESCONOCIDO: Hola. Soy [inaudible]. Lo que yo les digo a mis alumnos es que la próxima guerra mundial no va a ser con soldados y armas sino que va a ocurrir en el ciberespacio. Hace algunos años, el presidente de Estados Unidos ordenó un ciberataque a Irán. ¿Cuál es la solución en términos de países que son ciberpotencias? Hay países que no lo son. ¿Cuáles son sus recomendaciones?

CYNTHIA JADE MAKORY: Quizá sea una suerte o no que yo sea estudiante de Derecho. Soy muy escéptica respecto del orden legal internacional. El mundo está establecido con un sentido hegemónico donde hay países más fuertes y países más pequeños. Para que pueda existir un consenso, los distintos países deben saber qué es lo que está

puesto sobre la mesa. Incluso cuando hablamos de un tratado y de tratar de redactar que pueda resultar en la protección de los distintos países, debemos formar quizá un comité porque antes de que entre en efecto cualquier tratado siempre hay comités que realizan investigación para poder así investigar de qué modo se puede hacer que incluso los países más pequeños se beneficien de este tratado a pesar del hecho de que no son superpotencias. Esto también implica tener un fuerte énfasis en los estados nacionales que tengan mecanismos defensivos para que también puedan contrarrestar estos ataques.

Para Kenia, por ejemplo, estas son investigaciones que demoraron siete años y ni siquiera sabíamos nosotros que estábamos recibiendo un ataque, que estábamos bajo ataque y que teníamos la capacidad de poder enfrentar algunos de estos desafíos. Una de mis recomendaciones es la evolución. La gente debe empezar a ver el problema que enfrenta el mundo y también tratar de ponerlo a nivel nacional, donde empezamos a ver estos problemas como algo que las distintas naciones deben empezar a centrarse.

ORADOR DESCONOCIDO: Un comentario más. En términos de los tratados internacionales, ¿a usted le parece que deberíamos recurrir a las Naciones Unidas o a algún otro organismo?

CYNTHIA JADE MAKORY: Si recurrimos a las Naciones Unidas, lo que tenemos son resoluciones. Un tratado es algo que normalmente existe por fuera del orden de Naciones Unidas porque los distintos países deciden firmarlo y después ratificarlo. Se pueden obtener las resoluciones de la ONU pero, si no existe un tratado que es independiente de la ONU, donde los distintos países se comprometen a tomar estas obligaciones… Cuando uno ratifica un tratado, está obligado. Necesitamos algo que haga que la gente sea responsable por las obligaciones que toma. Por eso yo optaría por algo que esté por fuera de las Naciones Unidas.

DEBORAH ESCALERA: Una pregunta simple para todos. ¿Cómo podemos mejorar la protección de la infraestructura crítica? ¿Cómo puede estar protegida de los ciberataques?

CYNTHIA JADE MAKORY: Les voy a dar el ejemplo de Kenia, porque ese es mi país. Recientemente, no sé si fue a finales del año pasado, nuestro gobierno decidió apartar un dinero que normalmente es apartado por la autoridad de comunicaciones para analizar qué ocurre con la ciberseguridad. Esto es muy importante porque si los distintos países hacen que esto sea su prioridad, como ocurre

en este caso, también le ponen foco a eso y eso también permite que se pueda aplicar a los ciudadanos. Esto debe empezar a nivel nacional. Gracias.

DEBORAH ESCALERA: Muchas gracias, Jade. Nuestro próximo presentador es Adisa. Un momento, por favor. Vamos a poner la presentación. Puede comenzar.

ADISA BOLUTIFE: Hola a todos. Soy Adisa Bolutife. Voy a hablarles hoy sobre la autenticación y la seguridad adaptiva del sistema de nombres de dominio. Les voy a contar un poco qué es lo que vamos a ir discutiendo aquí. Vamos a ver cómo funciona el DNS, las vulnerabilidades del sistema de nombres de dominio y vamos a tratar también de entender qué es el DNSSEC, qué es la seguridad del sistema de nombres de dominio que tenemos actualmente. También cuál es el estado actual de la validación de DNSSEC en el mundo pero también en África. Vamos a hablar también sobre las recomendaciones futuras y cómo podemos avanzar.

El sistema de nombres de dominio, cómo funciona. El DNS normalmente traduce los hostnames a las direcciones IP. Básicamente, uno escribe una dirección web en un navegador y

el DNS básicamente ayuda a conectar esa dirección a una dirección IP y a darle la información que necesita. El DNS lo hace utilizando un resolutor. El navegador utiliza el resolutor que transmite a lo que nosotros llamamos un servidor recursivo que existe en el sistema de DNS y el servidor recursivo atraviesa todos los servidores para encontrar el que tiene la información que está buscando. Es decir, básicamente va a una jerarquía, empieza a partir de los servidores raíz y luego va hacia los otros.

Funciona del siguiente modo. Cuando el resolutor recibe la información y la almacena en una caché, la próxima vez entonces que tiene que transmitir, básicamente accede a la dirección web a través de la caché para no tener que hacer ya nuevamente el proceso de resolución. Esa fue entonces una breve descripción de cómo funciona el sistema de DNS. Cuáles son las vulnerabilidades del DNS. Primero, en el sistema original del DNS desarrollado en los 80, ahí la Internet era mucho más pequeña y la seguridad no era una consideración primaria de diseño. Los resolutores abiertos permitían a clientes que no eran parte del dominio administrativo usar el servidor para hacer resolución de nombres recursiva. Básicamente esto significa que cualquiera podía acceder al sistema DNS y hacer sus propias consultas.

El efecto de esto fue básicamente que el sistema era vulnerable a los ataques. La mayoría de los ataques eran del tipo de

denegación de servicio y luego denegación de servicios distribuida. Sobre esto vamos a hablar un poquito más después. Como resultado, entonces, cuando el resolutor recursivo envía una query al autoritativo, el servidor no tenía manera de verificar la autenticidad de la respuesta. Este era en realidad una de los fallos más comunes.

Las vulnerabilidades del sistema de DNS son las siguientes. El primero es envenenamiento de la caché. Estos ataques ocurren cuando un atacante envía un registro falsificado al resolutor del DNS. Algunos de nosotros quizá conozcamos esta situación. Por ejemplo, entrar al sitio web de un banco y encontrar que estamos en otro lugar. Esto es porque los datos han sido sometidos a spoofing. Lo que deberíamos recibir en una query normal no sucede porque es enviado al DNS. Los datos son almacenados en la caché y en la próxima query va al servidor raíz porque ha sido básicamente envenenado con el sitio web incorrecto. Esto se hace para obtener información sobre datos bancarios y luego cometer un delito.

Luego tenemos los ataques de amplificación y reflexión del DNS, que básicamente consisten en enviar mensajes a múltiples resolutores abiertos utilizando direcciones IP falsificadas. Se hace cierta edición de la dirección y esto produce fallas en el servidor y esto le preocupa mucho a las empresas.

El tercer tipo de vulnerabilidad es el ataque de utilización de los recursos. En este ataque se consumen todos los recursos disponibles para impactar de manera negativa a las operaciones del sistema del resolutor. Aquí luego se consideró incorporar cierto nivel de seguridad al sistema de resolución. Surge DNSSEC. DNSSEC básicamente suplementa la naturaleza jerárquica del DNS de lo que nosotros llamamos caracteres criptográficos. Con esto podemos garantizar que el DNS garantice la autenticidad de las queries que se envían al sistema, lo que lo hace más seguro. Lo hace a través de firmas criptográficas que se publican en formatos más seguros como para que no se puedan acceder fácilmente. Parte del efecto de esto es que consume más, utiliza más bytes de memo. En un mensaje normal del DNS tenemos 512 bytes mientras que en DNSSEC son hasta 4.096 bytes.

Con respecto a los índices de adopción y validación, en el mundo se considera que es el 20% pero en África la validación del DNSSEC llega al 22% de los usuarios. Ese fue el porcentaje a mediados de 2016 pero vemos que ha declinado al 12% a comienzos del 2018 y volvió al 18% de adopción a comienzos del 2019. ¿Por qué fluctúan estos datos? Porque a la gente no le interesa utilizar este sistema que parece aparentemente proporcionar más seguridad al sistema del DNS. Uno de los argumentos por los cuales la gente no quiere usar DNSSEC es

que aumenta el tamaño y la ineficiencia del sistema, considerando los tiempos, considerando que algunas queries pueden ser bloqueadas. La validación también lleva más tiempo y también los costos pueden superar el beneficio potencial para las empresas.

Como resultado, algunos no adoptan este sistema de seguridad. Para los que usan DNSSEC, que es altamente recomendable, son personas que consideran la seguridad de Internet como una prioridad. Son personas que también consideran que la confianza de los consumidores es vital y además DNSSEC hay que considerar que es un trabajo en progreso. Aun cuando no es perfecto, aun cuando los ingenieros trabajan en el sistema día a día, se considera que todavía hay aspectos a mejorar. Sin embargo, brinda más seguridad al espacio de Internet.

Debemos preguntarnos entonces cuán importante es la seguridad de nuestro espacio de nombres de dominio en comparación con los costos que deben afrontar las empresas que manejan este sistema. Para personas como ustedes y como yo, que estamos expuestos a sufrir el riesgo de situaciones como esta, deberíamos respaldar tener un sistema de nombres de dominio más seguro y más confiable. Mi recomendación, pienso que es algo sobre lo cual todos debemos reflexionar, es que para la seguridad del DNS no hay plan B que no sea el DNSSEC. Hay que respaldar la seguridad del DNS desde los mismos usuarios

finales y la experiencia operacional guiará el mayor perfeccionamiento de las herramientas del DNSSEC. Muchas gracias.

DEBORAH ESCALERA: Gracias, Adisa. ¿Alguna pregunta?

ORADOR DESCONOCIDO: Quería aclarar algo. El despliegue del DNS se hace a nivel ISP o a nivel host.

ADISA BOLUTIFE: Es a nivel ISP. Por eso dije que algunos consideran que esto no es conveniente desde el punto de vista económico, que no es un problema pero para los usuarios finales como nosotros, podríamos sufrir ataques. El envenenamiento de la caché y otras cosas que pasan. Es importante que nosotros a ellos los hagamos responsables y asegurarnos de que lo implementen.

ORADOR DESCONOCIDO: Entonces DNSSEC se despliega en los servidores autoritativos que usted mencionó. Hace firma digital, ¿verdad? ¿Cuál es la diferencia, por curiosidad, entre la firma digital…? Se tiene en la URL, se ve un lock cuando se ve un sitio web y se escribe un dominio, eso es firma digital. ¿Qué diferencia tiene con la firma

digital en los servidores autoritativos? ¿Cuál es la diferencia, me pregunto? ¿Qué diferencia proporciona en términos de seguridad?

ADISA BOLUTIFE: El sistema DNS funciona de dos maneras. Hay una conexión desde el usuario final cuando entra el nombre de dominio hacia el resolutor. Hay un resolutor stub. Del stub pasa al resolutor recursivo. En el recursivo hay un puente, un bridge. En el stub hay otro bridge. Entre estos dos espacios, el DNSSEC encripta el mensaje que va entre los dos extremos que son los dos extremos que podrían ser atacados. Eso es lo que lo hace tan único.

ORADOR DESCONOCIDO: Firmas digitales.

ADISA BOLUTIFE: Firma digital, de hecho, eso es lo que es el DNS. Claves criptográficas. Cuando uno tiene el HTTPS, cuando lee que hay HTTPS es más seguro.

ORADOR DESCONOCIDO: Si me permite, voy a corregir lo que decía. Estoy hablando en realidad de certificados digitales. En la URL, cuando aparece por

ejemplo facebook.com aparece un candadito al lado. ¿Qué protección significa eso? Por curiosidad.

ADISA BOLUTIFE: Significa que el query está encriptado. Eso es lo que hace el DNSSEC. ¿He respondido?

ORADOR DESCONOCIDO: Gracias.

ORADOR DESCONOCIDO: ¿DNSSEC significa que el usuario final tiene algún rol a la hora de garantizar la seguridad de los datos en el sitio web?

ADISA BOLUTIFE: Sí, exacto. Eso es lo que quería transmitir. A menudo, cuando una determinada tecnología o mejora no afecta directamente a la empresa, suelen no hacer nada. Eso lo vemos en África. Algunos casos ha habido donde se ha usado DNSSEC y después lo sacaron. ¿Por qué? Porque algunas de las consultas hacían que el sistema fuera más lento, costaba más dinero, representaba un mayor know-how administrativo. A lo mejor tenían que contratar a alguien. La relación costo-beneficio no cerraba y lo quitaban. Lo que digo es que nosotros, como

usuarios finales, nosotros no lo instalamos pero podemos exigir responsabilidad y que se garantice que el DNS sea seguro.

ORADOR DESCONOCIDO: Un comentario respondiendo a su pregunta sobre el navegador. Ese candado lo que significa es que se está usando HTTPS y cuando se usa HTTPS significa que es seguro, que la comunicación entre el navegador y el sitio está encriptada y no solo eso sino que el navegador valida la encriptación. Dice: "Este es un sitio web válido" y los certificados verificados por Verisign o por otra parte son válidos mientras que DNSSEC lo que hace es otro nivel, un nivel inferior. Lo que hace es decir: "Este es el nombre real". Previene algunos de los ataques como el de envenenamiento de la caché.

ORADOR DESCONOCIDO: ¿Podría darnos un ejemplo o una estimación de los costos y beneficios?

ADISA BOLUTIFE: Okey. Para ello necesito algunas estadísticas. Alguna la di en las diapositivas. Hablé de la memoria que se consume comparando 512 con 4.096 bytes. Esa es la diferencia. Imagínense los datos que hay que almacenar. También considerando el hecho de que tienen que emplear a una persona más, a un experto. El costo

aumento. Una desventaja que tiene es que no está totalmente refinado. No está perfeccionado. Por eso no es plenamente eficiente. A veces algunos sitios web se bloquean y las empresas no quieren ver sus sitios caídos. Creo que se ha hecho mucho en la seguridad actual del DNSSEC y se llegará al punto en que todos nos sintamos cómodos.

ANDY BATES: Soy Andy Bates, de Global Cyber Alliance, que es una organización que lucha contra el ciberdelito. Nosotros tenemos Quad9 que soporta muchas de las tecnologías de las que se ha hablado. Tenemos un paper que podemos compartir que muestra los beneficios no solo del filtrado del DNS sino también DNSSEC. Estoy de acuerdo con mi colega aquí pero el servicio Quad8 de Google y el servicio Quad9 de nuestra parte, todos esos son sin costo y tienen un impacto menor sobre el sistema.

ORADOR DESCONOCIDO: Yo asistí a la reunión del GAC donde hablaron del aspecto de política de DNS sobre HTTPS y TLS. A la hora de hacer una evaluación, ¿cuál diría usted que es el beneficio del DNSSEC? ¿DOH sería suficiente? Esto indica que un determinado nombre de dominio es auténtico. Me gustaría que usted me haga una comparación, una evaluación.

ADISA BOLUTIFE: DNSSEC es una de las medidas de seguridad que se pueden adoptar. Es una de las más importantes. Hay otras medidas de seguridad técnica que también se pueden aplicar. Lo principal del DNSSEC es su autenticación y encriptación. Si se necesita más seguridad hay otras tecnologías que se pueden agregar al sistema actual como él mencionó, Quad9.

DEBORAH ESCALERA: Gracias, Adisa. Nuestro próximo orador es Yashvi.

YASHVI PAUPIAH: Hola a todos. Gracias por venir. Soy Yashvi Paupiah, estudiante de Ciberseguridad de la Universidad de Mauricio y asociado en Ciberseguridad. Soy de una pequeña isla que se llama Mauricio que está ubicada a la derecha de la isla de Madagascar. Es conocida por sus playas, por ser un paraíso turístico. Con solo 24km^2. No tiene problemas de Internet importantes. La mayoría de las familias en 2018 no tenían acceso a Internet. Hay cuatro ISP que manejan los precios y vendrán otras empresas con más ancho de banda. Mauricio se está convirtiendo en uno de los países líderes en actividad en Internet que hará bajar los precios.

Esta presentación no es sobre la Internet en Mauricio sino sobre un equipo que intenta hacer un cambio en el país. ¿Quiénes

somos? Somos hackers.mu, una organización sin fines de lucro cuyo rol es empoderar a la población con herramientas para crear un mejor país. Empezamos siendo pequeños, con lecciones tales como usar GitHub, Hackathon. En IETF nos encontramos con estudiantes universitarios. Hacemos patching de código, a nivel universitario nacional e internacional.

Nuestro proyecto actual es el desarrollo de software para mejores prácticas. Está desarrollado sobre el zend framework 3, que será lanzado con una licencia opensource. Vamos a simplificar el uso de patrones. Será un marco basado en entidades. Es decir, podremos crear con mucha más facilidad operaciones [inaudible]. Con un hub simple tenemos encriptación para cualquier aplicación con actualización automática de seguridad. Los cambios van a ser aplicados en todas partes sin necesidad de acción. El propósito principal de este marco es construir proyectos para empoderar a la gente. Todos son proyectos comunitarios.

Estos son los proyectos en los que estamos trabajando ahora. Una aplicación móvil y web para dar recomendaciones sobre alimentación a gente que sufre de diabetes porque en Mauricio la prevalencia de diabetes en adultos entre 25 y 74 fue del 22,8%. Además, un servicio que permitirá transfusión de sangre más sencilla. El tercer proyecto es un servicio de prevención de desperdicio de alimentos vinculando a la gente que tiene

necesidad de alimentos y aquellos a los que les sobran los alimentos. Son todos proyectos comunitarios y gratuitos. Este es el equipo responsable del cambio. Tenemos una persona que trabaja en Dinamarca. También es un ingeniero en software, Yasir Auleear. Neeraj Joypaul trabaja en una organización de ingeniería. Van a encontrar más detalles en hackers.mu. Gracias.

DEBORAH ESCALERA: Muchas gracias. ¿Hay alguna pregunta?

ORADOR DESCONOCIDO: ¿Necesitan ustedes algún apoyo de la comunidad?

YASHVI PAUPIAH: Sí, claro. Necesitamos apoyo. En Mauricio, a nivel nacional, tratamos de que la empresa nos apoye, nos respalde, porque estos proyectos son proyectos comunitarios y la empresa puede dar algo. Nosotros siempre estamos necesitados. ¿Hay alguna otra pregunta? Muy bien. Gracias.

DEBORAH ESCALERA: Gracias. Nuestro próximo presentador es Ajani.

OLUWASEUN AJANI: Hola. Soy Oluwaseun Ajani. Soy de la Universidad de Ibadan, en Nigeria. Les voy a hablar de las soluciones de las ciudades inteligentes y de la propiedad intelectual. Voy a seguir este bosquejo para esta presentación. El objetivo es examinar el concepto de ciudades inteligentes e identificar las soluciones de ciudades inteligentes así como enumerar el nexo entre las ciudades inteligentes y la propiedad intelectual.

Las ciudades inteligentes son muy complejas. Este es un concepto que integra información y tecnología y distintos dispositivos que están conectados a la Internet de las Cosas para optimizar la eficiencia de las operaciones y los servicios de las ciudades. Las soluciones de las ciudades inteligentes crean ciudades globales, prósperas, sostenibles y muy vivibles. También lo que se desea es lograr un desarrollo sostenible y mejorar la infraestructura.

Se utilizan estas soluciones en situaciones de tráfico, por ejemplo, en las ciudades. También se utilizan para mejorar la calidad del aire y para reducir la congestión de tráfico. Se utilizan también en la gestión de la energía para poder maximizar el uso de la energía en la ciudad. También da información sobre el uso del agua en la ciudad. El uso de sensores también es aplicable a las ciudades inteligentes. También hay datos sobre la prevención del delito y plataformas del mapeo del delito. También se utilizan estas soluciones en distintas situaciones de gestión.

Vamos a conceptualizar la propiedad intelectual. La OMPI, la Organización Internacional de la Propiedad Intelectual divide la propiedad intelectual entre las creaciones de la mente y los trabajos artísticos, lo cual incluye símbolos, nombres, imágenes que se utilizan en el comercio. También se puede dividir en dos categorías que incluyen la propiedad industrial y los derechos de autor. La propiedad industrial incluye patentes de invenciones, marcas registradas, diseños industriales e indicaciones geográficas.

En cuanto a las indicaciones geográficas, tenemos un problema con el Amazonas y el .AMAZON. Amazon quiere el nombre de dominio se utilice para su empresa pero los países del Amazonas no están de acuerdo con ellos. Esto es parte de un problema industrial. Los derechos de propiedad intelectual son los derechos exclusivos del creador, a sus ideas y a sus activos tangibles. Tenemos distintos tipos de propiedad intelectual. Los derechos de autor se utilizan para proteger las creaciones artísticas, dramáticas y literarias de los autores como los poemas y las novelas. Las patentes se utilizan para la protección de soluciones innovadoras a los problemas y las soluciones deben estar caracterizadas por ser novedosas. Pueden ser invenciones, descubrimientos, etc.

También tenemos marcas registradas que establecen protección y derechos exclusivos al propietario y se utilizan para identificar

un bien o un servicio en particular. También se utilizan para identificar una empresa como Google o Microsoft. Ellos tienen distintas marcas registradas. Otra forma de propiedad intelectual es el secreto comercial. Un secreto comercial es utilizado por las empresas para que puedan tener una ventaja económica.

Ahora vamos a examinar el nexo entre la propiedad intelectual y las soluciones de ciudades inteligentes. Existe un problema con la propiedad de los datos. Dado que las ciudades inteligentes producen una gran cantidad de datos que pueden ser utilizados para generar predicciones, visualizaciones y otras formas de datos analíticos, la pregunta que tenemos ante nosotros es quién va a regir estos datos en las ciudades inteligentes. Quién tiene el derecho de la propuesta de los datos y quién controla a esos datos. Los usuarios de las ciudades inteligentes son los contribuyentes y ellos deben tener la propiedad de sus datos y no las empresas que los utilizan para su propio beneficio. Es decir, deben tener el consentimiento de darles a los propietarios la posibilidad de usarlos cuando quieran.

Otro tema también es el de la privacidad. Como dije antes, las soluciones de ciudades inteligentes están conectadas a la Internet de las Cosas y el problema con la Internet de las Cosas es la privacidad y la seguridad. Si vamos a maximizar el paradigma de las ciudades inteligentes debemos focalizarnos en

cómo proteger la seguridad de estas soluciones y la privacidad también para que podamos tener un crecimiento sostenible de estas soluciones.

¿Cómo se vincula la ICANN con la propiedad intelectual? La ICANN tiene una unidad constitutiva de propiedad intelectual que representa a los usuarios de la comunidad de propiedad intelectual en todo el mundo con un énfasis particular en las marcas registradas, los derechos de propiedad intelectual y sus efectos e interacción con el sistema de nombres de dominio.

Como dije antes sobre el tema del Amazonas y .AMAZON, se quiere usar un nombre en particular para una solución. Se trata aquí de un indicador geográfico. La ICANN debería tratar de asegurarse de que los derechos de las ciudades sean protegidos cuando los nombres de dominio se registran.

En conclusión, las ciudades inteligentes proveen una gran cantidad de oportunidades para la innovación en las ciudades sostenibles y la protección de los derechos de propiedad intelectual expanden estas soluciones. Si vamos a tener una proliferación de ciudades inteligentes y de interconectividad debemos estar seguros de que vamos a proteger la propiedad intelectual de los creadores de estas soluciones.

También es importante que tengamos una estrategia de gobernanza de datos. Las ciudades inteligentes los deben

brindar para que la privacidad esté bien protegida. Podemos utilizar estrategias para promover la innovación y que se puedan dar a los creadores de estas soluciones derechos explícitos sobre sus inventos. Gracias por haberme escuchado.

DEBORAH ESCALERA: Muchas gracias. ¿Hay alguna pregunta?

IHITA GANGAVARAPU: Gracias, Ajani, por la presentación. Soy embajadora de NextGen. Quisiera saber si hay alguna recomendación o política o propuesta dentro del país que se ha presentado por el gobierno o por alguna organización del sector privado. ¿Quién debe tener la propiedad entonces de los datos? Quién la tiene y quién la debe tener. Cuáles son los procesos. ¿Hay alguna recomendación o política dentro del país?

OLUWASEUN AJANI: En general, no hay una política sobre quién está a cargo de los datos en las ciudades inteligentes porque estamos entrando en el paradigma de las ciudades inteligentes. Las soluciones de ciudades inteligentes están comenzando a penetrar en el mercado de la Internet de las Cosas en el continente africano. Estamos hablando de la protección de los datos de los usuarios que no es realmente por el momento una inquietud. Se le ha

presentado una estrategia al presidente de Nigeria pero por ahora no ha sido aprobada. Gracias.

ORADOR DESCONOCIDO: Este es un comentario y quizá una recomendación. Lo que está ocurriendo es que todo el mundo está recolectando datos y los guardan como un tesoro, lo que no resulta utilizable para nadie. ¿Qué pasa si estos datos se ponen a disposición de la comunidad académica y quien los pueda utilizar para data mining? ¿Qué es lo que ocurre con la inteligencia? Creo que esta debería ser una de las recomendaciones.

ORADOR DESCONOCIDO: Quisiera agregar algo. Tengo una pregunta y algo para agregar. Primero, nosotros tenemos un honeypot IoT. Son dispositivos de IoT. Nosotros compartimos los datos con universidades en el mundo pero podemos compartir incluso más. Para cargas los dispositivos de IoT en un honeypot tenemos que utilizar ese software y tenemos que tener la propiedad intelectual. Uno le da un software a alguien que no lo conoce. Quisiera saber qué es lo que ustedes piensan sobre los beneficios de la protección de dispositivos IoT. Usted está hablando de los desafíos y no es normal que se divulgue el código a un tercero.

OLUWASEUN AJANI: La propiedad intelectual, nosotros promovemos la competencia entre las empresas. Por eso es importante. Se debe tratar de proteger la propiedad intelectual para que otros sean lo suficientemente innovadores para desarrollar sus propias soluciones de ciudades inteligentes, que haya un buen desarrollo sostenible.

GLENN MCKNIGHT: Hola. Soy Glenn McKnight, miembro de la junta directiva de ISOC y voluntario de NextGen. Yo estoy involucrado en algo que se llama IEEE Ciudades Inteligentes que tiene un proyecto en Nigeria. Seguramente ustedes vieron este concepto de las ciudades inteligentes. ¿Lo han dividido ustedes en ciudades más pequeñas?

OLUWASEUN AJANI: No.

GLENN MCKNIGHT: Le voy a dar un contacto para las ciudades inteligentes.

OLUWASEUN AJANI: Gracias.

DEBORAH ESCALERA: Muy bien. Vamos ahora a nuestra última presentadora, Sulaimon. Un momento, voy a cargar la presentación.

MORIAM SULAIMON: Hola a todos. Soy Moriam Sulaimon, de la Universidad de Ilorin en Nigeria. Les voy a presentar el tema de Internet como una herramienta para empoderar a las mujeres en África. Vamos a hablar del acceso a Internet en África que está limitado porque hay una baja penetración. Solo un cuarto de los africanos tiene acceso a una Internet rápida aunque la región está creciendo. De acuerdo con la UIT, el crecimiento es 54% en África desde el año 2000 hasta el 2019. La penetración es menor porque hay menos mujeres con respecto a otros lugares del mundo. De acuerdo con la ONU se trata del 54% y la mayoría de ellas no pueden usar Internet. Solamente hay actividades. En general se las ve como objetos que solamente tienen que tener hijos y no deben tener una voz. Sin embargo, la Internet va a ser una voz para todos.

Tenemos barreras para las mujeres africanas y para que accedan al uso de Internet. El acceso de las mujeres africanas en Internet aumenta pero el número de dificultades todavía persiste. Vamos a ver algunas. La falta de conciencia sobre la Internet y su uso. La mayoría de las mujeres en África ni siquiera sabe qué es Internet. No saben cómo funciona ni mucho menos lo saben usar. No tienen suficiente información sobre Internet.

En cuanto a las barreras, como la mayoría de los hombres en áfrica, las mujeres en áfrica están muy interesadas en hacer uso de Internet. Quieren saber cómo evoluciona Internet pero vamos a hacernos preguntas. Hay mujeres que creen que simplemente tienen que ocuparse de sus hijos y de su familia. La usabilidad también es una barrera para las mujeres en África. Vamos ahora a hablar de los sitios web. El diseño de los sitios web puede ser un factor que permite la participación de las mujeres.

En cada país en África hay un idioma propio que se utiliza. Por ejemplo, en Nigeria tenemos distintos idiomas. Por eso tenemos que tener un idioma estandarizado para Internet, que pueda soportar distintos idiomas. Es decir, que cuando las mujeres estén interesadas en hacer uso de eso, no pueden tener problemas con el diseño y no tengan problemas con los iconos ni tampoco en cómo están diseñados los sitios web.

Luego está el tema de los problemas de disponibilidad. La mayoría de ellas no tienen trabajo. La mayoría de las veces las mantienen sus maridos. No tienen dinero, no tienen los recursos financieros para poder incluso estar cerca de utilizar Internet. Luego tenemos el ciberacoso. Las mujeres están muy afectadas por este tema. Sus comunicaciones, les envían mensajes donde las intimidan. Tienen un muy bajo nivel de conocimiento y de educación. Estamos hablando de muchas personas en estos países que no tienen acceso. Es poco posible que conozcan los

idiomas internacionales que dominan la Internet. No tienen habilidades informáticas. La mayoría de ellas ni siquiera tiene una capacitación. No tiene educación. No tienen otros idiomas más allá de su idioma nativo.

Otro factor o barrera que las afecta es que tienen poco tiempo. Las mujeres en África tienen unas responsabilidades. Muchas de ellas ni siquiera pueden utilizar Internet. No tienen el tiempo de hacer uso, de poder evaluarlo. Hablemos ahora de la cuestión geográfica. Las mujeres en África viven en áreas rurales, más que los hombres. En esas áreas rurales la infraestructura es menos accesible y por eso para ellas viajar a los centros geográficos es difícil por el tiempo, el costo y la resistencia cultural.

Luego, en los departamentos de Ciencias e Ingeniería en universidades, la mayoría de estos departamentos de Ingeniería, de Matemáticas tienen dominación masculina. Cuando hay mujeres a las que les interesa participar en estos departamentos, sufren intimidación. Un ejemplo en mi facultad. El departamento de Ciencias de la Computación. Hay muchas mujeres en realidad pero cuando van a las clases hay más hombres que mujeres. “¿Cuándo van a tener estas mujeres tiempo para programar?”, se les dice. Se tienen que ocupar de los hijos, de los hogares. No tienen una voz real.

Ahora quiero hablar sobre cómo podemos superar estas barreras. Para las mujeres en África, el acceso y el uso de la Internet deben ser encarados con ciertas medidas. A través de, por ejemplo, la capacitación y la educación formal. Capacitación y educación formal. La mayoría de las mujeres no usan dispositivos de TIC pero se les podría brindar capacitación como un outreach en tecnología, capacitación que les permita a estas mujeres usar las tecnologías, incluir la educación en Internet en los planes de estudio de las escuelas, educación sobre tecnologías de la información y la comunicación para que desde el comienzo tengan interés porque así si empiezan a leer desde una temprana edad van a promover el uso con un sistema que produzca contenidos y aplicaciones.

Muchas de estas mujeres viven en áreas rurales. Si queremos garantizar que se use la Internet, tenemos que alentar el uso y la adopción local para generar interés porque verán contenidos locales estas mujeres que les resultarán beneficiosos a ellas. Así harán uso de las TIC y de la Internet.

Luego apoyo y asesoramiento continuos en el uso de la Internet. Debemos continuar con el asesoramiento, con el apoyo, dándoles cada vez más empoderamiento en el uso. Las mujeres, a través de este apoyo y asesoramiento constantes, las mismas mujeres generarán un cambio en el uso de Internet porque les podemos dar capacitación formal y educación. Todo esto tiene

que generar un cambio en el uso de la Internet. Si yo creo que algo es bueno y útil para mí, esto significará un progreso a través del cambio que yo voy a promover.

Cuando exponemos a las mujeres a los beneficios, van a querer participar. Cuando ven a otras mujeres en este espacio que progresan, piensan: “Yo también puedo hacerlo”. Promover un mayor empleo de las TIC para las mujeres. Estas empresas no tienen mujeres empleadas porque en África se considera que el hombre se desempeña mejor en el sector de las TI pero no es así. Aumentando el empleo femenino en este sector genera una mayor confianza en que yo puedo trabajar en este sector. Las mujeres no creen que desde la escuela pueden ser capaces de trabajar en este sector.

Luego mejorar el diseño y la usabilidad. Hay que simplificar el diseño, que sea sencillo y comprensible, asegurarse de que el lenguaje local y nativo sea utilizado según el país. Luego brindar cobertura y acceso. Brindar cobertura y acceso. Estas áreas rurales en África no pueden usar Internet o acceder a ella porque están en áreas rurales. No se usa Internet en estas áreas porque se creen rurales y no creen poder hacerlo pero si se amplían las áreas rurales, hará que no sea necesario viajar, salir de estas áreas rurales. Podrán usar la Internet cerca de sus hogares. Si pueden usar Internet, podrán tener acceso a servicios. Hay que asegurarse de que no sean servicios costosos. Estas mujeres no

tienen grandes ingresos al hacer servicios accesibles, ellas harán más uso y ahí comprenderán el valor del uso de la Internet. Tienen que conocer este valor de usar la Internet. Si usan Internet, tendrá un impacto positivo sobre ellas.

¿Cuál es el camino a seguir para tener éxito en el futuro? El advenimiento de Internet ha cambiado el escenario global y muchas áreas que antes no habían sido exploradas ahora lo son. Nosotros tenemos que aprovechar los beneficios al máximo. Tal como hablamos de las barreras, hay barreras comunitarias pero también en el futuro, si nosotras, las mujeres africanas, estamos listas para aceptar el uso y alentamos el uso y la participación, cada hogar tradicional ortodoxo en África puede usar la Internet, las mujeres no necesitarán salir de sus casas. Podrán cuidar sus hogares y sus niños desde sus propios hogares. Hay mujeres emprendedoras, muchas en África, que pueden dejar su marca a nivel global solo si participan, solo si las familias las apoyan y si hay instalaciones, solo si pueden participar en este sector de las TI. Con una simple capacitación y más conocimiento podremos hacer una gran diferencia.

Como conclusión, si bien Internet ofrece eficiencia y ganancias de productividad, se puede compartir información, almacenamiento y comunicación, más conocimiento, diseminación, debe ser para propósitos específicos. Hay todavía barreras que superar para mejorar el acceso de las mujeres y el

uso de Internet y que participen plenamente en el ecosistema de Internet. Las mujeres africanas tienen una mentalidad ya adoptada de que la inteligencia puede desarrollarse. Deben creer en sí mismas y persistir a pesar de los obstáculos y ver el esfuerzo como un camino hacia la pericia y abrazar el desafío de usar Internet. Deben relacionarse con la tecnología para poder participar en esta conformación del ecosistema de Internet y abrazando este desafío promover la estabilidad y la seguridad de Internet. Así podremos cambiar esto para beneficio no solo de las mujeres en África sino de las mujeres de todo el mundo. Podremos tener una mayor voz y esto promoverá la inclusividad en el ecosistema de la Internet donde ambos géneros participarán por igual en el ecosistema. Gracias por su atención.

DEBORAH ESCALERA: Gracias. ¿Alguna pregunta?

IGITA GANGA VARAPU: Gracias pos su presentación. No tengo una pregunta sino una breve sugerencia. Seguramente después de esta reunión, al volver a su país seguramente planificará eventos. Quizá un programa de concientización o un taller de capacitación en habilidades. Hace seis meses en India organizamos la Universidad de Mujeres. Usted mencionó este problema de que las familias ortodoxas no permiten a las niñas. Habría que

alentarlas a participar en estas actividades. Lo que nosotros hicimos fue un evento con cobertura mediática. Ustedes podrían comenzar con niñas o jóvenes que ya están estudiando algún curso de IT, Políticas, Derecho, no importa. Que sean estudiantes universitarias. ¿Qué pasa si se comienza con estudiantes universitarias? Se arma un equipo, un equipo para trabajar a futuro y luego se las va capacitando para contactar a familias que no comparten estos objetivos del todo. Además, otra cosa que ayuda mucho es la cobertura mediática, en especial en nuestros países en desarrollo. Gracias.

MORIAM SULAIMON: Gracias. Entiendo.

INNOCENT ADRIKO: Gracias. Quiero hablar de un caso en Uganda. En Uganda nosotros no menospreciamos a las mujeres porque ya ocupan muchos cargos, tanto en el espacio tecnológico como en otros. Mi pregunta en este momento es la siguiente. ¿A las mujeres realmente les interesa este espacio de la tecnología? En Uganda, aun cuando las oportunidades están abiertas para ellas vemos muy pocas mujeres en el espacio de la tecnología. Por ejemplo, en mi curso, Tecnologías de la Información, somos 30 y hay solo cuatro mujeres. Mi pregunta es: ¿A las mujeres realmente les interesa el espacio de la tecnología? Si no, ¿cómo las podemos

atraer? ¿Cómo podemos convencerlas de que tienen que ser parte? Por supuesto, hay otros factores. Por tradición, en África las mujeres supuestamente tienen que estar en la cocina pero ya dejamos atrás esa era, me parece. Creo que ya la dejamos atrás. Tendríamos que pensar en la próxima etapa. Deberíamos apoyar a las mujeres. Gracias.

CYNTHIA JADE MAKORY: Soy Jade Makory, NextGen. En relación con lo que decía Innocent, yo considero que como África es el foco y como geográficamente hay disparidad entre los distintos pueblos africanos e incluso dentro de cada país, desde la capital hasta las áreas rurales, hay diferencias. Creo que hablar en general de todas las mujeres africanas no sería la mejor descripción porque los distintos lugares muestran realidades distintas.

DEBORAH ESCALERA: Yo soy Marcus Okwu Eke, de BC. Muchas gracias por la presentación. Si me permiten una sugerencia, yo creo que en África la mayoría de las mujeres son tratadas como bienes. Cuando se habla de la Internet para las mujeres habría que pensar qué hacen en Internet. Una sugerencia, si me la piden, es la siguiente. Hacer un proyecto o tener una estrategia para incluir a las mujeres financieramente, para que puedan hacer negocios en Internet. Un proyecto, un programa que se organice

para estas emprendedoras, estas comerciantes. Ver cómo involucrarlas, ayudarlas a entender las herramientas básicas para hacer negocios, comercio. Ese sería mi enfoque. Gracias.

ORADOR DESCONOCIDO: Yo soy [inaudible], de Nigeria, de la unidad constitutiva comercial de la ICANN. Buena presentación pero hace 20 años que estoy en el espacio tecnológico. Es curioso que el espacio tecnológico para las mujeres en Nigeria, y voy a hablar de Nigeria, no puedo hablar de África, es muy desafiante. En la práctica, es masculino. Hay que pensar y actuar como un hombre. He sido la única estudiante mujer en mi universidad, en toda mi carrera. Entiendo lo que usted dice pero hay ONG que hoy día trabajan en proyectos en Nigeria, [WTech], el Centro de la Mujer. El problema principal tendría que ser no llevarlas a la complejidad de la tecnología, no incorporarlas sino llevar la tecnología a ellas. El hecho de llevar a las mujeres al comercio, sé que hay algunos proyectos, algunas mujeres son buenas en artesanía. Quizá le podemos enseñar a promover sus emprendimientos en las redes sociales, alentarlas a hacer ventas. Es un proceso gradual. No se hace de la noche a la mañana sino paso a paso. Se va construyendo a medida que se avanza, a pesar de los obstáculos. En 1998 recuerdo que cuando comenzó en Nigeria este desarrollo, hay que seguir trabajando

porque si no, estaremos igual en 50 años. Esfuércense y va a funcionar.

MORIAM SULAIMON: Gracias, [inaudible].

ROGER BAAH: Soy Roger Baah, de Ghana. También de la BC. Buena la presentación que seguí con atención. Yo trabajo en Ghana con un proyecto de habilidades para niñas y jóvenes, [inaudible]. Lo vemos desde los planes de estudio que se usan en las escuelas, que no son amigables para las mujeres. Lo que estamos haciendo ahora es trabajar con el Ministerio de Educación. El plan de estudios se desarrolla con un espacio específicamente técnico, con instituciones profesionales para desarrollar el plan de estudios, para que sea amigable para las mujeres porque en las escuelas técnicas hay solo varones. Ahora estamos tratando de introducir nuevos cursos que resulten atractivos para las mujeres. Este es un muy buen paso que va más allá de la pequeña organización. Hay que tener una perspectiva más amplia. Los planes de estudio, hay que analizarlos. Creo que es muy buen paso y lo voy a seguir. Cualquier ayuda que necesite, aquí estoy. Gracias.

DEBORAH ESCALERA: ¿Alguna otra pregunta? Como nos queda un poco de tiempo quería saber si quedaban preguntas para los presentadores anteriores de hoy o de ayer sobre cualquiera de las presentaciones vistas. Adelante.

ORADOR DESCONOCIDO: Una pregunta para Adisa que tiene que ver con lo que pregunté antes. ¿Podría nuevamente indicarme la diferencia entre DNS sobre HTTPS, DNS sobre TLS y DNSSEC?

ADISA BOLUTIFE: Gracias por la pregunta. DNSSEC es bastante diferente de DNS sobre HTTPS y el DoT también. Básicamente, DNSSEC funciona con la autenticación y garantizar que el nombre de dominio sea auténtico y válido. El DoH sobre HTTP funciona en un nivel diferente. La encriptación en DoT no se hace a nivel del usuario, lo cual significa que el resolutor no está encriptado pero para DNS sobre HTTPS hay una encriptación que va desde el usuario hacia el resolutor recursivo que está en el sistema de nombres de dominio.

El DOH se considera más seguro que el DoT, lo cual en base a la recomendación actual es el más seguro. Creo que esto sería lo mismo que lo que estaba tratando de aclarar también. Cuando usamos un sitio web que tiene HTTPS sabemos que es más

seguro, es una forma más segura de conectarse a Internet. Espero haber podido responder.

ANDY BATES: Yo puedo agregar algo más. Hay unas buenas diapositivas de ayer que están de acuerdo con lo que usted dice. Sería bueno decir que es bueno tener DNSSEC y luego implementar uno de los otros factores, DoH y DoT, que se complementan. DNSSEC confirma el ingreso del DNS, mientras que las otras dos soluciones evitan que haya un ataque de una persona en el medio mientras se espía lo que está ocurriendo. Uno va de punta a punta y hubo mucho debate ayer sobre el hecho de que los navegadores, el navegador Mozilla por ejemplo, automáticamente configura a qué resolutor va. Había mucha emoción también en la sala en el sentido de qué es lo que tiene que hacer el usuario. Uno es completamente punta a punta, lo que parece muy bien, pero tiene desventajas en términos de los servicios a los que lo lleva. En esencia, hacer DNSSEC y DoT o DoH hace que el mundo sea un lugar un poco más seguro.

DEBORAH ESCALERA: ¿Podría clarificar por favor a qué sesión de ayer se refería?

ANDY BATES: Sí. Denme un minuto y se lo voy a decir.

MELCHIZEDEK ALIPIO: Hola. Soy Mel, embajador de NextGen. Mi pregunta es para Ajani. Me da curiosidad saber si hay investigaciones sobre las ciudades inteligentes en África y cómo hace uno para solicitar una patente sobre las ciudades inteligentes. Gracias.

OLUWASEUN AJANI: Nosotros tratamos de reducir el estudio al contexto de Nigeria.

MELCHIZEDEK ALIPIO: Claro, ¿pero conoce usted alguna universidad africana o en su país que desarrolle ciudades inteligentes? Quizá no un proyecto enorme pero al menos un proyecto pequeño que implique soluciones para ciudades más inteligentes.

OLUWASEUN AJANI: En realidad hay una cantidad de empresas que desarrollan soluciones IoT para ciudades inteligentes. No puedo recordar sus nombres realmente. Si me ve después, le puedo dar algunos detalles más específicos.

ORADOR DESCONOCIDO: Esta es mi experiencia en Nigeria. Uno de los desafíos centrales de las ciudades inteligentes siempre ha sido la conectividad. Para desarrollar esa tecnología se necesita una cierta velocidad,

un cierto nivel. En este momento en Nigeria tenemos problemas con la electricidad. Siempre hay un desafío en ese sentido con los problemas de la electricidad. También con el ancho de banda. En Estados Unidos y en China están pensando en el 5G, que sería excelente para la innovación pero todavía la red en Nigeria es muy lenta. Creo que para África sería lo mismo en otros países. Sé que Sudáfrica, quizá Kenia, ellos tienen mejores desarrollos en ese sentido.

ORADOR DESCONOCIDO: Algo que también pueden tener en cuenta es el plan de desarrollo de [inaudible], que es un proyecto de ciudad inteligente de Kenia. Kenia está tratando de generar esa tecnópolis. Creo que sería algo muy bueno a tener en cuenta ahora que ustedes pueden ver la investigación. Creo que Sudáfrica también tiene algo parecido. Creo que podemos de hecho compartir información.

DEBORAH ESCALERA: Este es el nombre de la sesión.

ANDY BATES: Fue ayer a las 15:15 y se llama “Aspectos de política del DNS sobre HTTP y DNS sobre TLS”.

DEBORAH ESCALERA: Muy bien. Pueden tomar nota y pueden ver la sesión que queda colgada online después de la reunión así que si no pudieron ir, pueden ir y verla por Internet. ¿Hay alguna otra pregunta final? Tenemos a alguien más allí atrás.

ORADOR DESCONOCIDO: Hola. Mi nombre es [inaudible], de Botsuana. Quisiera comentar sobre la presentación de Cynthia. Ella hablaba de todo lo ciber. Con lo ciber es difícil porque solamente podemos hacer intentos. Podemos utilizar nuestra infraestructura técnica una y otra vez para que sea lo mejor posible. También podemos implementar programas nacionales para tratar de luchar esta guerra. Gracias.

ORADOR DESCONOCIDO: Quisiera retornar a la sesión que usted quiere que veamos online. Me parece que no puedo encontrar el link.

DEBORAH ESCALERA: Yo los puedo ayudar. No las postean directamente. A veces tarda un tiempo hasta que las cargan pero seguramente lo van a tener ahí. Glenn tiene un anuncio.

GLENN MCKNIGHT: Algunos de ustedes me preguntaron sobre los vídeos. Las fotos ya están subidas. Las pueden ver en Flickr. Que nadie venga y me pregunte otra vez. Ese es el número uno. Número dos, todos son de Creative Commons. Pueden tomarlas, las pueden mandar a su mamá, a su abuela. Se lo recomiendo mucho. También a su empleador, a sus profesores. Esto es algo muy importante que ustedes hicieron aquí. No todo el mundo es seleccionado para NextGen, por eso es importante que utilicen las redes sociales efectivamente y que expliquen por qué lo están haciendo.

Número dos, los vídeos. Tuve que ir a hacer otra foto pero creo que tengo todos los vídeos excepto la primera persona. Podemos hacerlo de nuevo. Los vídeos de todos van a ser cargados. Algunos están listos. No lo puedo cargar hasta que terminemos. Creo que ya terminamos con los vídeos. Fue muy bueno. Muchas gracias por su buen trabajo.

ORADOR DESCONOCIDO: Mi trabajo es el suyo y su trabajo es el mío. También tenemos un problema con los nombres.

ORADOR DESCONOCIDO: Creo que usted también mencionó la investigación de su organización.

ANDY BATES: Hay una Global Cyber Alliance, globalcyberalliance.org. Si alguien quiere ayuda con algo de esto, se la podemos dar.

DEBORAH ESCALERA: ¿Alguna última pregunta? Con esto entonces vamos a cerrar la sesión un poco más temprano pero vamos a darle un aplauso a este excelente grupo de NextGen. Gracias a todos por su trabajo. Como dijo Glenn, compartan lo que hicieron. Vamos a hablar de eso también en el almuerzo. Estén orgullosos de lo que hicieron. Expliquen a la universidad de su país lo que han hecho aquí. Gracias.

GLENN MCKNIGHT: Con ISOC nosotros acabamos de mejorar el programa de fellowship. Pueden mirar el sitio web de ISOC. Hemos hecho cambios para que esté focalizado en la gente que está en la mitad de su carrera. Esto debe ser parte de su currículum.

[FIN DE LA TRANSCRIPCIÓN]