ICANN72 | Reunión General Anual Virtual – Presentaciones de NextGen
Lunes, 25 de octubre de 2021 – 10:30 a 12:00 PDT

DEBORAH ESCALERA: Hola a todos, bienvenidos a la sesión de NextGen en la reunión ICANN72, soy Deborah Escalera y soy gerente del programa de NextGen en la ICANN, coordinaré la participación remota durante esta sesión. Esta sesión está siendo grabada y se rige por estándares de comportamiento esperado de la ICANN.

En esta sesión solo se leerán las preguntas y comentarios presentados en el formato que indiqué previamente en el chat, leeré las preguntas y comentarios en voz alta cuando quien preside o modera la sesión me lo indique. Tenemos interpretación al inglés, francés y al español, hagan clic en el ícono de interpretación en Zoom y elijan el idioma que deseen escuchar durante la sesión.

Para tomar la palabra levanten la mano en Zoom y cuando el coordinador diga su nombre, el equipo técnico les permitirá habilitar su micrófono y tomar la palabra. Antes de hablar asegúrense de seleccionar el idioma en que hablarán en el menú de interpretación, digan su nombre para los registros e indiquen el idioma en el que hablarán, si se trata de un idioma que no sea inglés.

Asegúrense de silenciar todos sus dispositivos y notificaciones al tomar la palabra, hablen en forma clara y a una velocidad adecuada para permitir una interpretación correcta. Por favor, utilicen el menú

desplegable en el chat y elijan la opción “responder a todos los panelistas y participantes” para que todos puedan ver sus comentarios.

Tengan presente que los chats privados solamente son posibles entre los panelistas, cualquier mensaje que se envié entre un panelista y un participante estándar será visto por los demás participantes.

Dicho esto, les doy la bienvenida, nuevamente, a esta sesión y les agradezco muchísimo a todos los participantes del programa NextGen por su arduo trabajo para preparar estas sesiones y también quiero agradecerles a nuestros mentores que trabajaron incansablemente para preparar a los participantes para que estén listos para estar aquí hoy en esta reunión ICANN72.

Esto no habría sido posible sin su colaboración, así mismo, le agradezco muchísimo a mi colega, Siranush Vardanyan quien se encargará de compartir pantalla y mostrarnos las presentaciones durante la sesión. En virtud del tiempo disponible, le voy a dar la palabra a Sarah Alsamman quien será la primera oradora y continuamos aguardando a que Siranush comparta la pantalla.

Sarah, tiene la palabra. Muchas gracias, Siranush, por mostrarnos la presentación. Sarah, adelante por favor.

SARAH ALSAMMAN: Muchas gracias, Deborah. Hola a todos, gracias por invitarme a participar hoy, quiero hablar acerca del DNS y el uso indebido de los contenidos en la web, específicamente la desinformación. Para quienes no estén familiarizados con el termino, el DNS o Sistema de Nombres de

Dominios, es el sistema que hace posible que se conecten los dispositivos con el internet y al igual que otros sistemas, es proclive al uso indebido.

Como lo dijo el comité asesor gubernamental de la ICANN, son quienes tienen la misión de administrar la infraestructura del DNS, deben tomar las medidas para asegurarse de que este recurso público sea seguro y confiable para que el público confíe en internet y pueda realizar o efectuar sus comunicaciones.

Mis objetivos para esta presentación es incentivar el diálogo con la comunidad acerca de esta cuestión tan importante y también incentivar a la comunidad de la ICANN a que continue combatiendo el uso indebido de esta herramienta.

Antes de poder abordar adecuadamente el uso indebido del DNS, tanto registros como registradores deben comprender cómo definir este uso indebido, según el marco para el uso indebido del DNS publicado en el marco de políticas sobre internet y jurisdicciones, tenemos estas cinco instancias de uso indebido, Malware o software malicioso, botnets, phishing, pharming y spam.

También tenemos el uso indebido del contenido que no es técnico y, por lo tanto, amerita su propia distinción, para proteger la libertad de expresión los registros y registradores, en general, no tienen que cumplir con la obligación de actuar en lo que respecta al uso indebido del contenido, sin embargo, hay excepciones específicas que tienen que ver con materiales de abuso sexual infantil, tráfico de personas,

distribución ilegal de sustancias opioides en línea y también incitaciones probadas y creíbles a cometer actos violentos.

Ahora bien, ahora que hemos definido el uso indebido del contenido en el DNS, quiero contarles acerca de los botnets que funcionan en las redes sociales. Todos sabemos que los algoritmos de procesamiento de datos son cada vez más importantes en lo que respecta nuestra percepción de la realidad.

En general, se busca manipular la opinión pública en lo que respecta o dentro de aplicaciones de redes sociales que usamos a diario, en general, estos botnets tratan de generar una percepción pública que tiene un impacto directo sobre nuestras prioridades políticas o sociales, esto se ve en la propaganda computacional y les voy a compartir algunos casos de estudio más adelante.

Según estos estudios, estas situaciones se dan en situaciones de crisis porque en estos momentos se genera una incertidumbre colectiva, entonces esto hace que el público en las redes sea sumamente influenciable.

En una publicación británica del British Journal of Sociology, una revista especializada en sociología, se publicó este caso acerca de un atentado en Manchester en el cual salió una publicación en redes sociales indicando que una persona estaba alojando a 60 niños y había publicado su número telefónico. Esto se publicó en Twitter y en Facebook, a esta mujer se le denominó el ángel de Manchester en uno de los periódicos más importantes, pero esto nunca sucedió.

Esto se conoce como evento ghosting o evento falso, la mujer declaró que jamás había compartido su número telefónico y que estaba muy asustada porque recibía llamados telefónicos durante la noche. Hubo aproximadamente 20 de estos eventos falsos que crearon caos durante toda la noche.

Hubo otro incidente en el cual se hizo una publicación en Facebook y se decía que había una persona armada disparando contra las personas en un hospital, este posteo fue compartido en distintas cuentas, 368 cuentas de Twitter, el hospital negó esta información falsa, sin embargo, esta información continuó circulando en momento cruciales posteriores al atentado terrorista.

Algunos equipos de emergencia siguieron esta información falsa y evitaron llagar al hospital. Estas situaciones son muy peligrosas porque impactan el bienestar y la seguridad de las comunidades a gran escala porque en las redes pueden interrumpir las comunicaciones entre los servicios de emergencia y el público al cual tienen que prestarle un servicio.

Entonces el uso indebido del contenido en los sitios web representa una amenaza para la seguridad civil y para la vida en general, con lo cual tenemos que incentivar la adopción de medidas proactivas para combatir este uso indebido y esto se debe hacer en la comunidad de usuarios a futuro. Muchas gracias.

DEBORAH ESCALERA: Muchas gracias, Sarah, muy buena presentación. ¿Alguien tiene alguna pregunta para Sarah? Voy a ver en la sala de Zoom, no veo ninguna pregunta, no veo que nadie este levantando la mana. Muy bien, también podemos formular preguntas al final de todas las presentaciones.

Ahora le damos la palabra a Meri que será nuestra próxima oradora, vamos a aguardar a que se vea su presentación en pantalla.

MERI BAGHDASARYAN: Muchas gracias, Deborah y Siranush. Buenos días, buenas tardes, buenas noches a todos, soy Meri Baghdasaryan, estoy estudiando derecho en la facultada en la Universidad de Pensilvania y me interesa mucho el tema de la acreditación de servicios de privacidad y proxy o representación.

En el 2013 la Junta Directiva de la ICANN aprobó en nuevo acuerdo de acreditación de registradores o RAA, es el contrato que rige las relaciones entre la ICANN y sus registradores acreditados, sus disposiciones tienen un impacto sobre los registratarios y las terceras partes que participan en el sistema de nombres de dominio.

Estas disposiciones se acordaron entre la Junta Directiva de la ICANN y el grupo de partes interesadas de registradores y la Junta Directiva de la ICANN solicitó un informe específico sobre este tema y en consecuencia el consejo de la GNSO comenzó un PDP especifico, se identificaron inquietudes pendientes que tiene que ver con los servicios de privacidad y representación.

El RAA de 2013 contiene una especificación temporaria que tiene que ver sobre servicios de privacidad y representación, el plazo de caducidad fue prorrogado varias veces y caducará el 21 de julio de 2022, o bien cuando la ICANN implemente en nuevo programa de acreditación, lo que suceda primero.

Veamos de qué se tratan estos servicios, tenemos algunas especificaciones que los definen, un servicio de privacidad permite que todos los detalles de contacto del titular de un nombre registrado o, mejor dicho, sean brindados no por el registratario mismo, sino por un proveedor de servicios de privacidad.

En el caso de los servicios de representación, estos permiten que el uso del nombre de dominio sea licenciado a un tercero y la información de contacto en el directorio correspondiente, sea proporcionada por un proveedor de servicios de representación o proxy.

DEBORAH ESCALERA: Meri, usted está siendo muy clara en su presentación, pero le pido que por favor hable un poco más despacio.

MERI BAGHDASARYAN: Sí, como no. Continúo. Entonces dentro de esta especificación que se encuentra vigente, tenemos un conjunto mínimo de requisitos aplicables a los servicios de privacidad y representación que son los cuatro que vemos en pantalla. La divulgación de los términos claves de servicios, la publicación de datos de contacto para informar casos de uso indebido o incumplimiento, la publicación de información de

contacto comercial y la custodia de los datos de los clientes. Siguiente diapositiva, por favor.

Ahora bien, ¿por qué estamos hablando de este tema? ¿Por qué es esto importante? Si nos retrotraemos al 2011 vemos que la Junta Directiva de la ICANN remarcó la urgencia de tratar esta cuestión de los servicios de privacidad y representación porque aumentaría la protección para los registratarios y también reduciría las instancias de uso indebido del DNS con lo cual se está trabajando con mucha persistencia y esto se ha exacerbado durante la pandemia.

En la sesión sobre uso indebido del DNS en el GAC en la ICANN68 se hizo hincapié en que en muchos casos de uso indebido estaban relacionados con los servicios de privacidad y representación, también se habló acerca de reclamos en el marco del GDPR en torno al uso indebido del DNS que tenían que ver con la falta de cumplimiento de dar a conocer información de contacto por parte del proveedor de servicios de privacidad o representación.

Como resultado, los registratarios debían recurrir a terceros para que validaran sus acciones judiciales correspondientes y para poder recibir la información de contacto de la parte maliciosa que estaba realizando el uso indebido del Sistema de Nombres de Dominios, esto tiene que ver también con los recursos pendientes y necesarios para obtener la información de contacto para seguir adelante con su reclamo.

Entonces tenemos que proteger a los registratarios para disminuir el uso indebido del DNS y también los reclamos en el marco de la UDRP.

Ahora vemos qué sucedió con respecto a la solicitud formulada por la Junta Directiva de la ICANN a la GNSO.

Aquí vemos un pantallazo general del PDP de la GNSO, une vez aprobado el RAA del 2013 por parte de la Junta Directiva de la ICANN, la GNSO comenzó este PDP, se adoptaron las recomendaciones de políticas por parte del consejo de la GNSO en enero del 2016 y luego fueron aprobadas por la Junta Directiva en agosto de 2018. Posteriormente la Junta Directiva impartió instrucciones para que se implementara la recomendación.

Con respecto a nuevo programa de acreditación, vemos que tiene muchos más matices en cuanto a los requisitos y a la especificación que ya analizamos. Queda claro que en este programa se abordan las cuestiones que hemos tratado en relación con los servicios de privacidad y representación, por ejemplo, tenemos un marco específico para responder a las autoridades de cumplimiento de la ley o a los titulares de propiedad intelectual.

También hay requisitos estándares para que los proveedores de estos servicios se comuniquen con terceros en cuanto a lo que tiene que ver con los servicios de privacidad y representación que les brindan a sus clientes. Pido disculpas porque estoy hablando muy rápido, disculpen.

Entonces este nuevo programa tiene por objetivo abordar las cuestiones planteadas en esta especificación y brindar una mayor transparencia y un marco más razonable para la acreditación de estos servicios.

Como les mencioné, después de que el consejo de la GNSO adoptara las recomendaciones de los grupos de trabajo que fueran aprobadas por la Junta Directiva de la ICANN, las mismas fueron enviadas a la organización de la ICANN para su implementación.

Se espera que un nuevo programa de acreditación reemplace a las especificaciones contenidas en el RAA, sin embargo, actualmente se ha detenido o suspendido la implementación de este programa, esto se debe a que la ICANN está tratando de cumplir con las normas de protección de datos de la Unión Europea.

En julio de 2018 después de la decisión de la Junta Directiva de la ICANN de adoptar la especificación para los datos de registración de los gTLD, la GNSO comenzó un EPDP. Este fue el primer proceso expeditivo de desarrollo de políticas en la historia de la ICANN.

Posteriormente el consejo de la GNSO adoptó el primer informe de este grupo de trabajo de la primera etapa de este EPDP y 27 de 29 de las recomendaciones contenidas en este informe fueron aprobadas por la Junta Directiva de la ICANN, sin embargo, en la recomendación 27 de la etapa uno, quedó claro que teniendo en cuenta estos nuevos acontecimientos en torno al GDPR y a las prácticas que está implementado la ICANN.

Sería necesario contemplar todas las prácticas pertinentes que guardan relación con datos de registración sin carácter público y por eso este programa se encuentra momentáneamente suspendido, estando pendiente la revisión y los comentarios de la comunidad.

Este programa de acreditación, sus recomendaciones y el EPDP persiguen el mismo objetivo, es decir, terminar un mecanismo legítimo para acceder a los datos de registración sin carácter público. Una vez que se reanude la tarea de implementación, esperamos que se soliciten los comentarios de la comunidad sobre los documentos que se redacten posteriormente.

Los comentarios de la comunidad se solicitarán sobre la política de acreditación de proveedores de servicios de privacidad y representación, también sobre el acuerdo correspondiente, sobre las políticas y los procedimientos de acreditación.

Entonces vemos que esta cuestión de la acreditación de los servicios de privacidad y representación es muy importante en los procesos de políticas de la ICANN, pero también entra en juego el cumplimiento del GDPR por eso se ha suspendido la tarea de implementación, la idea es armonizar todos los componentes de esta situación, todas las piezas de este rompecabezas.

De todas maneras, este programa tiene muchos más matices que los requisitos de las especificaciones, como les dije, esta situación de uso indebido a través de estos servicios se ha exacerbado durante la pandemia, espero que esta especificación y todo este trabajo siga avanzando para dar respuesta a todas estas cuestiones que les he planteado. Muchas gracias y espero aprender a cerca de este tema.

DEBORAH ESCALERA: Parece que hay una pregunta en el chat. Dice: "¿Podría explicar, por favor, el tema de la custodia de datos, en el contexto del tema en debate?"

MERI BAGHDASARYAN: Sí, es un tema muy extenso, así que, quizás puedo escribir mi respuesta si desean avanzar con el debate, pero en síntesis tiene que ver con la forma que los servicios de privacidad y representación encaran las solicitudes de las autoridades de cumplimiento de la ley y obtenedores de IP, de cómo mantienen ese proceso y los datos que poseen los servicios. Esa sería una respuesta acotada, pero voy a dar una explicación más detallada por escrito.

DEBORAH ESCALERA: Muchas gracias. ¿Hay alguna otra pregunta para Meri? Bueno, vamos a seguir mirando el chat. Muchas gracias, muy bien hecho. Entonces vamos a seguir adelante al siguiente orador que es Sai Chandrasekaran. Tiene la palabra.

SAI CHANDRASEKARAN: Muchas gracias, Deborah y Siranush. Siranush, ¿va a compartir la pantalla? Denle un minutito por favor, para subir las diapositivas.

DEBORAH ESCALERA: Quizás haya alguna dificultad técnica, pero lo vamos a lograr. Allí esta.

SAI CHANDRASEKARAN: Gracias, Deborah y Siranush. Estoy muy interesado sobre mi investigación, es sobre la moderación de contenido, vamos a hablar de los desafíos presentados, la lista de privacidad de moderación de contenido y cómo podemos reservar ese tema.

DEBORAH ESCALERA: Recuerde, Sai, hablar lentamente y claramente.

SAI CHANDRASEKARAN: Sí, Deborah. Voy a contarles un poco brevemente, soy graduado de ciberseguridad de la universidad de indiana y vengo trabajando en la investigación de algunos temas como gobernanza, incluido moderación de contenido, así que, estoy muy entusiasmado de contar las novedades sobre este tema. Siguiente diapositiva, por favor.

Para la mayoría de ustedes, los que están escuchando las noticias o las redes, se habrán encontrado el tema de la moderación de contenido, habrán visto gobiernos tratando de ver el tema de la información incorrecta, especialmente en tiempos de pandemia, hay temas de uso indebido, hay investigadores que están tratando de lograr algún tipo de norma por el tema de la moderación de contenido y también esto parece afectar la libertad de prensa, de habla y el tema de la privacidad.

He presentado una línea de tiempo de moderación de contenido, definitivamente quiero mencionar alguno de estos puntos para darles el contexto de por qué este tema es relevante, este es un tema sumamente complejo desde hace unos meses, tuvimos una defensa abierta del cirujano general de los Estados Unidos sobre este tema por

el tema de la información errónea en cuanto a salud, la responsabilidad civil y moral.

Después las redes sociales trataban de detectar la información errónea, una cosa que tenemos que comprender es que no es un tema localizado en los Estados Unidos, sino un tema global, recientemente en india se van a aprobar una serie de leyes para que los proveedores de las redes moderen el contendido y esto encontró una resistencia importante de WhatsApp que ya había presentado una demanda en respuesta a la nueva normativa.

Recientemente hace unas semanas hubo novedades de Facebook, dieron un testimonio respecto de las prácticas de optimización de contenido y sus efectos en la sociedad. Si uno le pregunta a cualquier persona que está en el área de seguridad y privacidad, le dirán que la mejor manera de comprender el problema es hacer una evaluación de riesgo respecto de la privacidad y la moderación de contenido, de la taxonomía y las normas de la industria.

Tenemos aquí de pronto, información que se intercambia a algún mensaje encriptado, por ejemplo, de WhatsApp. Como usuario tengo algunas expectativas de privacidad y confidencialidad respecto al mensaje intercambiado, pero supongamos que tengo un algoritmo que utilizo para ver si los mensajes son dañinos y lo expongo al mensaje.

En ese caso, hay una infracción de la privacidad y la confidencialidad, pero cuando se desarrolla algo nuevo, una nueva capacidad no solo hay que pensar en cómo utilizarla, sino cómo se puede hacer un uso indebido de ella teniendo en consideración que este tipo de tecnología

especialmente la encriptación se puede utilizar por actores del gobierno maliciosos, se puede promover una vigilancia para ver si se toma información no debida.

DEBORAH ESCALERA: ¿Puede hablar un poco más lento, por favor, Sai?

SAI CHANDRASEKARAN: Otra cosa que les quiero comentar es que a veces la divulgación de información puede ser irreversible sobre temas sexuales, uso de sustancias que queda expuesto al dominio público. No tengo medidas de protegerme del sufrimiento emocional grave y el efecto de esa divulgación.

Si también se libera información financiera es distinto, por ejemplo, puede bloquear una tarjeta de crédito o puede tomar alguna medida, pero en estos casos ya está expuesta la información, por cual no puede tomar algunas medidas.

DEBORAH ESCALERA: Por favor, Sai, ¿podría bajar la velocidad? Disculpe que lo interrumpa, respire profundo y trate de hablar más lento.

SAI CHANDRASEKARAN: Disculpas, Deborah. En mi diapositiva anterior hablaba de las amenazas de privacidad por la moderación de contenido, pero hay otros argumentos presentados también por el otro lado, por ejemplo,

supongamos que algunas personas digan que la moderación de contenido se puede utilizar para evitar la violencia y, finalmente, para prevenir la muerte en caso de violencia.

Y podemos adoptad un contenido de privacidad respecto de moderación de contenido, uno es técnico organizaciones técnicas, instituciones de educación, pueden colaborar con técnicas de encriptamiento seguras que verifiquen, detecten la información errónea que no afecte la privacidad y la confidencialidad, por ejemplo, en este caso podemos utilizar una técnica criptográfica segura multiparte que haga barridos y los compare con la imagen objetivo para verificar que la imagen no sea la misma, eso se informaría al prestador del servicio llegado el caso.

Otro pilar importante del que les quiero hablar es el proceso, esto es un modelo de guardia de información, de watchdog, no se divulga información a los proveedores de servicios para tener un modelo de confianza y actuar en caso de información errónea.

CRISTINA RODRÍGUEZ: Disculpas que la vuelvo a interrumpir. Es muy difícil para el intérprete poder seguirlo, le rogamos por favor que hable más lentamente, entendemos su entusiasmo, pero le rogamos que hable más lento.

SAI CHANDRASEKARAN: Disculpa, Cristina. El último pilar del que les quiero hablar es el principio que quiere establecer algún tipo de confianza entre las partes interesadas, tomemos un ejemplo, si soy proveedor de servicios

activamente moderando contenido, tengo que verificar que haya transparencia en los algoritmos para tener la confianza de todas las partes interesadas.

Esto me lleva a mi última diapositiva, considero que la moderación de contenido como tema es muy similar al cambio climático, tenemos distintos países que quieren encarar el tema, prácticamente todos los países quieren hacerlo, pero tienen distintas bases y enfoques.

La mayoría de estas cosas no van de la mano entre sí, quisiera alentarlos con que utilicen el enfoque de múltiples partes interesadas para la moderación de contenido, divulgando o denunciando la información falsa a los proveedores de servicio con la ayuda del conocimiento, la ayuda de educadores e instituciones.

Las plataformas tienen que ver los déficits de información y priorizar su detención, ver a los depredadores, los delincuentes residentes y las partes interesadas claves tienen que trabajar con los gobiernos de todo el mundo, también con organizaciones sin fines de lucro y las privadas hacia un terreno común para lograr medidas jurídicas respecto de la moderación del contenido. Gracias por su tiempo y paciencia, si tienen preguntas, por favor, adelante.

DEBORAH ESCALERA: Muchas gracias, Sai. ¿Alguna pregunta para Sai? No veo nada en el chat, hubo cierta dificultad con esta presentación, pero se está grabando la sesión, así que, van a poder reiterarlas a posteriori si no han podido verla esta vez. Vamos a pasar al siguiente orador.

Hay una mano levantada. Enoch, ¿tiene alguna pregunta? Por favor adelante.

ENOCH NIKINGBOUNG DUUT: Una pregunta rápida respecto del contenido, es un tema de dos caras, respecto de la libertad de expresión y todo este tema, también hay contenido que no debiera estar en el dominio público entonces, ¿cómo se logra una solución intermedia para mitigar el riesgo y permitir que la gente a la vez pueda decir las cosas de esta manera sin afectar la libertad de expresión? Si consideramos las redes sociales, ¿cómo podemos tener independencia de los reguladores?

SAI CHANDRASEKARAN: Lamentablemente en este momento no tenemos una manera de brindar el equilibrio entre la información errónea y la libertad de expresión, pero una cosa viendo las noticias recientemente, habrán escuchado del tema de Apple, se quiere hacer un barrido del lado de los usuarios para proteger los mensajes y también estaba el tema del abuso de menores. Esto también tiene que ver con la seguridad y la privacidad.

Como sugerí en mi presentación, tenemos la técnica multipartes seguras, podemos pasar esas imágenes, compararlas con las de abuso, si coincide se le informa al prestador de servicios y no se transfiere. Espero haber respondido su pregunta.

ENOCH NIKINGBOUNG DUUT: Muchas gracias. Lo puede poner en el chat, por favor.

SAI CHANDRASEKARAN: Sí, sin duda.

DEBORAH ESCALERA: Muchas gracias por la pregunta. ¿Hay alguna otra pregunta para Sai? Pasamos a Kady Hammer.

KADY HAMMER: ¿Me escucha, Deborah?

DEBORAH ESCALERA: Sí, la escucho bien.

KADY HAMMER: Es un poco confuso porque me veo a mí misma. Soy Kady Hammer, soy estudiante de derecho de la Universidad de American en Washington D.C. Vamos a hablar sobre el control de acceso, los protocolos o mecanismos de seguridad para permiso de acceso. Siguiente, por favor.

En primer lugar, quiero revisar brevemente cómo llegamos aquí y cómo estamos hablando de este tema de control de acceso y los protocolos, no soy tecnóloga, sino estudiante de derecho, así que, me ha llevado bastante tiempo comprender cómo funciona la infraestructura de internet, pero estoy segura que usted desconoce que esta fue creada primeramente con fines de comunicación, la seguridad no era algo necesario, ni las primeras preocupaciones cuando desarrollamos la infraestructura de internet.

Luego empezó a ser una preocupación creciente en el mundo actual, considerando la existencia de amenazas cibernéticas y ataques. En 1989 se desarrolló el protocolo BGP, entre otros, es el protocolo de control de acceso de frontera y de ahora en adelante lo llamaremos BGP.

Se basa en redes individuales que comparten información constantemente sobre sí misma, las direcciones IP, que es la manera en que el internet sigue creciendo en la red vasta en la que se ha convertido. Algo que tenemos que conocer es que BGP no requiere autenticación ni direcciones IP para el sistema autónomo, sino que opera en un marco de confianza, quizás lo conozcan como sistema de honor donde las redes confían a las otras redes en que son buenas, que son buenos actores.

Entonces, en general, BGP es sencilla, brinda información y soluciones para los protocolos de enrutamiento y una estructura versátil para dudar décadas. Acá tenemos una revisión, un diagrama y una lista de los distintos protocolos, como les decía, el BGP es uno entre otros protocolos en uso, el objetivo primario es el enrutamiento de tráfico de internet entre dispositivos, sistemas y como les decía antes, no garantiza la seguridad en la entrega de la información.

Esto, nuevamente, vuelve al marco de confianza en el sistema del que hablábamos. Como verán, hay una lista considerable de tipos de protocolos, no se los voy a leer ahora, pero en el grafico a la derecha de la pantalla vemos una reseña de cómo BGP u otro protocolo, el EGP, cómo funciona, cómo se comunican entre sí, también con los sistemas

autónomos que voy a explicar un momento y una reseña visual en caso de que les interese. Siguiente, por favor.

Para llegar un poco más a los puntos específicos del protocolo de acceso de frontera, es un protocolo de enrutamiento (BGP y un vector de ruta) que está entre los sistemas autónomos de internet, en lugar de hacer un seguimiento de la topología completa, se basa en la información de router o enrutadores vecinos a esos sistemas y después elige el camino más corto para incluirlo en una tabla de enrutamiento.

Cada router entonces anuncia la ruta a los vecinos, si la política lo permite intercambia información. Cuando estamos hablando de los sistemas autónomos o las redes que utiliza BGP para comunicarse, quizás nos escuchen hablar del sistema autónomo que incluye un sistema singular, sin embargo, los sistemas autónomos a veces incluyen toda una organización con múltiples routers o enrutadores y dispositivos, ese término se utiliza para hablar de manera más general de este tema.

Los números de sistema autónomos de internet son asignados por el proveedor que es la manera en que el usuario final se conecta o a veces lo asigna un registro, al fin y al cabo BGP elige el camino más corto para transmitir es información y la razón por la cual es tan importante este protocolo es que, porque hacer el seguimiento de todo el sistema de internet es per se un objetivo, se trabaja para el intercambio de información de manera que esta llegará al lugar al que queremos ir con mayor rapidez.

Esto es importante por la manera en que funciona BGP, los sistemas pueden unirse y atacar a un solo lugar, puede haber un ataque a todo un sistema autónomo que puede incluir organizaciones, empresas y demás. Siguiente, por favor.

Lo que les quiero comentar en este momento son los temas de problemas de seguridad, que surgen en los protocolos, más específicamente… Muchas gracias por la explicación que están enviando en el chat. Específicamente quiero hablar de los temas de seguridad que van surgiendo en el protocolo de frontera de entrada, aunque los temas de seguridad no son específicos de BGP, sino de varios protocolos.

Uno de los temas importantes es el error humano, por ejemplo, lo que pasó con Facebook, que a pesar de que no fue un tema de BGP uno lo puede considerar como un ejemplo de lo que puede suceder. El error humano entonces puede crear configuraciones erróneas accidentales que en una organización o en un sistema de internet autónomo puede hacerlo caer, lo que se pierde en internet, pero fundamentalmente quiero hablar de la interferencia maliciosa.

Todos los protocolos pueden ser objetivos de los ataques, ya sea spoofing, secuestro de sesión, ataques de denegación de servicios y de distintas maneras, los actores pueden introducir información incorrecta en las tablas de BGP. Un ejemplo de esto sería porque BGP se confía en las redes vecinas y puede ser un actor malicioso que introduzca información incorrecta, en lugar de un sitio o alguna otra variable.

Como confían entre sí los BGP no hay un mecanismo de autenticación puntual que exista en BGP, por lo cual no hay manera de validar hoy por hoy qué es lo que están diciendo los sistemas de red, si la información está validada, si es confiable, si es creíble. Otra cosa es que, la autenticación criptográfica no es algo obligatorio, vamos a hablar del tema en la siguiente diapositiva.

Para explicar este tema les voy a mostrar un caso de estudio, como se da el secuestro de BGP mediante el sistema del DNS de Amazon. En 2018 actores maliciosos utilizaron un ataque de BGP (lo que se llama ataque de intermediario) para re enrutar el tráfico al servicio de rutas 53 de Amazon con un centro de datos de IBX de Chicago permitiendo que diversos actores interceptaran el tráfico globalmente, especialmente apuntaron a MyEtherWallet.com; que es una plataforma de blockchain de Ethereum, lo hicieron redireccionando su tráfico de clientes a su página y robaron la información del cliente.

¿Y cómo lo hicieron? El tráfico de internet fue redireccionada a un servidor en Rusia que pretendió ser la página que utilizaba el certificado falso y robaron las criptomonedas de los clientes. El ataque requirió acceso a los enrutadores de BGP de los proveedores de servicios de internet requiriendo recursos de computación significativos, es algo que vale la pena saber porque tenían que manejar una cantidad significativa de tráfico del DNS que ingresaba al servidor.

Entonces, ¿por qué es importante esto? Este ataque resalta las preocupaciones existentes de seguridad, tanto en BGP como en el DNS y también en distintos protocolos de enrutamiento, y este es el ataque

más importante conocido de estas escalas que muestran la fragilidad de BGP y DNS que es un tema que van a hablar otros oradores. En la parte de abajo tenemos una infografía con una reseña de cómo se ha dado esto.

Entonces, ¿cómo hacer la protección del acceso? En general, hay algunas cosas que necesitamos cuando queremos considerar cómo hacer que los protocolos de enrutamiento sean más seguros, especialmente los BGP. En general, necesitamos software de routers o enrutadores que implementen IPsec, también infraestructura de clave pública, firmas digitales, determinar también el papel de los registros regionales, la certificación de la autoridad y de las responsabilidades de la persona que está a cargo para los prefijos de dirección, la asignación y su ubicación.

Un componente importante que implica inversiones importantes en la infraestructura de hardware, incluidos los routers, ISP y suscriptores para determinar el papel de los ISP en el manejo y certificación de esta información, por supuesto, actualizar el hardware físico implica un costo de inversión importante, así que tenemos que pensar de manera más estratégica y ver cómo mejorar el BGP hacia el futuro, especialmente teniendo un enfoque con la mente en seguridad logrando más reactividad y proactividad, y utilizando esto como criterio.

¿Cómo determinamos si el enrutador, la red o cualquier entidad es seguro o está validado, o es una fuente confiable? ¿Qué criterios vamos a utilizar para permitir o no que las redes interactúen y cooperen en el

ecosistema del internet? Entonces las tres soluciones que les muestro en pantalla ninguna es nueva, provienen de la creación de BGP desde principios de los 90', entonces hay soluciones existentes sobre cómo podemos proteger y asegurar los protocolos.

Específicamente una opción es el protocolo seguro de frontera de entrada o S-BGP, este mecanismo permite autenticar la dirección de IP o bloques de dirección IP, también puede haber aun atributo de camino transitivo para verificar las firmas digitales que autentiquen la información del enrutador por donde viaja la información, hay una marca en esa información. También se puede utilizar IPsec, que se utiliza para brindar datos que autentican la información antes de que se la intercambie a través de BGP.

Otra solución sería BGP de origen seguro, que tiene que ver con el tercer punto de la primera solución. Antes del intercambio de la información cada entidad tiene que certificar o ser certificada, o sea que se validen sus credenciales.

Cada certificado de autorización debe ser validado y esto tiene que ver con el papel de los registros, cuáles son los planes de los proveedores de servicios, la información contenida en el certificado de la política debe estar correlacionada con la base de datos en la que está alojado y esto certifica que tenga un papel cada una de las partes interesadas en la certificación de la base de datos y de la seguridad de la misma.

Otra solución se llama transporte escalable de BGP y esto reemplaza al TCP, otro protocolo de enrutamiento, y con un protocolo de transporte del propietario. Esta solución en particular puede no ser la más factible,

dado que lo estaría privatizando, pero si utilizamos una técnica que se llama flooding o inundación para transportar estos datos solamente a los vecinos inmediatos, en lugar de que pase por todos los enrutadores y por toda la red. Siguiente diapositiva, por favor.

Obviamente hay desafíos en el BGP seguro, por eso las soluciones existentes todavía no están listas y por eso estamos teniendo este debate, la preocupación inicial es el costo propiamente dicho de estas soluciones en términos de la infraestructura personal y coordinación, asignación de responsabilidades. Estos son los componentes claves de las primeras dos soluciones y ya hablamos de la última solución, pero requiere financiación importante.

Si uno cambia todo un protocolo puede no funcionar y sería propietario, así que, no es gratuito y puede no ser accesible, y al fin y al cabo la autoridad o el mecanismo de control estaría en manos del propietario. Adicionalmente, en general, uno de los desafíos más importantes es la complacencia o la falta de urgencia hasta que llega la crisis y golpea.

Ya hablé del enfoque reaccionario, la mayoría de las partes interesadas y yo hemos tomado esto ante la seguridad, en lugar de actuar de manera proactiva con las soluciones, por supuesto, dada la longevidad del internet y el tiempo que hace que exista ser proactivo es realmente difícil.

Otra cosa es que, este problema se considera como algo menor dada la pequeña escala en la que se dio. En cuanto a los ataques, no se conocía tanto el tamaño de este, se pensaba que solo era una empresa, pero imagínense los ataques en la dimensión que pueden tener y los

problemas que pueden causar. BGP es uno de los focos más nuevos de los ataques maliciosos.

DEBORAH ESCALERA: Se ha excedido mucho de los diez minutos, no le había dicho nada, pero…

KADY HAMMER: Estuve tratando de hablar lentamente.

DEBORAH ESCALERA: Está haciéndolo muy bien, simplemente tengamos en cuenta que tenemos dos oradores adicionales.

KADY HAMMER: Ya hablé prácticamente de todo lo que está acá, por qué es importante esto… Perdón, hay una intrusión. Una de las cosas que quería comentar es que, aunque esto es una preocupación seria, tenemos modelos existentes y podemos pensar en cómo cambiar el enfoque para asegurar el BGP, por ejemplo, podemos considerar HTTP como pasó a HTTPS que podría resolver este problema. Siguiente, por favor.

Eso es todo, muchas gracias a todos por su tiempo y les pido disculpas por el tiempo que tomé, pero no quise hablar rápido.

DEBORAH ESCALERA: Muy buena presentación, realmente muy interesante. Hubo debates en la sala del chat durante su presentación, claramente un muy buen tema, un tema muy interesante para todos los participantes. Quisiera saber si alguien tiene alguna pregunta más para Kady…

Muy bien, Kady, felicitaciones, una excelente presentación y muy bien estructurada también. Si no hay más preguntas, les repito que pueden enviarlas incluso después de esta sesión, así que, dicho esto, vamos a pasar a Scott Kim quien tomará la palabra a la brevedad. Un momento por favor, aguarde a que podamos ver su presentación en pantalla.

SCOTT KIM: Hola a todos, estoy haciendo mis estudios de posgrado, trabajo en seguridad de la información, así que tengo que recopilar información sobre este tema y compartirlas con las partes interesadas correspondientes. Hoy hablaré acerca de la herramienta de búsqueda de la ICANN para ver los indicadores de una posible actividad maliciosa, les voy a hablar acerca del APT41 y de qué se trata, les voy a presentar algunos casos prácticos y, por último, les presentaré algunas recomendaciones.

El APT41 no es muy conocido por el público en general, pero sí lo es para la comunidad de seguridad de la información, tiene distintos nombres según cada empresa, se le conoce como Wicked Panda, también Blackfly, entre otros nombres, pero básicamente se trata de un grupo patrocinado por el estado chino y que se dedica a llevar adelante actos de espionaje que se remontan a 2012.

Este grupo, como les dije, está patrocinado por el estado chino y ataca a los sectores de telecomunicaciones, de videojuegos, entre otros. En septiembre el departamento de justicia de los Estados Unidos acusó formalmente a destinos actores relacionados con este grupo, hace poco el equipo de investigación e inteligencia de BlackBerry descubrió una campaña de malware llevada a cabo justamente por este grupo utilizando un perfil específico para ocultar su tráfico en la red.

Asimismo, este grupo utiliza otras herramientas para perpetrar sus ataques, lo que hicieron fue ver los distintos indicadores de una posible actividad maliciosa vinculadas a otras firmas dedicadas a la seguridad informática. Como vemos aquí, en estos dominios lo que tratan de hacer es ocultar sus dominios de Microsoft y lo que tratan de hacer es simular que son esos dominios, los vemos en los últimos dominios que están en esta tabla.

Ahora bien, tenemos una herramienta de búsqueda de datos de registración en la ICANN que nos permite ver la información de los nombres de dominios y de los recursos numéricos, los usuarios tienen que ir a WHOIS.ICANN.ORG e ingresar un nombre de dominio. Por ejemplo, yo elegí en este caso el nombre que vemos en la pantalla, ese nombre de dominio, y cuando ingresé ese nombre recibí esta información por parte del sistema.

Vemos algunas fuentes abiertas de información que nos revelan ciertas conexiones y ciertas relaciones que son pertinentes para los investigadores. Este nombre de dominio pertenece a la dirección de IP que vemos en pantalla y que figuraba en la campaña de malware de la

cual les hable, entonces se pudo hacer esta relación y se pudo también ubicar estas direcciones IP, ver para qué se las estaba utilizando y cuál era la infraestructura que podían penetrar.

Como vemos, estos dominios solamente tienen un año de duración y sus certificados, y esta es una alerta para quienes trabajamos en seguridad porque, por lo general, estos actores utilizan estos dominios y hacen este estacionamiento o parking de dominios, lo reservan, para estas actividades maliciosas con lo cual podemos realmente obtener mucha información.

Como conclusión quiero decirles que, el equipo de BlackBerry pudo recopilar toda esta información estableciendo relaciones entre distintos blogs y distintas publicaciones de expertos en seguridad, con lo cual quiero incentivarlos a compartir información porque justamente compartir este tipo de información nos permite tener un panorama completo de estos actores maliciosos, de sus actividades en curso. Así que, dicho esto, les agradezco su atención y estaré atento a sus preguntas. Muchas gracias.

DEBORAH ESCALERA: Muchas gracias, Scott. ¿Tenemos alguna pregunta para Scott? Veo que no.

Muy bien, muy buena presentación y también vamos muy bien con el tiempo, tenemos a nuestro último orador, James. James, una vez que vea la presentación en pantalla puede comenzar.

JAMES PAEK: Muchas gracias, Deborah. Soy James Paek, voy a hablar acerca del autoritarismo digital y vamos a ver qué es.

Muchos de ustedes se preguntarán justamente qué es el autoritarismo digital, básicamente es el uso de internet y sus tecnologías digitales afines por parte de líderes que tienen tendencias autoritarias para disminuir la confianza en las instituciones públicas, incrementar el control político y social, y también socavar las libertades civiles.

Entonces todo tipo de invasión a la privacidad, a la libertad, todo aquello que damos por sentado y que no tenemos presente que los gobiernos pueden controlar, bueno, constituye este autoritarismo digital y es lo que hace un gobierno autoritario. ¿Cuáles son los motivos? Pueden ser una inestabilidad económica, política, social, también lograr una mayor legitimidad o autonomía, controlar y manipular la opinión pública, y causar temor, miedo, es decir, que haya miedo entre la gente acerca de qué le depara el futuro.

Hay mucha incertidumbre, por supuesto, debido a la pandemia y a todos los acontecimientos que estamos viviendo, y creo que por eso vemos cada vez una mayor falta de confianza por parte del público, hay un cierto descontento que a veces pasa inadvertido y también, por supuesto, entre las causas de este autoritarismo digital está el populismo y el nacionalismo. Esto es cada vez más parte de la realidad de una gran cantidad de países.

Bien, creo que se están viendo tendencias, vamos a ver, por ejemplo, qué pasa en China. Definitivamente hay una mayor vigilancia, hay video vigilancia, hay cámaras en cada esquina de cada ciudad, vemos que hay

circuitos cerrados de televisión y sus cámaras correspondientes que potencialmente pueden censurar cada uno de nuestros comportamientos o lo que se considere un comportamiento social inapropiado.

Estas son las cuestiones o las situaciones que estamos viendo cada vez más, lo vemos en Hong Kong, donde el gobierno de China está tratando de reprimir a los ciudadanos, también lo vemos con respecto a la reciente aprobación de seguridad de la información. Y quiero decirles que esto proviene de una revolución cultural que se remonta a la década de los 50', donde se empezó a tener este tipo de revolución de control para controlar a las personas.

Definitivamente estamos viendo también el sistema de crédito social y quiero hablarles en más detalles. Ustedes se preguntarán qué es este sistema, bueno, este sistema nos da una puntuación por nuestro comportamiento social, califica nuestro comportamiento social, lo hace el gobierno y lo hace el partido comunista chino que decide qué es o no es un buen comportamiento social, es decir, que las personas pueden ser castigadas, o bien tener privilegios o perder esos privilegios, tales como poder viajar a otro país.

Vemos que esto sucedió previamente en Corea del Sur donde el Servicio Nacional de Inteligencia comenzó a hacer una lista negra de personas famosas en Corea porque eran demasiado liberales o tenían tendencias consideradas de izquierda, también empezaron a intimidar a los usuarios de internet y vemos una mayor vigilancia y censura de aquellas

personas que hacen o realizan actividades consideradas contrarias al estado.

En otros países, por ejemplo, vemos lo que sucede en Bielorrusia, en Rusia, en Francia donde estamos viendo mucha vigilancia, mucha censura, vemos el fraude electoral de Alexander Lukashenko, vemos la intervención en los comicios en Rusia y cómo interfieren los comicios de otros países. Por ejemplo, vimos cómo se hizo este fraude electoral y creo que esto genera una inquietud en lo que respecta a la credibilidad de los comicios y acerca del sistema electoral.

Potencialmente esto puede tener una influencia en el comportamiento social, lo vemos también en Francia donde hay una ley de seguridad nacional que le otorga a la facultad de vigilancia, al gobierno francés, para monitorear a las personas que, por ejemplo, realizan acciones contrarias a las actividades de cumplimiento de la ley y les pueden iniciar acciones penales.

Ahora bien, ¿qué se puede considerar autoritarismo digital? Definitivamente la vigilancia y la censura lo son, también la represión de la población, la desinformación y la información errónea, la brutalidad policial y la manipulación de los comicios.

Por supuesto, vemos esto a gran escala y vemos el reconocimiento facial, esto también entra en la categoría de autoritarismo digital y no pensamos nunca en este tema del autoritarismo digital que incluye el espionaje, las noticias falsas, los videos falsos en los cuales, por ejemplo, se manipula una foto o un video original para transmitir otro mensaje o que tenga otro formato.

Vemos que hay muchos usuarios de internet y ciudadanos que no pueden identificar el origen de una fuente de información y esto tiene un gran impacto en cómo la sociedad interpreta la información.

¿Cuáles son las amenazas que representa el autoritarismo digital? Bueno, básicamente socava la democracia, incluidas las instituciones, también puede causar un disturbio social, político, cultural y económica, causa violaciones a los derechos humanos y a las libertades civiles, también podría incrementar el acoso sexual y otros tipos de conductas nocivas para la humanidad.

Entonces, vemos otras amenazas que constituyen el autoritarismo digital y esto puede tener consecuencias no deseadas a corto plazo, aquí vemos una publicación reciente, esto lo publica la unidad de inteligencia de la publicación The Economist, es un índice de las democracias.

A escala mundial vemos que durante la pandemia muchos países y gobiernos en el mundo están aplicando herramientas y poniendo excusas acerca de cómo proceder durante la pandemia y también cómo podemos volver a las autoridades democráticas en el orden público.

Vemos que hay regímenes híbridos o democracias fallidas, o deficientes, y vemos que hay democracias que están comenzando a deteriorarse a la vista de acontecimientos recientes. Por otra parte, en la otra parte del mundo vemos que hay una gran cantidad de países con democracias deterioradas, lo cual es preocupante y alarmante porque si no hacemos nada para contrarrestar este autoritarismo digital los

gobiernos continuarán utilizando estas herramientas para intervenir en nuestra vida diaria, lo cual va en detrimento de nuestra sociedad.

No queremos llegar al totalitarismo de Corea del Norte, ni tampoco queremos llegar a un extremo con respecto a las cámaras de vigilancia en China, por ejemplo. Siguiente diapositiva, por favor.

Ustedes se preguntarán, ¿cuáles son las soluciones? ¿Cómo podemos contrarrestar el autoritarismo digital? Yo diría que tenemos que promover la democracia y los derechos humanos en casa, esa es nuestra prioridad. Estados Unidos debe predicar con el ejemplo, debe ser un ejemplo a seguir, si no podemos gestionar nuestras propias cuestiones en casa difícilmente podremos ser un ejemplo para el resto del mundo y difícilmente podremos decirles a otros países que tienen que ceñirse a nuestros derechos, a nuestro concepto de derechos humanos, etc.

Desafortunadamente si Estados Unidos no puede abordar sus propias cuestiones internas, entonces no podrán liderar con el ejemplo o ser un ejemplo para los demás países del mundo. Si uno es miembro de una misión diplomática y representa a los Estados Unidos, la gente tiene una percepción de nuestro rol, de nuestra función y de la clase de persona que somos en ese rol.

Entonces tenemos que aumentar la confianza en las instituciones públicas y en los gobiernos, asimismo, podemos fortalecer a la Sociedad Civil para evitar un disturbio social o político, podemos mitigar las tensiones en Estados Unidos. Esto es algo que personalmente no me gusta, debemos solucionar estos problemas, sé

que esto es algo muy difícil; sino lo más difícil de hacer, pero tenemos que asegurarnos de tener un comportamiento que nos represente para poder fortalecer la libertad en internet.

Esto incluye diversas medidas, acciones, incrementar las coaliciones multilaterales, tenemos el diálogo sobre seguridad cuadrilateral, la asociación Five Eyes. Probablemente se arme un equivalente a la OTAN para la región asiática, no lo sabemos a ciencia cierta, pero es lo que puede suceder y también necesitamos definitivamente invertir en el capital humano.

Sé definitivamente que China está incrementando su inversión en el capital humano para tener profesionales de ciberseguridad y garantizar la continuidad de este talento, sin embargo, en Estados Unidos vemos que nos hace falta personal capacitado en ciberseguridad. Así que, necesitamos talento proveniente de los campos de la matemática, de la tecnología, de la cibernética, de la ingeniería, de lo contrario, tendremos que enfrentarnos a las consecuencias.

Tenemos que invertir en el desarrollo social también, asimismo, debemos fortalecer distintas tecnologías, fortalecer el cifrado y definitivamente tenemos que avanzare hacia el futuro, asegurarnos de contratar a los mejores profesionales, de tener el mejor talento para poder enfrentar cualquier tipo de crisis, como la pandemia en este momento y también asegurarnos de seguir siendo los líderes mundiales en el campo de la tecnología.

Aquí tienen las referencias, las citas y las fuentes bibliográficas que he consultado. Con esto finaliza mi presentación, les agradezco su

atención, gracias por su tiempo, por escucharme, muchísimas gracias. Si tienen alguna pregunta, por favor, con todo gusto se las voy a responder, gracias.

DEBORAH ESCALERA: Muchas gracias. Hay una pregunta en el chat, una pregunta de Brian, y creo que es una pregunta para todos los oradores, pero se la voy a hacer a usted.

"¿Qué piensa acerca de la libertad de expresión en internet durante la pandemia de COVID-19?"

JAMES PAEK: Brian, muchas gracias por su pregunta. No estoy seguro de comprender su pregunta, si pudiera ser más exacto por favor.

DEBORAH ESCALERA: Brian, ¿puede aclarar su pregunta por favor?

JAMES PAEK: ¿Qué hago? ¿Me baso en mi propia interpretación para responder o desea que aguarde a que aclare la pregunta?

DEBORAH ESCALERA: Adelante, por favor, responda según usted ha interpretado la pregunta. Tiene aproximadamente diez minutos.

JAMES PAEK: Brian, esta pregunta; según como se interprete, puede tener distintos significados. Ahora bien, pensando en la libertad de expresión de las personas en internet durante la pandemia de COVID-19, bueno, vemos; según mi presentación, que el autoritarismo está aumentando. Lo vemos en China, en Rusia, Bielorrusia.

Y bueno, definitivamente no es cierto tampoco que en Estados Unidos tengamos todas las libertades digitales o en internet, lo vimos en un caso que sucedió, el caso de Edward Snowden, vimos como el gobierno recopilaba masivamente datos en pos de la seguridad nacional, después de los ataques del 11 de septiembre.

Ahora bien, estamos viendo cada vez más un comportamiento autoritario que controla a nuestra sociedad y, por lo tanto, se están deteriorando nuestras libertades en internet, por ejemplo, en la región africana recientemente hubo un apagón de internet y no se bien cuáles fueron los países impactados en la región, pero básicamente el gobierno no debería tener la potestad de controlar la libertad de información en internet porque lo que podría pasar es que esto tuviera consecuencias gravísimas.

Por ejemplo, que el gobierno empiece a controlarnos según un algoritmo de datos que posee y según ese algoritmo puede pensar que nuestro comportamiento es peligroso, y el gobierno no tiene que tener el derecho de espiar nuestra conducta o nuestro comportamiento.

Nosotros tenemos el derecho de proteger esta libertad y de asegurarnos de que los gobiernos no se excedan en sus potestades, no tienen por qué intervenir en nuestra vida personal o privada, no queremos ver a

otro gran hermano; como ha sucedido en años anteriores, como se vio en Corea del Norte y China va tras los pasos de Corea del Norte.

Yo definitivamente no quiero ver esa realidad porque realmente eso constituye una invasión de nuestra privacidad, de nuestra vida, de nuestras libertades civiles, de nuestra libertad de expresión que se van a deteriorar a un punto tal que será inaceptable. Veo que hay muchos países que tienen tendencias autoritarias y creo que debemos preservar, proteger nuestra libertad de expresión.

Ahora bien, nosotros damos todo esto por sentado y no sabemos o no queremos, mejor dicho, que los gobiernos autoritarios se apoderen o tomen control del mundo, queremos entonces incrementar la confianza del público en las instituciones, queremos hacer mayores campañas de educación no solo en Estados Unidos, sino en el resto del mundo.

Debemos asegurarnos de escuchar activamente y respetar todas las percepciones, todas las perspectivas y los comportamientos, por eso hablé también de una mayor amabilidad. Esto va mucho más allá del autoritarismo digital, entra en juego el aspecto psicológico, debemos ser abiertos y tolerantes de quienes tienen una opinión distinta de la nuestra. Muchas gracias.

DEBORAH ESCALERA: Muchas gracias, James. Creo que Brian aclaró su pregunta en el chat, le voy a leer el comentario de Brian, pero le voy a pedir que sea breve cuando responda. El dice: “Usted menciona que los gobiernos controlan la libertad de expresión en internet, ¿cree que esto es algo

bueno en un mundo democrático?" Le voy a dar dos minutos para que responda.

JAMES PAEK: Bueno, como dije, tenemos que invertir en capital humano en nuestras personas para que haya una mayor alfabetización digital y tecnológica, de lo contrario, enfrentaremos consecuencias no deseadas. Tenemos que asegurarnos de promover nuestra democracia, primero en casa en nuestro propio país y asegurarnos de que otros países sigan nuestros pasos, y también tengan su democracia propia.

Obviamente la democracia no es lo mejor del mundo, no estoy hablando en contra de la democracia, sino que, definitivamente, lo que quiero decir es que las democracias necesitan una mejora, por eso debemos asegurarnos de que el público confíe en las instituciones. Primero debemos confiar en nosotros mismos, ser más amables unos con otros y respetarnos mutuamente.

DEBORAH ESCALERA: Muchas gracias. Creo que tenemos una pregunta más, le voy a dar un minuto nada más para que responda. Enoch, tome la palabra.

ENOCH NIKINGBOUNG DUUT: Creo que es muy importante tener presente que algunos gobiernos se aprovecharon de la pandemia de COVID-19 y consideraron que les daba derecho a intervenir en las comunicaciones digitales de las personas y

valerse de este motivo para llevar adelante una suerte de persecución tecnológica o intervención tecnológica.

Todos estaban en contra de la desinformación y la información errónea, por supuesto, durante la pandemia, pero hubo leyes que no tenían que ver con la enfermedad o con la pandemia en sí, sino que fueron leyes que se aprobaron aprovechando la situación para impedir o limitar la libertad de expresión de las personas durante la pandemia.

Creo que esto es algo que tenemos que considerar y analizar en profundidad.

DEBORAH ESCALERA: Muchas gracias por su comentario. Dicho esto, entonces vamos a concluir nuestra sesión, quiero agradecerles a todos por participar, gracias a Siranush por compartir la pantalla y pasarnos las presentaciones. Gracias a los oradores, hicieron un excelente trabajo, han presentado temas muy interesantes, gracias a nuestro equipo de reuniones y de apoyo técnico, y a nuestros intérpretes. No podríamos llevar a cabo esta sesión sin ustedes.

Muchas gracias a todos los que se conectaron a esta sesión del programa NextGen durante la reunión ICANN72, es un placer haberlos tenido con nosotros y para los participantes del programa de NextGen bueno, les deseo que disfruten, quizás los acrónimos y todos los términos pueden ser un poco abrumadores, pero tómenselo con calma y disfruten de las sesiones. Muchas gracias a todos por participar, que tengan un excelente resto de su jornada.

[FIN DE LA TRANSCRIPCIÓN]