

partes interesadas

ICANN67 | Foro virtual de la comunidad – Un mundo, ¿un Internet? Ciberseguridad y geopolítica en un entorno de múltiples partes interesadas
Miércoles, 11 de marzo de 2020 – 13:45 a 15:15 CUN

MICHELLE DESMYTER: Bienvenidos a esta sesión. Vamos a comenzar en los próximos minutos. Por favor, si van a tomar la palabra en el día de hoy les pedimos que silencien sus notificaciones de correo electrónico, de Skype o cualquier otro tipo de notificación sonora para no interferir con la labor de las intérpretes. Muchas gracias.

Hola a todos. Bienvenidos a esta sesión. Vamos a comenzar en los próximos minutos. Les agradecemos a todos por su paciencia.

Vamos a comenzar en unos minutos. Muchas gracias por su paciencia.

Joanna, estamos en horario para comenzar la sesión. ¿Desea comenzar o aguardar?

JOANNA KULESZA: Podemos comenzar. Tenemos muchos temas a tratar. Están todos los oradores en la sala así que comencemos, por favor.

MICHELLE DESMYTER: Por supuesto. Vamos a comenzar. Buenos días, buenas tardes y buenas noches a todos. Soy Michelle Desmyter, del personal de la

Nota: El contenido de este documento es producto resultante de la transcripción de un archivo de audio a un archivo de texto. Si bien la transcripción es fiel al audio en su mayor proporción, en algunos casos puede hallarse incompleta o inexacta por falta de fidelidad del audio, como también puede haber sido corregida gramaticalmente para mejorar la calidad y comprensión del texto. Esta transcripción es proporcionada como material adicional al archivo, pero no debe ser considerada como registro autoritativo.

ICANN. Bienvenidos a la reunión virtual ICANN67. En este caso vamos a estar en la sesión “Un Mundo, Una Internet. Cuestiones de geopolítica y ciberseguridad en un entorno de múltiples partes interesadas” a las 18:45 UTC. La sala de Zoom será en idioma inglés en el horario y el programa de actividades de la reunión. Tienen los enlaces para la transmisión de audio en español y en francés. También tienen detalles de esta sesión en la página wiki de At-Large. No vamos a verificar asistencia en virtud del tiempo pero se va a registrar la asistencia de los representantes del ALAC y de los distintos integrantes de los equipos de liderazgo. Si desean hacer una pregunta o un comentario en francés o en español, por favor, escríbanlas en el chat comenzando su participación con las palabras QUESTION o COMMENT. Sean breves, por favor. Las preguntas en francés o en español van a ser traducidas al inglés y serán leídas por la persona a cargo de participación remota. Por favor, identifíquense con nombre y apellido al hacer este tipo de participación. Si están en la sala de Zoom y desean tomar la palabra, pueden levantar la mano y el personal va a ir organizando la fila de oradores. Por favor, pronuncien su nombre al tomar la palabra, no solo para las transcripciones sino también para que los intérpretes los puedan identificar en los canales de audio correspondientes. Al igual que todas las actividades de la ICANN, esta sesión se rige por los estándares de comportamiento de la ICANN. Voy a publicar un enlace a estos estándares de comportamiento en la sala de chat a la brevedad. Ahora entonces le doy la palabra a Joanna Kulesza, que va a comenzar esta sesión.

JOANNA KULESZA:

Muchas gracias, Michelle. Gracias a todos nuestros panelistas, a nuestros participantes de At-Large, del ALAC. Estamos realmente muy entusiasmados con esta sesión que es un ejercicio de creación de capacidades y de consenso también. Estoy muy contenta de ver que tenemos una diversidad de oradores en la sesión de hoy. Voy a ir presentándolos brevemente y voy a dar unas palabras de apertura. Luego le vamos a ir dando la palabra a los distintos oradores. Los participantes también van a poder formular las preguntas que consideren pertinentes.

Antes de avanzar quiero reiterarles que esta sesión es un ejercicio de creación de capacidades y de consenso. Queremos tener una narrativa contemporánea para el tema de Un Mundo, Una Internet. Con lo cual, queremos tener una narrativa integral, intercomunitaria que nos sirva para comunicar dentro de la ICANN y dentro del mundo en general este tema. Con respecto al mundo en general, vamos a ver cuestiones y eventos en cuestiones de geopolítica con debates en curso en distintos foros. Dicho esto, le doy la bienvenida a León Sánchez, el vicepresidente de la junta directiva de la ICANN. Estoy muy interesada acerca de lo que nos va a decir León con respecto a la posición de la junta directiva y cuál es el rumbo que la junta directiva desea que sigamos con respecto a estas cuestiones de geopolítica también. Es la primera vez que se menciona la palabra geopolítica en documentos de planificación. Dicho esto, le doy la palabra también a León y le damos la bienvenida porque él hablará acerca de la cuestión geopolítica.

Veni Markovski, de la organización de la ICANN, ha publicado recientemente un documento. Tenemos el enlace a este documento en el temario de esta sesión. Les recomiendo que lean este documento. Realmente no es un documento muy extenso. Lo pueden leer inmediatamente después de la sesión. Veni nos va a presentar un resumen de este documento y vamos a ver si la ICANN tiene un lugar, si debería tener un lugar o una función en el diálogo en curso en materia de geopolítica.

En representación de la NCUC contamos con Milton Mueller, que ha realizado muchísimo trabajo en investigación y con muchas publicaciones acerca del proceso de fragmentación de la Internet. Milton nos va a dar una presentación acerca de la soberanía de los distintos estados y gobiernos. Queremos trabajar también al respecto en relación con nuestra tarea en materia de políticas.

Por último, pero no menos importante, contamos con Patrik Fältström quien, a raíz de las conversaciones que hemos mantenido, llegó a la conclusión de que valía la pena participar en este panel y está con nosotros de manera remota. Le agradecemos su participación en esta reunión virtual de la ICANN. Me interesa mucho escuchar a Patrik, quien nos va a dar un marco técnico de toda esta perspectiva acerca de la ICANN y del marco de trabajo de la ICANN.

Por último tenemos 15 minutos para preguntas y respuestas. Entiendo que Milton Mueller tiene otro compromiso después de esta sesión. Después de su presentación vamos a tener un breve espacio para

preguntas y respuestas. Luego continuaremos con Patrik y finalmente tendremos la sesión de preguntas y respuestas que figura en el temario. Los que me conocen saben que soy muy estricta con el tiempo. Como les dijo Michelle, nuestro maravilloso personal va a estar monitoreando la sala de chat, prestando atención a las preguntas que van a ser incluidas en la sesión de preguntas y respuestas.

Ahora pasamos a la próxima parte de esta presentación porque quiero contarles acerca de los temas de nuestro interés. También me interesa escuchar sus opiniones. Sé que tenemos participantes de distintas comunidades y también tenemos representantes externos a la comunidad de la ICANN que están aquí hoy para hablar acerca de la ciberseguridad y el ciberdelito.

Muy bien. Vamos a comenzar hablando de la fragmentación de la Internet. Entiendo que Milton se va a centrar en este tema. Este es nuestro punto de partida y seguramente ninguno de los participantes en esta sesión pasó por alto el título que dice que los estados quieren ejercer su soberanía asegurándose de que su porción de Internet sea segura. Al trabajar en el entorno de la ICANN nosotros sabemos que Internet es una red que queremos mantener segura. Estas narrativas no son muy compatibles con nuestra postura y este es nuestro punto de participación. Queremos ver si la fragmentación es posible, si debería ser posible y a cuánta profundidad se debería llegar en términos de fragmentación en las capas de Internet. Es decir, ¿se puede ir más allá de la capa de contenidos?

Nosotros venimos abogando por una narrativa en común acerca del uso indebido del DNS. Cuando hablamos acerca de uso indebido del DNS fuera del ámbito de la ICANN hablamos de ciberdelito y ciberseguridad. En reuniones de la ICANN escuché que estas dos narrativas o estos dos relatos deberían ir de la mano. Nos gustaría encontrar una narrativa en común que encaje en la narrativa de uso indebido del DNS tanto dentro como fuera de la ICANN para incluir ciberseguridad y ciberdelitos. Esta es una vía que podríamos analizar. Es decir, tener un punto en común entre ciberdelito, ciberseguridad y uso indebido del DNS.

En el día de ayer tuvimos un seminario web sobre DoH y DoT en At-Large y tuvimos la oportunidad de aprender un poco más acerca de estos recursos técnicos. Nos contaron un poco acerca de los Simpson también, con DoH, pero me gustaría relacionar este tema con la sesión de hoy y estoy muy contenta de que Patrik esté aquí junto a nosotros. Estoy muy contenta de que vamos a tener más perspectivas acerca del grupo de expertos gubernamentales y también del grupo de trabajo abierto de la ONU. Me encantaría saber más acerca de esa participación en esas plataformas y el GAC en la ICANN. Nosotros les hemos extendido una invitación a los miembros del GAC y espero que puedan participar de manera remota ya que no pueden estar en el panel y que también participen en la sesión de preguntas y respuestas.

También quisiera ver si tenemos un punto de encuentro entre el trabajo del GAC y el diálogo entre los gobiernos a nivel de Naciones Unidas. Veo que la ICANN ya ha tenido algunas sesiones de creación de

capacidades con los gobiernos y me interesa saber un poco más al respecto. También ahí podemos tener una oportunidad para que la comunidad participe en este proceso. Con esto llegamos al punto seis. Cuál es nuestra función como comunidad para mantener a la Internet como una sola red disponible para todos y que también sea segura.

Por último vemos la última pregunta en el temario que nos sirve como una transición para nuestro próximo orador. En la junta directiva están muy al tanto de esta cuestión y tienen planes justamente para que en los próximos años se inicie un diálogo a nivel de la comunidad y de la organización también y de la junta directiva. Dicho esto, puedo darle la palabra a León, que nos va a hablar acerca de cómo afrontar estos desafíos en el ámbito geopolítico.

LEÓN SÁNCHEZ:

Gracias, Joanna. Gracias por invitarme. Gracias por tenerme aquí con ustedes en esta sesión. Creo que este tema es muy importante y a modo de contexto acerca de una posible respuesta, porque no creo que nosotros como junta directiva tengamos la respuesta absoluta a estas preguntas, pero a modo de contexto para complementar sus palabras, usted habrá notado que en el plan estratégico para los próximos cinco años tenemos un objetivo estratégico que implica justamente las cuestiones geopolíticas que tienen un impacto sobre la misión de la ICANN de garantizar una única Internet global e interoperable.

Nosotros consideramos que estos riesgos afectan la interoperabilidad de una única Internet y que las políticas gubernamentales ya han tenido un impacto sobre las operaciones o el funcionamiento de Internet. Por ejemplo, tenemos el GDPR. Ustedes ya conocerán este acrónimo. Consideramos que tanto esta como otras iniciativas podrían afectar la manera en que funciona Internet y, hasta cierto punto, podrían cambiar la situación actual en caso de que se implementaran estas medidas y se concretaran en una realidad.

Para alcanzar este objetivo estratégico de las cuestiones geopolíticas que podrían impactar la misión de la ICANN tenemos dos metas estratégicas. En primer lugar adoptar o identificar y abordar los desafíos y las oportunidades globales dentro del ámbito de incumbencia de la ICANN mediante el desarrollo de sistemas de alerta temprana como por ejemplo los informes de la organización de la ICANN sobre iniciativas en materia regulatoria. Si hablamos acerca de un rol estratégico, hablamos acerca de un esfuerzo continuo para identificar estos desafíos y estas oportunidades globales. Estamos hablando acerca del ámbito acotado de la misión de la ICANN. No se trata de abarcar todo el ecosistema de gobernanza de Internet y sus tendencias sino solamente todo lo que tiene que ver con la misión acotada de la ICANN.

En tal sentido tenemos resultados específicos que queremos lograr. Por ejemplo, que se continúe desarrollando y mejorando sistemas para detectar iniciativas en materia de legislación y también acciones o iniciativas gubernamentales que podrían afectar la misión o las

operaciones de la ICANN. En tal sentido, creo que su pregunta acerca del rol de los grupos de partes interesadas de la ICANN en este debate sobre la división de la red y sobre estas tendencias, creo que su pregunta es realmente muy pertinente y sumamente importante porque somos conscientes de que no estamos solos en esto, que no estamos aislados y confiamos en el trabajo y los aportes de nuestra diversa red de voluntarios en la comunidad para poder identificar estos desafíos y tendencias.

Para mí, la respuesta a esta pregunta de cuál es el rol de los distintos grupos de partes interesadas de la ICANN es clave y creo que es clave que la comunidad y la organización logren estos objetivos y estas metas. Tenemos que trabajar juntos como comunidad, como organización, como junta directiva para identificar estos desafíos y tratar de trabajar de manera constructiva para encontrar vías comunes de acción.

Otro resultado específico es que la ICANN trabaje con la comunidad para concientizar acerca de los sistemas de alerta temprana. Juntos podemos trabajar para educar a quienes necesitan esta educación o esta capacitación. No me refiero a un grupo en particular sino a que gran parte de las iniciativas que estamos tratando de implementar apuntan a relacionarnos con los decisores para que tengan una perspectiva más amplia y evitar consecuencias no deseadas que derivan de normas regulatorias que no tienen en cuenta el funcionamiento de Internet y cómo interactúan las distintas capas

operativas en este funcionamiento con respecto a las cuestiones técnicas.

Otro resultado específico es que la ICANN tenga procesos específicos para recibir los aportes y los comentarios de la comunidad. Tenemos que continuar trabajando al respecto. Ustedes sabrán que el grupo de trabajo intercomunitario sobre gobernanza de Internet que ahora se transformó en un grupo de relacionamiento o participación está realizando una labor y creo que su labor y sus debates son esenciales para lograr este resultado específico. Cuanto más podamos interactuar y cooperar entre nosotros y compartir información, más efectivos seremos.

Otro resultado específico es que la ICANN congrege a las partes relevantes para hablar acerca de distintas oportunidades a nivel global también. Creo que tener una comunicación cercana y un relacionamiento cercano con la comunidad, con la organización y con la junta directiva también será esencial para lograr este objetivo. Hemos identificado algunos riesgos estratégicos de la ICANN con respecto a su participación en la gobernanza de Internet y con respecto a la intervención de gobiernos, estados o entidades externas. Esto a veces hace que la ICANN entre en una modalidad reactiva. Su rol como partes interesadas individuales es realmente muy valioso al respecto. Si nosotros podemos juntos identificar estos desafíos y abordarlos, entonces vamos a tener mayores oportunidades de éxito.

El segundo objetivo estratégico es seguir forjando alianzas en el ecosistema de Internet y juntos sensibilizar a las partes interesadas globales acerca de la misión y las políticas de la ICANN. Quizá les sorprenda pero no todo el mundo sabe qué es la ICANN o qué hace. Para generar estas alianzas y sensibilizar acerca de cómo trabajamos y qué hacemos, etc., necesitamos hacer este trabajo para mitigar los riesgos de manera tal que podamos abordar los desafíos que implica esta situación geopolítica.

También tenemos algunos resultados específicos acerca de identificar riesgos estratégicos y uno de estos resultados es que la ICANN fomente una relación exitosa y mutuamente beneficiosa con socios regionales y globales para garantizar que se difunda el conocimiento acerca de la ICANN. Nuestra comunidad sigue siendo nuestra principal fortaleza. Si podemos generar estas alianzas colaborando estrechamente con la organización y con las distintas partes de la comunidad en todo el mundo, podríamos lograr un impacto muy importante.

Además, quisiéramos que la ICANN involucre, reconozca y exprese sus valores en los ámbitos donde se discuten estos temas. Queremos que la ICANN sea un jugador confiable y reconocido en esta área. Aquí nuevamente la colaboración en la comunidad es sumamente importante. También nos gustaría que la ICANN tenga un rol importante a la hora de crear conocimientos y concientizar entre los legisladores, las partes interesadas acerca de su misión en las distintas propuestas legislativas y de otra naturaleza en el ecosistema de la ICANN.

Yo creo que uno de los beneficios que disfrutamos en este plan estratégico es que lo tomamos como un documento vivo. No es un documento que haya sido diseñado ni construido para ponerlo en un estante y olvidarlo. Hemos discutido cómo hacer para mantener vivo el documento, cómo actualizarlo periódicamente. No solo por el simple hecho de actualizarlo y decir que se identificaron nuevas tendencias sino hacer este ejercicio para garantizar que el plan estratégico y, por supuesto, sus objetivos y sus metas, sigan siendo actuales y estén a la altura de los desafíos que se vayan enfrentando en los distintos momentos.

Además, como venía diciendo, hemos identificado algunos riesgos estratégicos relacionados con la construcción de las alianzas. Uno es la no comprensión de cuál es el ámbito de acción de la ICANN. Creo que eso se debe a que no hemos participado lo suficiente en los distintos campos o foros. Si nosotros no transmitimos, no hacemos conocer claramente la misión y el ámbito de acción de la ICANN, corremos el riesgo de que surjan malentendidos con respecto al alcance del trabajo de la ICANN.

Otro riesgo es que la infraestructura de la Internet, la seguridad y el control sigue estando en manos del control nacional. Aquí el trabajo de la comunidad es esencial. Nosotros no sabemos todo pero sí tenemos una red muy rica y diversa de socios en la comunidad que pueden ayudarnos a sortear estos desafíos y trabajar juntos para superarlos. Además, tener una Internet única e interoperable,

trabajando con las raíces o aumentar los aspectos comunes, esto mejoraría la situación global.

Como ustedes habrán visto, esta es la visión de la junta directiva con respecto a este objetivo estratégico. Yo no tengo las respuestas a todas las preguntas que ustedes han formulado pero sin duda las preguntas seis, siete y creo que también la tres son muy importantes a la hora de tratar las cuestiones geopolíticas que podrían impactar la misión de la ICANN. En este sentido, definitivamente les aliento a que continúen trabajando juntos, a que sigan planteando las cuestiones que vemos que van emergiendo, que siga la discusión y que, por supuesto, continuemos hablando constructivamente, deliberando cuáles son las mejores maneras de abordar estas cuestiones geopolíticas correctamente.

A veces en estos temas nos enfrentamos a la frustración, a las dificultades de no contar con todas las herramientas que necesitaríamos para concretar nuestros objetivos en este campo. Para esto nuevamente la comunidad es clave, es crucial. Lo vemos como una de nuestras grandes fortalezas. Bien, con esto, Joanna, permítanme agradecerles y estoy aquí abierto a cualquier comentario o pregunta que puedan tener. Gracias.

JOANNA KULESZA:

Muchas gracias, León, por permanecer y darnos su tiempo. Veo un chat muy activo que es fantástico para cualquier moderador. Veo que hay algunos que discuten. Veo una mano alzada pero le voy a pedir que me

permita como moderadora delegar su pregunta a la sesión de preguntas y respuestas de este panel porque primero vamos a recibir las presentaciones de los otros panelistas. Como nos decía León, hay muchos temas que son algunos muy controversiales que tienen impactos regionales desde lo jurídico. Aun cuando me siento tentada a hablar, no voy a hacer ningún comentario ni pregunta específica. Por cuestión de tiempo voy a tratar de llevarnos a la presentación de Veni, quien nos va a dar un contexto para lo que nos contaba León. Haciendo este énfasis de que la ICANN intenta relacionarse con otras partes interesadas para concientizar a otras partes del mundo acerca de lo que pasa en otros lugares.

Veni y su gente trabajan en los procesos de Naciones Unidas. Creo que es un aspecto muy interesante de discusión. La pregunta en general es si ICANN tiene algún ámbito de acción en estos procesos. Está el grupo de trabajo abierto, el OEWG. La pregunta es si ICANN puede participar allí o alguno de nosotros. Las respuestas quizá las encuentren en el documento de Veni. Otra pregunta. ¿Cuál fue la génesis de estos dos grupos de trabajo? El grupo de expertos gubernamentales y el OEWG. Le voy a pasar la palabra a Veni para que nos explique. Muchísimas gracias, Veni. Tiene la palabra.

LEÓN SÁNCHEZ:

Habla Jim Prendergast en el chat. Creo que quiere hacer un comentario. Si me permite interrumpir, le voy a pedir a Göran que responda la pregunta de Jim Prendergast en el chat.

partes interesadas

GÖRAN MARBY: ¿Pueden oírme?

JOANNA KULESZA: Sí.

GÖRAN MARBY: Es una pregunta de Jim. Para empezar no fue hace un año cuando surgió esta idea de tener esta interfaz entre nuestras interacciones con los gobiernos y un punto en la comunidad con el cual pudiéramos hablar de manera regular. Presentamos esta idea a los líderes de las SO y AC que creo que los llevaron a sus respectivas comunidades. No está en nuestras manos tomar la decisión sino que la comunidad tomará esta decisión. Creo que todos acordamos que sería bueno tener una interfaz regular entre el trabajo que nosotros hacemos en el plano gubernamental y este intercambio con la comunidad que sea mejor. Respondiendo a su pregunta, Jim, está en mano de ustedes. Nosotros simplemente lo hemos propuesto. Mientras tanto, lo que hemos iniciado y Veni les contará más porque de hecho produjeron la primera actualización, es un documento informativo acerca de lo que estamos observando en los distintos ámbitos políticos del mundo. El primer es Naciones Unidas y el segundo es la perspectiva de Bruselas, etc.

Además, en coordinación con las partes interesadas de la India, y esto está publicado en la página de correspondencia, hay algunas visiones

partes interesadas

u opiniones técnicas sobre los posibles impactos que tendrá la futura legislación en la India. Es un espacio donde la comunidad podrá discutir estos temas de una manera más ordenada. Esa era la propuesta.

JOANNA KULESZA:

Muchas gracias, Göran. Ahora sí, le paso la palabra a Veni, quien seguramente por un lado nos dará más detalles sobre este tema y aquí estoy siguiendo el tiempo. Además, Veni nos dará contexto. Veni, tiene la palabra.

VENI MARKOVSKI:

Gracias. Primero quiero decir que esta sesión es fantástica. La verdad, León ya contó varias de las cosas que yo quería compartir con ustedes. Lo primero que quería decir es que la comunidad At-Large está en todas partes del mundo y su magnitud y su comprensión de lo que pasa a nivel nacional y regional, e incluso a veces a nivel global, puede aumentar la comprensión que tenemos de los casos. Ustedes me pueden dar información a mí de legislaciones regionales o nacionales o discusiones de política, temas de interés que a veces pueden llegar a Naciones Unidas.

Ustedes mencionaron el documento varias veces. No espero que la gente lo haya leído aunque el vínculo está en el chat. En su momento, cuando tengan tiempo para leerlo, es un antecedente histórico de lo que ha hecho la ICANN en Naciones Unidas con algunos resúmenes de

las recientes discusiones respecto de la cibercriminalidad y la ciberseguridad. Lo que pasa en Naciones Unidas. En particular, hacemos énfasis en las cosas que mencionan a ICANN directa o indirectamente. Sí, hay instancias en que los gobiernos hablan de la ICANN y a veces hablan de lo que la ICANN hace y prestamos atención. Lo que hacemos, lo que yo hago, es asegurarnos de que se entienda bien.

Naciones Unidas es muy distinto del trabajo que hacemos con el GAC. El GAC está formado generalmente por representantes de las administraciones de telecomunicaciones de los gobiernos. A veces hay representantes que vienen de los ministerios de Relaciones Exteriores. Por eso, como explicamos en el documento, hacemos muchas acciones de educación, de difusión externa. Nosotros no hacemos lobby por ICANN. No necesariamente explicamos solo lo que la ICANN hace aunque sí lo hacemos sino que también hablamos de cuál es la función, cuál es nuestro rol.

Los diplomáticos en Naciones Unidas y los otros delegados que hablan de cibercriminalidad y ciberseguridad trabajan en comités y luego presentan sus trabajos a la asamblea general. Nosotros tratamos de llevar toda la información, todos los hechos a estas personas para asegurarnos de que sepan, de que si tienen preguntas, siempre nos pueden preguntar a nosotros. Si no tenemos las respuestas, tenemos recursos, personas en la comunidad de la ICANN a quienes podemos pedir ayuda. No sé quién hizo una pregunta acerca de si él o ella o ellos podían participar en estas discusiones. Estas deliberaciones que

tienen lugar en Naciones Unidas no son abiertas al público. La única manera de participación es que alguien tenga acceso a Naciones Unidas o desde el Congreso se otorgue acceso a las deliberaciones.

Esta es una reseña general del trabajo en Naciones Unidas. Más concretamente, como dice el documento... Joanna, usted mencionó un par de grupos que trabajan en paralelo en este momento en Naciones Unidas. Son grupos abiertos, entonces se van agregando miembros. Está el OEWG, que es el grupo de trabajo abierto, y luego el GGE, que es el grupo de expertos gubernamentales. Luego está el OECE, el grupo de trabajo abierto del comité de expertos. El primer grupo está abierto a todos los estados miembro. El GGE está abierto solo a 25 estados miembro. Sus miembros son solo 25 que son expertos, enviados por los gobiernos. El último grupo trabaja en una nueva convención sobre el ciberdelito. Todavía estamos a la espera de ver qué producen.

El OEWG ya ha tenido dos sesiones. Una el año pasado y una el pasado febrero. También tuvo una consulta abierta en Naciones Unidas con más de 100 organizaciones que participaron, organizaciones interesadas en ciberseguridad. Lo que nosotros hacemos es seguir lo que está pasando en estas sesiones y si alguien habla de la ICANN, nosotros nos aseguramos de que lo que se diga sea conforme a los hechos, sea correcto. Si no, proporcionamos información. Tratamos de incorporar, agregar conocimiento a esta discusión desde nuestro punto de vista, que es una organización técnica que se ocupa de un segmento muy pequeño del sistema de identificadores únicos. Creo

partes interesadas

que el documento se explica por sí mismo. Quise publicarlo antes de la reunión de la ICANN para que pudieran leerlo y saber si ustedes tienen preguntas. No sé, Joanna, si he respondido las preguntas que se han formulado desde el principio de la sesión. Si no, hágamelo saber.

JOANNA KULESZA:

Muchas gracias, Veni. Creo que hay más preguntas pendientes. La pregunta general es cómo podemos ayudar nosotros. Usted ya dijo que estos grupos no están abiertos al público. Mi concepción es que podamos tener una narrativa compartida en la comunidad que podamos compartir con las partes externas. Usted dijo que a lo mejor el GAC no sería la mejor comunidad para desplegar esta narrativa. Desde la perspectiva del usuario final, la pregunta es cuál es nuestro interés, cómo podemos tener esta narrativa coherente y cómo nosotros como comunidad de ICANN podemos brindar apoyo a esto porque usted indicó que el trabajo que hacen es dar información fáctica, hechos acerca de lo que está pasando. La pregunta es si hay algo que nosotros podamos hacer para desarrollar esta narrativa compartida para sacarla de esta burbuja que es la ICANN para respaldar este concepto de Un Mundo, Una Internet.

VENI MARKOVSKI:

Una corrección. Yo no dije que el GAC no sea el mejor [inaudible]. El GAC es muy relevante. Yo lo que dije es que los miembros de Naciones Unidas no necesariamente saben lo que hace el GAC. Es como comparar gente de ministerios de Telecomunicaciones con los de

Relaciones Exteriores. Hacemos difusión externa entre diplomáticos. La manera de ayudar es llegar a los respectivos parlamentos y hablar también con los ministerios de Relaciones Exteriores que cubren la delegación en Naciones Unidas y hacer contactos, difusión externa. Hay muchísimos temas por cubrir. La gente puede entonces identificar quién es la persona delegada ante Naciones Unidas y otras organizaciones intergubernamentales y contribuir en el seguimiento de estos temas. A veces los grandes confines tienen grandes misiones. Cuanto más se limita el accionar, más reducido es el tema. Obviamente, hay muchas sesiones en estos dos grupos. Si la discusión no la consideran importante, a lo mejor los participantes no aparecen y las discusiones se dan por otras vías.

En el Consejo de Seguridad de Naciones Unidas obviamente se habla de la guerra y la paz y pueden no considerar importante la parte técnica. Obviamente, ahí nosotros podemos ayudar. El consejo se reunirá en los próximos meses. Creo que una manera de ayudar y creo que lo dije al comienzo es llegar a los parlamentos, a los congresos, a los ministerios de relaciones exteriores e identificar aquellas personas de los países que están involucradas o interesadas en las deliberaciones de Naciones Unidas y de otras organizaciones intergubernamentales.

JOANNA KULESZA:

Muchas gracias, Veni. Si les parece, con esto nos detenemos y esperamos a las preguntas al final. Ahora quisiera pasar a darle la

partes interesadas

palabra a Milton. Sé que él tiene una presentación. Vamos a escuchar su presentación mientras vemos las diapositivas. Luego tendremos unos tres o cuatro minutos de discusión sobre esta presentación sola, específica, teniendo en cuenta que Milton tiene que irse por otro compromiso, y luego pasamos rápidamente a Patrik. Milton, tiene la palabra.

MILTON MUELLER:

Gracias, Joanna. Realmente esta es una pregunta muy interesante. Estoy muy agradecido porque usted haya organizado esta sesión y le pido a la persona a cargo de la sala que vaya cambiando las diapositivas. El tema de mi presentación se basa en un libro que yo he escrito. No vengo aquí a publicitar mi libro sino más bien a decirles que hay ideas muy desarrolladas acerca de este tema. Si ustedes están interesados en este tema, entonces les recomiendo que estén al tanto de estas ideas.

Los orígenes de mi pensamiento acerca de todo este tema se remontan a tres o cuatro años atrás, cuando se realizó un debate acerca de la fragmentación de la Internet. Me dieron ganas de explorar este tema porque quedaba claro que no había una definición coherente acerca de lo que la gente quería decir cuando hablaba de fragmentación. De hecho, era más bien una palabra que asustaba a todas las personas que participaban en un debate.

Aquí tenemos una lista de todos los componentes que a veces la gente denomina fragmentación según el contexto. Por ejemplo, si alguien

corta un cable fuera de mi casa de manera accidental porque está haciendo una excavación, ¿esa es una fragmentación de Internet? Porque de repente mi casa ha quedado desconectada junto con otros siete u ocho hogares. No creo que eso sea una fragmentación de Internet. Simplemente es una interrupción temporaria del servicio en un lugar local.

Ahora hablemos de la localización de datos. Tenemos a veces el tema de la fragmentación que deriva en gran medida de los datos localizados. Para mí esta fue una muy mala idea, la localización de datos, porque no tiene sentido llamar a esto fragmentación de Internet. De hecho, los datos localizados siempre están disponibles. Hay que buscarlos dentro de una jurisdicción.

También escuché hablar de bloqueo de contenidos en cuanto a fragmentación. También las distintas medidas de pago o barreras de pago que limitan el acceso de algunas personas a Internet pero si esta es una instancia de fragmentación, entonces estamos en problemas porque hay muchos servicios en línea, incluso proveedores de servicios de Internet, que justamente dependen del pago de los clientes para poder ofrecer un servicio. Luego tenemos el tema de la Internet a nivel nacional que también se llama fragmentación. En el libro tienen un análisis en mayor profundidad al respecto.

En gran medida, todo aquello que llamamos Internet nacional no lo es sino que más bien se trata de una Internet que tiene mucho nivel de regulación o de restricción o censura pero en ningún caso se niegan

esos países a conectarse a la Internet global. Por ejemplo, tenemos el caso de Corea del Norte. Luego tenemos un concepto por ejemplo acerca de las diferencias lingüísticas. Eso no es una fragmentación de Internet sino más bien una diferencia cultural o fragmentación cultural. No es el resultado de la fragmentación de Internet.

De qué trata este debate. Por qué estamos hablando acerca de la fragmentación de Internet. Yo intenté buscar un término mejor para describir esta situación y se me ocurrió el término alineación. La alineación se refiere al desfase entre los límites territoriales entre los gobiernos y la conectividad global de Internet. La alineación es el proceso mediante el cual los gobiernos nacionales intentan ejercer la soberanía sobre un ciberespacio que no es territorial. Es realmente el motor que impulsa las preocupaciones de la gente cuando justamente hablan de fragmentación.

Aquí tenemos una definición de lo que yo llamo alineación. Vemos a un hombre en pantalla que está intentando introducir un cilindro en un cuadrado. La alineación es la subyugación del dominio cibernético que es no territorial a las jurisdicciones políticas que en efecto son territoriales. Vemos aquí tres métodos de alineación. Uno de ellos es declarar que un ciberdominio es cuestión de seguridad nacional. Esto sucede en gran medida en Estados Unidos, en China, en Rusia y en otras ciberpotencias. También vemos la nacionalización y centralización de las amenazas en materia de inteligencia y la respuesta ante incidentes. Vemos una tendencia a adoptar normas técnicas nacionales que podrían derivar en la verdadera

fragmentación de Internet y vemos interruptores de apagado que permiten cerrar Internet o desactivar parte de Internet en respuesta a una amenaza a la seguridad nacional.

Otro método de alineación es la territorialización de los flujos de información. Por ejemplo, filtrando contenidos, más allá de una frontera nacional o localizando datos o también haciendo un bloqueo por zona geográfica. Por último, y esto es lo más importante para la ICANN, tenemos una suerte de alineación de recursos críticos en Internet. Me refiero a los nombres y a las direcciones principalmente. Probablemente escucharon hablar acerca de alguna iniciativa para crear raíces o rutas para nombres de dominio nacionales y también los registros nacionales de Internet que los gobiernos nacionales están tratando de crear para ser una fuente de distribución de direcciones IP. Pero los recursos críticos de Internet nacieron como un recurso global. Son parte de normas técnicas globales y se arraigaron en instituciones multinacionales como la ICANN y los registros regionales de Internet. Esta parte de la alineación es realmente muy difícil y probablemente nunca suceda.

Esta diapositiva la voy a pasar y voy a hablar acerca de la ciberseguridad más adelante. Muy bien. Veamos las limitaciones en materia de alineación. Tenemos tres en pantalla. En primer lugar, simplemente que la Internet tiene alcance global. Desde hace 25 años aproximadamente tenemos, y esto lo demuestran los hechos, nombres y número globalizados en lo que respecta a su administración. Tenemos una institución global que es la Corporación para la

Asignación de Nombres y Números en Internet que justamente se encarga del DNS a nivel global. También tenemos la interoperabilidad por defecto de los protocolos de Internet a nivel global de manera tal de tener esta compatibilidad global. Con lo cual, si uno quiere interferir en esa compatibilidad, es realmente muy difícil. Contrariamente a lo que funciona o a lo que sucede con los sistemas telefónicos o de comunicaciones telefónicas.

Luego tenemos la eficiencia económica como otra limitación. Todos sabemos acerca de las redes externas. Esto significa que algunos bienes cobran mayor valor a medida que se los usa en mayor medida. Estaríamos sacrificando economías compartidas, competencia e innovación si nos retirásemos de esta compatibilidad global. Luego tenemos la paradoja de la jurisdicción. Es decir, cuando un gobierno territorial quiere ejercer el control sobre la Internet dentro de su territorio, realmente tiene que elegir entre tener un control limitado e inefectivo o bien globalizar ese control. Aquí tenemos el ejemplo de Estados Unidos versus Microsoft pero hay un ejemplo más sencillo y mejor que es la idea del derecho al olvido.

Por ejemplo, el gobierno francés quiere que este derecho al olvido sea obligatorio en Google, en su jurisdicción, pero no puede realmente hacerlo porque no se puede hacer cumplir solamente en Francia. Los tribunales europeos deciden que Google lo tiene que implementar a nivel global y esta es una paradoja porque en algunos países, sobre todo en Estados Unidos, no está el derecho al olvido. Hay un estado

que termina globalizando su jurisdicción a costa de los demás. Por eso la soberanía para mí es incompatible con Internet.

Aquí viene mi postura más radical. Realmente no tengo reparos en decirlo. Soy extremadamente radical. Fundamentalmente hay una contradicción. Podemos hacer de cuenta de que se la puede solucionar y que podemos llegar a un término medio después de un cierto tiempo pero fundamentalmente el ciberespacio es global y los gobiernos son territoriales. Este problema de gobernanza se soluciona mediante una noción de soberanía popular del ciberespacio. Es decir, que el ciberespacio se tiene que autogobernar con cierto grado de independencia. No totalmente independiente pero en cierta medida separado de la jurisdicción territorial de los estados nacionales.

Para los que piensan que estoy loco o que estoy diciendo algo imposible, aquí les muestro la primera de mis pruebas. La prueba A. Esto es algo por lo cual luchamos y que conseguimos. Logramos la soberanía popular en el ciberespacio de manera tal que es pertinente para la ICANN. Estoy hablando de la transición de la custodia de la IANA. Para quienes no están en Estados Unidos, quizá no estén al tanto del grado de preguntas que surgió a raíz de la transición de la IANA por parte de los gobiernos nacionales y con respecto a la gobernanza global del DNS. Hay algunos legisladores de derecha o nacionalistas que se oponían a que el gobierno de Obama hiciera esta transición porque decían que Estados Unidos le estaba dando Internet a China. Detrás de esas aseveraciones se decía que algunos estados nacionales tenían que tener el control de Internet y que teníamos que ser nosotros

y no Rusia o China. Por supuesto que si ustedes recuerdan la idea de la transición era que el control debía estar en manos de lo que se denominaba la comunidad global de Internet. Es decir, que debíamos trabajar para nuestro propio autogobierno en el ciberespacio y no quedar en manos de los gobiernos nacionales.

Quiero darles algunos ejemplos que son pertinentes para la ICANN. En primer lugar, la situación, el estatus de la ICANN, nosotros creamos la ICANN específicamente para evitar la fragmentación en jurisdicciones o la alineación del DNS con los estados nacionales. Es por eso que existe la ICANN. Nosotros seguimos luchando esta batalla una y otra vez y tenemos que defender esta capacidad de la ICANN como entidad de gobernanza global. Otro ejemplo tiene que ver con las controversias en torno al WHOIS y su cumplimiento con el GDPR. Hay quienes dicen que el WHOIS cumpla con el GDPR pero solo en la jurisdicción europea o solo en una jurisdicción específica. Si el usuario y el registrador están fuera de esa jurisdicción, entonces que tengan normas diferentes. Aquí vemos una fragmentación de la autoridad en el contexto de la gobernanza de la ICANN. Creo que vale la pena comprender que todo este modelo se basa en un enfoque integral no soberano para la gobernanza de Internet. Joanna, ¿cómo voy con el tiempo?

JOANNA KULESZA:

Está cumpliendo con el tiempo asignado maravillosamente bien. Tenemos tres o más de tres preguntas en la sala de chat. Le voy a dar

partes interesadas

la palabra al personal para que lea estas preguntas y usted las pueda ir respondiendo.

MILTON MUELLER:

Perfecto.

JOANNA KULESZA:

Le voy a dar la palabra a Evin, que va a leer las tres preguntas dirigidas a usted y luego le vamos a dar la palabra a Patrik también. Esperamos que se quede con nosotros también para las preguntas y respuestas finales.

EVIN ERDOĞDU:

La primera pregunta es de Zakir para Milton. Dice: “¿Qué pasa con las raíces alternativas y la fragmentación y las pruebas recientemente implementadas por Rusia con respecto a la fragmentación?” Gracias.

JOANNA KULESZA:

Evin, por favor, lea las tres preguntas.

EVIN ERDOĞDU:

Sí, por supuesto. La segunda pregunta es de Javier Rua Jovet que dice: “Es una pregunta para quien la quiera responder. Veo mucha colaboración entre el ALAC y el GAC, lo cual es bueno. Tuvimos una muy buena reunión con el GAC donde llegamos a varios acuerdos y

algunos miembros del ALAC incluyéndome, hemos trabajado al respecto en el pasado. Estas conversaciones son naturales y fáciles. ¿Cuáles son los peligros al respecto en cuanto a la geopolítica, sobre todo la cuestión de que el DNS y la gobernanza de los IP estén bajo la soberanía de nosotros, el pueblo de Internet, y no dentro de la órbita de los gobiernos o de la UIT? El ALAC, que representa a las personas y no a los gobiernos, ¿no debería estar a la defensa del modelo de gobernanza de Internet no gubernamental?”

Luego tenemos la tercera pregunta de Imran Hossen. Dice: “Participo por primera vez en estas reuniones de la ICANN. Tengo preguntas acerca de los puntos de intercambio de Internet. Muchos de ellos emanan de comunidades y organizaciones privadas como los que estoy mencionando en el ejemplo. Uno de esos es BDIX. Veo que están pasando a otro tipo de comunidades. ¿Hay algún tipo de control o de política de la ICANN sobre esos puntos de intercambio de Internet? Si no hay ninguna política, ¿qué piensa al respecto? Gracias”. Estas son las tres preguntas. Ahora le doy la palabra nuevamente a usted, Joanna.

JOANNA KULESZA:

Muchas gracias, Milton. Le doy la palabra para que pueda responder a estas preguntas. Luego avanzamos con los otros presentadores.

MILTON MUELLER:

Voy a hablar acerca de Rusia en primer lugar. Con respecto a las raíces alternativas, esto tiene que ver con cómo Internet se basa en una red externa. Cualquiera puede crear una raíz alternativa pero esta raíz alternativa muy probablemente derive en una incompatibilidad en cuanto a recursos de nombres. Con lo cual, muy pocas personas van a querer usar esta raíz alternativa.

La raíz de la ICANN tiene compatibilidad global que se traduce en las elecciones de los usuarios. Es muy poco probable que alguien alguna vez cree una raíz alternativa. Algunos de mis alumnos están trabajando en el tema de Rusia y su raíz alternativa que no lo es. Hay que ver si Rusia sabe lo que está haciendo al respecto con esta legislación y es un poco dudoso porque a veces no entienden la legislación. Están creando un sistema alternativo de contingencia que los protegería ante una amenaza percibida que no es una amenaza real sino percibida contra su nombre de dominio o dominio de alto nivel. Es decir, si percibieran una amenaza de interrupción de servicio de su nombre de dominio de alto nivel, por parte de Estados Unidos por ejemplo, entonces podrían actuar al respecto. Es decir, en pocas palabras, están generando un sistema de contingencia que los protegería de la interferencia de Estados Unidos. Por lo menos yo lo entiendo de esa manera.

Con respecto a la segunda pregunta, alguien está hablando acerca del peligro potencial de que At-Large y el Comité Asesor Gubernamental cooperen demasiado estrechamente. Creo que ahí hay un temor en esa pregunta y el temor es que el ALAC sea cooptado. Entiendo que el

comité asesor At-Large tiene cierta alianza en lo que respecta a las políticas de la ICANN con el GAC porque no tienen un rol directo en el desarrollo de políticas sino que tienen un rol de asesoramiento. Con lo cual, a veces ambos comités tienen la necesidad de que sus puntos de vista sean tenidos en cuenta, lo cual está bien pero lo que yo pregunto es si el ALAC no debería estar a la vanguardia de la defensa de la soberanía popular en el ciberespacio. Sí. De hecho, sus orígenes fueron unos experimentos bastante extremos con respecto a la votación de miembros individuales dentro de la ICANN. Algunas elecciones tenían los resultados incorrectos. Con lo cual, esa medida no se permitió y se creó el comité asesor At-Large, el ALAC, en lugar de ser una entidad compuesta por miembros individuales. Yo creo que At-Large debería ir a la vanguardia de la defensa del empoderamiento de la gente, de las personas en Internet. Es decir, de los usuarios, consumidores y productores de contenidos en Internet en la gobernanza de Internet.

Asumo que IX son los puntos de intercambio de Internet. Si entendí bien la pregunta, era si están regulados por la ICANN. Por supuesto, puedo ver que miembros de la junta directiva y del personal se ponen nerviosos y dicen enfáticamente quizá con más énfasis que el que yo usaría que no, que no se regulan los puntos de intercambio de Internet desde la ICANN, que se manejan los nombres de dominio. Pero si ese punto de intercambio de Internet usa un nombre de dominio, en cierta manera está regulado por la ICANN pero no el punto de intercambio directo. En ese sentido, la ICANN no hace demasiado. Eso es todo de mi parte y ahora esperemos que Patrik tome la palabra.

partes interesadas

JOANNA KULESZA: Muchas gracias, Milton. Gracias por su provocadora presentación. Necesitamos ahora conocer un poquito más sobre DoH y DoT. Nos contaron un poquito sobre las raíces alternativas. También tenemos a Andrei, que comenta. A ver si usted nos da un poquito más de información.

PATRIK FÄLTSTRÖM: Muchísimas gracias. Soy Patrik Fältström, director técnico de una de las organizaciones que opera uno de los puntos de intercambio, Netnod. Interesante la pregunta que se hizo antes que después voy a volver a tratar. Lo primero que tenemos que recordar o mirar es cuáles son las reacciones que generan los problemas de seguridad. Lo primero que quiero que recordemos es qué es lo que hacemos cuando algo malo está pasando. Cuando hay un evento, cuando algo pasa, hay que tener un proceso para ocuparse del proceso. En el mundo global, tenemos tantos jugadores distintos que es importante tener esta coordinación global entre las organizaciones y a veces, como explicó Milton, de manera transfronteriza. Desafortunadamente, esto no es algo que los gobiernos hayan entendido y, como explicaba Milton, como tenemos este desfase entre las fronteras de países de jurisdicción y de las organizaciones más allá del servicio de provean, servicios bajo la ICANN, genera este desfase. Muchos gobiernos han impuesto a las organizaciones que tengan procesos muy formales para manejo de los incidentes. Este que ven aquí es mi proceso personal

pero tratar de hacer esto en una sociedad es muy, muy difícil. Gracias. La siguiente.

Cuando hablamos de problemas de seguridad que se llaman incidentes, yo he trabajado con la academia Real de Ciencias de la Ingeniería Sueca. Elaboramos un informe en el cual arribamos a la conclusión de que ninguno de los términos seguridad de la información, seguridad de IT y ciberseguridad están definidos. Cuando alguien habla de ciberseguridad, todos sabemos qué significa pero siempre pedimos explicación. Yo preferiría usar otra terminología como figura en el informe de la Academia. La seguridad de la sociedad de la información está relacionada con todo tipo de amenazas. La seguridad de la ICANN es cualquier amenaza relacionada con la digitalización. Es decir, cuando la información está digitalizada.

La ciberseguridad es cuando tenemos un incidente que está relacionado con un antagonista, cuando alguien quiere que algo realmente pase. La pregunta del spam, la cuestión es totalmente distinta porque es una herramienta que puede usar otro para un objetivo. Cuando hablamos de spam, no necesariamente es malo o bueno. El foco puede ser distinto. Como dijo Milton en el caso de Rusia, los legisladores y también legisladores de otros países, incluso en mi propio país, Suecia, a veces no saben cómo funciona Internet y legislan cosas incorrectas. Sobre esto voy a hablar un poquito más después.

Otra conclusión a la cual arribamos en el informe es que ya no tenemos caños. Históricamente, en las telecomunicaciones teníamos

un jugador responsable de absolutamente todo, desde los cables, los servicios y todo lo demás. Hoy día tenemos capas horizontales. Pasamos entonces de tener caños a tener una lasaña. En esta lasaña tenemos muchas capas. Tenemos la capa del acceso a Internet, el protocolo del HTTP y distintas capas. Cada una de estas capas en la arquitectura técnica, la arquitectura de la Internet, tiene un direccionamiento y hay que considerar cada capa, una por vez. Desafortunadamente, a la economía del mercado le interesa construir caños. Por eso el servicio de chat de Facebook solo lo brinda Facebook. La empresa Facebook. Sucede lo mismo con muchos otros servicios que son como caños pero la arquitectura de la Internet es como una lasaña. Son capas. Por eso tenemos un protocolo encima del otro.

Hoy día, para tener más seguridad, tenemos que la gente recurre cada vez más a la encriptación. En la encriptación, cada una de las capas de la lasaña se le aplica la mayor cantidad posible de seguridad. Tenemos que encriptar la capa. Tenemos que tener firmas digitales en las capas. A veces hay tecnología como blockchain que permite dar otra seguridad. Esta diapositiva muestra un gráfico del 2017. Es un poquito antigua pero ven el aumento del tráfico web que ha aumentado que tiene encriptación. También el IETF y otras organizaciones, todos nosotros tenemos cada vez más seguridad. Queremos ver ese candidato. Ya no queremos tener nombres de dominio que no tengan firma de DNSSEC. Queremos tener todo firmado pero no debemos olvidar que la seguridad se aplica una capa por vez. La siguiente.

Tomemos un ejemplo de esta arquitectura. Voy a simplificar las cosas diciendo que aquí solo tenemos tres capas. Abajo tenemos los paquetes de IP que fluyen en la red que utiliza direcciones IP entre el remitente y el destinatario. Entre los paquetes es posible identificar en la arquitectura de la Internet flujos de paquetes. Estos flujos utilizan quintuples que son el protocolo que es, por ejemplo, TCP o UDP. Está el puerto del remitente y del destinatario y la dirección IP. Son los elementos que identifican la comunicación que está teniendo lugar en la Internet. Usando estos flujos, uno o varios, surge una aplicación. La aplicación puede ser, por ejemplo, un navegador web que se conecta a uno o varios servidores web para transmitir la información para pintar una página web en un navegador web. Tenemos estas tres capas distintas. Vamos a ver cada una de ellas individualmente para ver qué pasa. La siguiente, por favor.

Si sucede que empezamos a encriptar la comunicación, qué pasaría por ejemplo con TLS y HTTP. Qué pasa. Estamos encriptando las dos de arriba que están en negro. El que vea el paquete ya no puede ver lo que está dentro del paquete, qué está fluyendo en esta capa. No obstante, puede ver el paquete IP con la dirección IP y puede hacer identificación de flujo de paquete pero no puede ver exactamente qué está pasando dentro del flujo. Esto significa que la encriptación dificulta o le hace más difícil a aquel que está mirando el tráfico, le hace difícil saber qué está pasando. Es mucho más difícil porque la entidad solo tiene las dos capas inferiores de esta lasaña en lugar de tener las tres. Son los únicos datos que le permiten tomar una

decisión, hacer una evaluación de lo que está pasando en la red. Por supuesto, esta es una de las metas que procura alcanzar la encriptación. La siguiente, por favor.

Ahora, volviendo a lo que decía Milton, que tenemos dos partes que se están comunicando, la roja y la verde, que usan dos ISP distintos que están en dos jurisdicciones diferentes. Fíjense en los dos caños. Uno que va desde el DNS y otro HTTP. Fíjense que el del DNS está roto. La consulta, la query del DNS, va de la verde a otro ISP que a su vez envía la query al otro ISP que responde y el verde abre la conexión a la roja para efectuar la transmisión de los datos. Así es como se veía históricamente. Vemos que ambos ISP pueden ver tanto dentro de los caños como fuera. La siguiente.

Lo primero que hicimos con Internet es empezar a encriptar el tráfico de HTTP. Al encriptarlo, es imposible que otro ISP en otra jurisdicción vea qué está pasando. De hecho, es imposible que un único ISP vea qué pasa en su jurisdicción porque la conexión entre el rojo y el verde está encriptada. La siguiente.

Lo que pasa ahora con la encriptación también en DNS es lo siguiente. Una manera de desplegar DNS sobre TLS es que tenemos DNS en un caño separado pero la conexión entre el verde y otro ISP ahora está encriptada. Ya no es posible, por ejemplo, hacer un ataque entre el verde y otro ISP. El resto de la conexión sigue igual. Ambos ISP pueden ver el tráfico y hacer lo que quieren con el tráfico. La siguiente.

Otra cosa que puede pasar es que la gente usa DNS sobre HTTPS. Con esto, qué pasa. No solo el tráfico del DNS es enviado directamente a un servicio de DNS que está en algún lugar sino que algunos despliegues envían el tráfico en el mismo caño, en el mismo flujo que HTTPS. Es como si el tráfico fuera directamente a un jugador que puede estar en otra jurisdicción. En este caso, tanto HTTPS como DNS están dentro del caño negro. Es imposible saber qué está pasando. Ningún ISP en ninguna jurisdicción puede saber qué está pasando. Lo único que pueden hacer estos dos ISP es ver los flujos que se usan y las direcciones IP de los tráficos que se están enviando. Nada más. La siguiente.

Aquí lo interesante es que por supuesto se podrían dar otros ejemplos y se habló de las raíces alternativas, cómo se firman y validan cosas firmadas por entidades que no son de confianza, cuál es el riesgo de que alguien pueda atacarnos pero aquí la idea, la noción, el problema, y aquí estoy de acuerdo con Milton, que es interesante porque ustedes que me conocen a mí y a Milton, hemos discutido mucho desde hace cinco mil años sobre este tipo de cosas, yo digo exactamente lo mismo que dice Milton. Las transacciones transfronterizas cuando hay reglas y jurisdicciones en conflicto que en definitiva se deben al uso conflictivo de normas en los distintos países, ¿cómo se maneja? ¿Qué se hace cuando dos jurisdicciones tienen conflictos entre sí?

Tenemos una jurisdicción. Tenemos una legislación. Se le pide a alguien que haga algo. Se le dice que de acuerdo con la legislación de esa jurisdicción, alguien tiene responsabilidad de hacer determinada

cosa. Tomemos por ejemplo una orden judicial. Se le ordena por ejemplo a un ISP bloquear el acceso a ciertas URL o páginas web. El ISP a veces lo implementa bloqueando los lookups del DNS de ciertos nombres de dominio. ¿Cómo lo puede hacer cuando el DNS está encriptado? Ya no lo puede hacer. La cuestión aquí es si está bien pedir al ISP que no puede ver las búsquedas en el DNS, pedirle que bloquee el acceso a las páginas web. La pregunta no es la correcta. La pregunta es quién es responsable. ¿Nadie? ¿Ninguno de los jugadores? En una jurisdicción, si hay una ley que dice que está mal el acceso a estas páginas web, ¿quién tiene la responsabilidad por bloquearlos? ¿Qué herramientas hay que usar? Quién sabe. Nadie lo sabe. La pregunta es quién es el responsable de cada cosa en transacciones transfronterizas. Cuando se aplica encriptación de seguridad DNSSEC a través de firmas que son soluciones técnicas pero están diseñadas para asegurarse de que nadie toque el tráfico, hay quienes pueden decir que esto es una competencia. Por eso es importante, como decía Milton, con lo cual estoy de acuerdo. Pero los legisladores tienen que entender estas capas de la lasaña y entender que las medidas de seguridad que se quieren tener aseguren que se protejan las tarjetas de crédito, por ejemplo, y que en la arquitectura ciertas cosas están encriptadas, otras están firmadas pero hay que acordar quién es efectivamente el responsable de hacer cada cosa. Eso es lo único que se puede implementar en jurisdicciones locales. Esperemos que con el tiempo surgirá una mayor homogeneización en las leyes de las distintas jurisdicciones porque eso es lo que, por supuesto, genera confianza. Gracias.

partes interesadas

JOANNA KULESZA:

Perfecto el tiempo, Patrik. Como soy moderadora no quiero abusar de mi rol. De acuerdo con la agenda vamos a proceder con el plan. Tengo una mano alzada. Hay preguntas en el chat donde ha habido muchas preguntas. Este es un ejercicio. Queremos saber qué piensa la sala, si este es un tema de interés y el chat así lo indica. Me gustaría continuarlo posiblemente en la próxima reunión presencial porque entiendo que esto sumaría a la conversación. Tenemos también a Jonathan en la llamada. Gente que indica que este es un tema de interés también para el CPWG. Este es un ejercicio para la creación de capacidades. Es pequeño pero es para informar a la comunidad de cuál es la situación actual, cuáles son las ideas que están existiendo.

Tras esta introducción voy a tomar tres preguntas del chat. Sé que Evin las está registrando diligentemente. Evin, por favor, ¿podría leer las preguntas? Si están dirigidas a un orador en particular le pido por favor que lo mencione. Entiendo que Milton tuvo que irse porque tenía otro compromiso. Nos quedan 10 minutos. Vamos a comenzar con tres preguntas del chat. Voy a reservar tres minutos para la mano que se ha pedido, SK Cyber, para que tenga una oportunidad de comentar o hacer su pregunta, que será respondida fuera de línea.

EVIN ERDOĞDU:

Actualmente tenemos dos preguntas más y un comentario. Voy a leer las dos preguntas primero y luego el comentario. La primera pregunta es de Gangesh. Pregunta: ¿Hasta qué punto la propuesta de soberanía

popular se alinea con el concepto del común global en el derecho internacional o el principio de herencia común? ¿Existe algún potencial de darle un marco a través de estos principios u otros similares en el derecho internacional? La otra pregunta es de Andrei Kolesnikov: ¿Se observa algún aumento del tráfico entre los trabajadores remotos por el COVID-19? La última es de Javier Rua Jovet, quien dice: Algunos estados han amenazado con generar Internet alternativas. Los beneficios de quedarse en la Internet global hacen que tales amenazas suenen huecas y difíciles de concretar. China quiere que compres en eBay y lo hace porque sabe que el sistema funciona. Eso es todo, Joanna. Le devuelvo la palabra.

JOANNA KULESZA:

Veo que Patrik ha levantado la mano. Entiendo que quiere responder la pregunta. Le daré la palabra a Patrik. Si Veni quiere comentar, por favor, levante la mano.

PATRIK FÄLTSTRÖM:

Sí. Así es. Quería responder al menos parcialmente la pregunta. No sé mucho sobre derecho internacional. Para mí es difícil el derecho internacional. Me gustaría que hubiera mayor coordinación entre los legisladores de las distintas jurisdicciones. Muchas leyes en lo que hace a la capacidad de construir Internet y acceso en el mundo están ocultas en las leyes de telecomunicaciones y no forman parte del derecho internacional genuino. Me gustaría que más países, incluyendo Suecia, por ejemplo, incluyeran alguna modificación o

ratificaran la convención sobre el ciberdelito. No creo que el derecho internacional alcance. Creo que la cooperación es internacional.

Con respecto a los puntos de intercambio de Internet, o IX, ha habido un mayor intercambio, más tráfico por el coronavirus. Sabemos que ha habido upgrades en especial en las consolas de juego, en especial en las últimas 48 horas. Habría que esperar tendencias. Necesitamos un mayor tiempo para una conclusión pero lo estamos viendo en las redes sociales, que mucha gente hace más trabajo remoto. Esperemos que la Internet se sostenga.

En lo personal, me pone un poco triste ver que la gente no toma Internet por sentada como el agua o la electricidad. Creo que el agua, la electricidad e Internet deberían ser tan estables como sea necesario para funcionar en todo el mundo. Esto incluye específicamente el tema del agua. El suministro de agua no está garantizado en todo el mundo. Con respecto a la Internet alternativa, es tecnología de contraseñas que es una tecnología en discusión. Es necesario seguir reflexionando. Hablar más. Saber exactamente qué significa, como decía Milton. Tenemos que hablar un poquito más en especial en el contexto del DNSSEC. Gracias.

JOANNA KULESZA:

Gracias, Patrik. No sé si Veni quiere hablar. Patrik habló de coordinación internacional. Sin duda esto es algo que las Naciones Unidas trabajan. No sé si Veni quiere comentar al respecto. De no ser

partes interesadas

así voy a tomar esa mano que hace rato está esperando. SK Cyber tiene la palabra. Adelante con su pregunta o comentario.

SK CYBER: Muchas gracias. Gracias por la presentación. Me preocupa el tema de los estándares técnicos. La necesidad de estándares marco e incluso mejores prácticas en el área de la soberanía técnica. La UIT, Naciones Unidas, en su lista de prioridades hablan de esto. Cómo manejar estos temas desde la ICANN. Segundo, hay estados que han promocionado ataques. Eso está probado. ¿Cómo podemos tener prueba de esto? ¿Cómo podemos educar y desarrollar capacidades en las comunidades, en la gente? Estas son mis principales preocupaciones.

JOANNA KULESZA: Muchas gracias. ¿Estas preguntas son para algún panelista en particular?

SK CYBER: Cualquiera puede responder.

JOANNA KULESZA: Muchísimas gracias. Si me permite recapitular, estamos hablando de ciencia forense cibernética. Estamos hablando de distintos temas que podrían tomar cualquiera de los miembros aquí presentes. ¿Podrían

partes interesadas

levantar la mano? Parece que no tenemos una respuesta específica para usted, señor.

PATRIK FÄLTSTRÖM:

Yo podría ayudar un poquito. Quisiera agregar un comentario. La atribución es importante. En muchas legislaciones, en muchos países, por ejemplo, sé el caso de Suecia, si surge un ataque sobre territorio sueco, por ejemplo, si ocurre que la atribución de ese ataque, y no estoy hablando de un ciberataque, si algo pasa sobre suelo sueco, si ese incidente ha sido generado por otro estado, entonces es un problema de las fuerzas armadas o del ministerio de Defensa. Se ocupan ellos.

Si no ha sido otro estado, es para la policía. La atribución es algo que a menudo es necesario, para empezar para saber quién va a manejar el problema. Como decía, esto no es específico de incidentes cibernéticos. Se aplica a todos los incidentes. Hay mucho trabajo académico, incluido uno en el cual yo participé pero es visto desde el punto de vista de la atribución. Gracias.

JOANNA KULESZA:

Patrik, parece que después de su última frase le perdimos. ¿Ha concluido?

PATRIK FÄLTSTRÖM:

Sí. Eso era todo.

partes interesadas

JOANNA KULESZA: Esto me da tres minutos más. Tengan en cuenta que hay mucho material para leer sobre la atribución de ciberincidentes. Veo la mano de Evin. Adelante, Evin.

EVIN ERDOĞDU: Tenemos una pregunta más, si me permite leerla.

JOANNA KULESZA: Adelante.

EVIN ERDOĞDU: Holly pregunta: “¿Cómo puede manejar una entidad el bloqueo de contenido con DoH/DoT?”

JOANNA KULESZA: No sé si Patrik puede responder porque es una pregunta muy específica y muy técnica.

PATRIK FÄLTSTRÖM: Ayer tuvimos una sesión donde tratamos los detalles de DoH y DoT. En SSAC explicamos esta diferencia que existe entre ambos protocolos y su implementación. Creo que lo importante es que, con una manera diferente de tratar el DNS, tenemos distintas entidades que manejan de manera distinta las queries del DNS. La pregunta es si se pueden

usar las mismas herramientas para el bloqueo que antes y si pueden las mismas entidades ser responsables del bloqueo y de la gestión del bloqueo como antes. Aquí hay grandes interrogantes. Creo que la respuesta es que hay que reevaluarlo. Esto también significa que es necesario reevaluar algunas leyes y algunos casos judiciales también hay que reevaluar. Es una pregunta muy difícil, muy buena. Lo que a mí me pone nervioso en lo personal, esto no es SSAC, es mi opinión personal, yo estoy nervioso porque no exista responsabilidad entre los proveedores de servicios, quienes son los que manejan hoy el resolutor local, que ellos al bloquear ciertos nombres de dominios, no sé si eso alcanza para bloquear el acceso a ciertos contenidos. La única manera real de bloquear el contenido es darlo de baja apropiadamente.

JOANNA KULESZA:

Fantástico el resumen. El rol que tienen los actores individuales en el uso indebido del DNS y las políticas nacionales, esa es la cuestión. Con esto voy a cerrar. Muchísimas gracias a nuestros panelistas. Estoy convencida de que las presentaciones han sido sumamente informativas. Aprendí mucho. Veo en el chat que ha habido muchos participantes. Gracias a nuestros intérpretes, al personal y apoyo técnico. Gracias a todos los que se han acercado a la llamada en horarios tan extraños. A medida que continúe el día, no duden en enviarme preguntas o dudas. Aquí estamos disponibles para preguntas o comentarios. Disfruten del resto del día o de la noche. Gracias. Adiós.

partes interesadas

ES

[FIN DE LA TRANSCRIPCIÓN]

