MONTREAL – Uso indebido del DNS
Miércoles, 6 de noviembre de 2019 – 10:30 a 12:00 EDT
ICANN66 | Montreal, Canadá

BRUCE TONKIN: Por favor, tomen asiento. Vamos a iniciar esta sesión. Sé que hay mucha gente interesada en este tema. Queremos hacer el mejor uso del tiempo empezando esta mañana. Hoy es miércoles pero para muchos de nosotros parece que hace como dos semanas que estamos aquí. El objetivo de esta sesión es reunir muchos de los debates que han estado ocurriendo en estos días en cuanto al tema del uso indebido o abuso del DNS.

El contexto de este tema es que hay unas cuantas referencias al abuso del DNS y a la recolección de información y a los acuerdos de registro y registrador. El tema fue considerado por el equipo de revisión de competencia, elección del consumidor y confianza del consumidor. Tenemos algunas recomendaciones. La organización de la ICANN también ha estado recolectando y publicando datos y estadísticas sobre los nombres de dominio que han sido reportados en los distintos registros y dominios de primer nivel vinculados con el uso indebido del DNS. También tenemos algunas prácticas que quizá no son muy conocidas. Desde el punto de vista de la comunidad creo que no queda claro cuáles son los requisitos para los registros y registradores. Tampoco queda claro qué es lo que sucede después de que se hace un reporte en particular del abuso del DNS.

El objetivo de esta sesión es darles una introducción a este tema. Tenemos un panel de expertos de la comunidad de la ICANN que van a comentar sobre estos asuntos. Luego quiero escuchar lo que tiene para decir la audiencia y permitir que hagan preguntas o sugerencias sobre cómo avanzamos en este sentido y básicamente cómo podemos proteger al usuario final del uso indebido del DNS.

Vamos a comenzar con una introducción muy rápida de los miembros del panel. Vamos a presentarlos. Pueden presentarse cada uno, decir su nombre, a qué estructura de la ICANN pertenecen y por qué les parece que este es un tema importante. Luego vamos a dar una breve descripción del tema. Se trata de una versión más breve de un seminario web que se hizo recientemente. Empezamos por la derecha. Gabriel.

GABRIEL ANDREWS: Hola. Mi nombre es Gabriel Andrews. Estoy aquí en representación del grupo de trabajo de seguridad pública, PSWG. Investigo el ciberdelito en Estados Unidos en mi trabajo diario.

FARZANEH BADII: Hola. Soy Farzaneh Badii. Estoy aquí en representación del grupo de partes interesadas no comerciales y trabajo en la Escuela de Derecho de Yale.

BRIAN CIMBOLIC: Soy Brian Cimbolic. Soy del grupo de partes interesadas de registro y trabajo en un registro que es el operador de .ORG.

GRAEME BUNTON: Soy Graeme. Trabajo para Tucows, un registrador canadiense. Estoy aquí en representación del grupo de partes interesadas de registro.

MASON COLE: Hola. Soy Mason, del estudio jurídico Perkins Coie y represente a la unidad constitutiva de negocios.

JEFF BEDSER: Soy Jeff. Estoy aquí en representación del comité de seguridad y estabilidad.

BRUCE TONKIN: Vamos a dar una versión más breve del seminario web que presentamos hace un par de semanas.

GABRIEL ANDREWS: Buenos días. Vamos a testear. Sé que hay muchas discusiones que están ocurriendo en cuanto al abuso del DNS y el deseo de algunos de encontrar una definición coherente. Desde la perspectiva del grupo de trabajo de políticas, ya hay muy buenos intentos de tratar de definir el espacio y, en particular, el asesoramiento que emitió el GAC, que lo pueden ver, es del año 2013. Lo pueden ver aquí en la pantalla. No lo voy a leer pero estas son algunas recomendaciones iniciales en base a

lo que nosotros consideramos que es el abuso del DNS. Tiene que ver con las obligaciones de los contratos que están en lo que nosotros denominamos especificación 11(3)(b). Creemos que es lo que los registradores y partes contratadas deben considerar como la responsabilidad para el abuso que ocurre online en este ecosistema de Internet.

Desde ese momento sabemos que ha habido muchas conversaciones sobre lo que se ha planteado, lo que han planteado las partes para adaptar estos entendimientos del abuso. Sabemos que los informes del uso indebido están tratando de cuantificar lo que hemos visto. La cuantificación es buena. Puede haber algunas metodologías que hay que mejorar.

El marco para tratar el abuso fue un esfuerzo colaborativo de algunas partes contratadas, algunas dentro de la unidad constitutiva de negocios, para ir más allá e incluso descubrir cuáles son algunos lugares donde el abuso puede y debe ser tratado. Agradecemos esos esfuerzos de colaborar y de tratar de generar soluciones.

Dicho esto, lo que quiero es que no perdamos de vista lo que efectivamente está ocurriendo en el mundo real y lo que nosotros podemos tratar aquí, que es el ciberdelito en el mundo real. Les voy a dar algunas imágenes para que todos puedan ver pero se trata entonces de ejemplos de la vida real de uso indebido que está ocurriendo ahora. Encontrar una definición mañana va a ser complicado. No debemos inhibir las acciones que podemos hacer hoy. Sería muy bueno tratar el delito que está ocurriendo ahora. Vamos a

ver tres ejemplos de lo que vemos en el mundo real. El primero es el compromiso de email comercial. Vemos que esto está siendo muy prolífico y a la vez simple. Una persona está mintiendo a la gente para que le envíe dinero. Este es un email real que fue utilizado para solicitar, creo, 250.000 dólares de una víctima no sospechada. Los fondos fueron protegidos.

Los dominios que ustedes ven aquí son todos reales. No se pidió permiso a los malos. Protegimos algunos de los nombres. Vemos que este es un esquema muy simple en el que no se necesita mucha habilidad. Es un cambio de caracteres con las dos direcciones. En vez de flyjetedge, pusieron flyietedge. El cambio en un solo carácter en un dominio representa un 80% de posibilidades de que un email sea BEC. Este esquema ha puesto en riesgo presupuestos de universidades. Representa 26.000 millones de dólares desde que lo comenzamos a rastrear en el 2013. Cada vez vemos más de todos estos esquemas combinados. Ha impactado en 177 naciones en el mundo. Me dicen que hay 195. No sé cuáles son las otras 18.

La segunda categoría. Esta es una diapositiva confusa pero quiero hablar de los botnets y un término que ustedes ya conocen que es algoritmos de generación de dominio. Es un poco confuso pero los botnets son los que infectan muchas computadoras. Quizá cuando ustedes ven que la computadora está muy lenta, a lo mejor tienen un botnet. Este mal actor hay que controlarlo y una de las formas en las que se hace es utilizando un algoritmo de generación de dominio que genera caracteres para la registración de dominio. Eso se ve en lo que está marcado en rojo. Son dominios que son generados por un

algoritmo. Son utilizados para controlar todas las máquinas infectadas en el mundo. Lo que es interesante es que los DGA, estos dominios, son utilizados por las personas malas para el spam también. Hay muchos más usos ilegítimos de dominios aleatorios generados por los DGA. Quiero invitarlos a que hablen conmigo y me cuente cuáles son los objetivos porque a veces veo que en el mundo real hay registradores que hacen DGA como parte del proceso de registro.

Finalmente la tercera categoría. El ransomware, además de los esquemas que discutí y que mencioné antes, es uno de los que más impacto tiene y de los que más vemos en el mundo. Si ustedes son como yo y tienen una conferencia de la ICANN y se levantan a la mañana, pueden encender seguramente las noticias y el lunes podrían haber visto esto. Esto es Nunavut. Me dicen que queda como a tres horas de avión de aquí. Es un pequeño pueblo. Como ven en el recuadro blanco, ellos fueron atacados por varias cadenas de ransomware. El ransomware es un malware que ataca la computadora, que encripta todos los archivos y nosotros no podemos acceder a ellos. No podemos ver qué es lo que tenemos en la computadora y va mucho más allá. Ataca todas las computadoras de la red y te cobran un rescate. Quizá uno puede obtener el acceso de nuevo a la computadora y quizá no. Este ataque en particular, aquí dice que esto provino de un email de spam, eso es lo que dice la foto, ¿ustedes creen que en Nunavut, cuando se preparan para el invierno, ustedes creen que les importa una definición exacta del abuso del DNS, a la gente que vive en Nunavut?

BRUCE TONKIN: Brian, si pudieras darnos una actualización sobre los registros y registradores.

BRIAN CIMBOLIC: Vamos a hablar tanto del registro como del registrador, de las obligaciones de ambos.

GRAEME BUNTON: Muy bien. Vamos a empezar con el requisito contractual del registrador, que es bastante directo. Hay tres disposiciones en nuestro contrato que se ocupan del uso indebido. El registrador debe mantener el contacto del uso indebido y debe tomar medidas razonables para investigar y responder apropiadamente al uso indebido. Hay que tener un contacto de aplicación de la ley las 24 horas y también se deben publicar los procedimientos para el tratamiento del uso indebido.

BRIAN CIMBOLIC: De la parte de los registradores, todo está contenido en la especificación 11(3)(b). Esto requiere que los registros realicen un análisis técnico periódicamente para buscar amenazas de seguridad como phishing, malware y botnets. También mantener informes estadísticos sobre las amenazas identificadas y cuáles son las acciones que se tomaron como resultado. Es importante reconocer al tener estas conversaciones qué es lo que un registro y un registrador pueden y no pueden hacer. Nosotros tenemos una opción práctica para tratar el abuso y esto es la suspensión de los nombres de dominio. Esto se

hace del lado de los registros y técnicamente nosotros podríamos redireccionar el dominio que se puede realizar y requiere una orden judicial. No puede ser dado de baja porque se puede re-registrar y se puede usar para el mismo objetivo. La suspensión del nombre de dominio, no permitir que el contenido o el mail se utilice, es quizá la herramienta más efectiva y quizá la única que un registrador tiene para tratar el abuso del DNS. Es importante pensar y tener en cuenta que actuamos a nivel del nombre de dominio. Si hay alguien que se quejó, nosotros quizá no tenemos la posibilidad de actuar a nivel del sitio web. Este proveedor de Internet puede remover el contenido, los registros y los registradores no, porque solamente actúan a nivel del nombre de dominio.

GRAEME BUNTON: A nivel del nombre de dominio, si es un tema de email, también es problemático porque no tenemos la posibilidad de impactar las direcciones de email a ese nivel de dominio. En cuanto a los nombres de dominio registrados, especialmente los DGA, no creo que muchos registradores tengan herramientas para evitar las registraciones que todavía no existen. Es un problema interesante ese para nosotros.

BRIAN CIMBOLIC: Los DGA, algoritmos de generación de dominios, son un área en la que los registros trabajan muy de cerca con el grupo de trabajo de seguridad y distintos organismos de aplicación de la ley. Un organismo como este va a descubrir cuál es este algoritmo DGA y va a trabajar con

los registros para que podamos registrar o bloquear un dominio en particular antes de que se pueda utilizar nuevamente.

Estos dos puntos son importantes. Lo que estamos obligados a hacer contractualmente y también una vez que hemos identificado el uso indebido, qué es lo que podemos hacer desde la perspectiva técnica. Esto es la línea de base pero es muy importante reconocer que los registros y los registradores van más allá rutinariamente de lo que están obligados contractualmente. Es decir, cada uno de ellos tiene una política de uso que puede cubrir el contenido de un sitio web. Como ha mencionado Dev, también hay varios registros y registradores que se reúnen y que publican un marco para tratar el uso indebido. Es importante decir que este no es un documento de los registros o los registradores sino una colección de prácticas recomendadas que registros y registradores responsables deben adoptar.

Las partes contratadas trabajan con notificadores en ciertos escenarios. Nosotros trabajamos por ejemplo con la Internet Watch Foundation para tratar de por ejemplo identificar material que tenga que ver con el abuso infantil. También muchos registros y registradores tienen un programa similar. También hay programas de incentivo que premian la buena conducta. PIR, tenemos el índice de rendimiento que analiza las métricas de uso indebido o de renovación de los registradores. Estos son puntos que miden la calidad de los nombres de dominio y se les dan incentivos financieros o de precios por tener registraciones de buena calidad. Esto es lo que se considera

en el uso indebido de los nombres de dominio. Lo mismo, por ejemplo, se usa con los IDN. Hay un operador que tiene un programa similar.

GRAEME BUNTON: Hay otro punto a tener en cuenta también. Probablemente los registradores, no voy a hablar por los registros pero los registradores son en realidad malos en autopromocionarse con respecto al trabajo que hacen en el espacio. En realidad los registradores toman acciones todos los días en materia de la seguridad del DNS. En Tucows, por ejemplo, nosotros sacamos unos 100 dominios por uso indebido al día. Nosotros no lo publicitamos pero les puedo garantizar que esto se ve en toda la industria. Hay mucha actividad que se lleva a cabo y es muy importante. En realidad no somos buenos en comunicar a la gente cuán importante es todo esto.

Con respecto a lo que dijo Gabriel, una definición adecuada del uso indebido del DNS, por eso se creó un marco. Queremos llegar a la acción porque podríamos debatir la definición eternamente pero queremos capturar lo que están haciendo los registros y registradores y a partir de ese punto seguir avanzando. Es decir, abordar las cuestiones en lugar de estar debatiéndolas durante mucho tiempo o eternamente.

BRIAN CIMBOLIC: En realidad este es un debate académico. Los registros y registradores sí actúan. Tienen acciones continuas al respecto. En el PIR lo que hacemos es publicar estadísticas de uso indebido y en el tercer

trimestre del 2019 suspendimos aproximadamente unos 28.000 nombres de dominio como resultado de una identificación de uso indebido. Colectivamente ya empezamos a hablar de qué hay que hacer y cuáles son los resultados.

BRUCE TONKIN: Creo que es importante tenerlo en cuenta con un registro y registrante de nuevos gTLD pero también tenemos que tomar esta diapositiva y seguir participando en los debates que tienen los operadores de cc como por ejemplo .EU. Es decir, hay una serie de cc que tienen programas financieros e incentivos con los cuales están trabajando. Muchos también trabajan con otros notificadores de confianza. Hay cuestiones que tienen que ver con los nombres genéricos o de alto nivel y eso también es abordado por los códigos de país.

Algunos de los oradores van a hablar de la definición del uso indebido del DNS. Es una definición que Gabriel dio en su primera diapositiva. Por ejemplo, el phishing, el malware y los botnets. Son diferentes formas de acceder al uso indebido. En los reportes de la ICANN hablan del spam. El spam tiene una forma distinta. A veces el spam tiene fines comerciales nada más. Se envía un correo a la mayor cantidad de personas posibles para tratar de vender un producto. Por ejemplo para tratar de que alguien se suscriba. Muchas veces hay muchas regulaciones en los países con respecto al spam. El spam también es un mecanismo de iniciar un ataque de phishing. Esto se hace a través de un correo electrónico que se envía a una cantidad masiva de personas.

Una de las aclaraciones que aparece en el documento de los registradores y registros es que están tomando acción con respecto al uso del spam para no permitir o para no dar lugar al farming, al phishing y a los malware y botnets. Aquí se está hablando de algunas definiciones generales pero la idea es poder acotarlas porque son muy amplias pero también queríamos saber cuál piensan ustedes que tendría que ser la definición del uso indebido del DNS. Farzaneh, ¿cuál es su punto de vista con respecto a la definición del uso indebido del DNS?

FARZANEH BADII: En la NCSG nosotros pensamos que el uso indebido del DNS se tiene que definir de una manera técnica. La ICANN no debería participar con los programas no técnicos que luchan contra el uso indebido del DNS. Lo que a mí me preocupa es que en realidad sí tenemos una definición. La definición no debería ser perfecta pero sí tendría que estar limitada y ser técnica porque no podemos pelear con todas las fuentes que existen del uso indebido del DNS y que tienen lugar en todo el mundo simplemente porque el DNS se utilizó en un cierto tipo de delito. Tenemos que analizar y ver si esto está dentro del ámbito de la ICANN. Realmente luchar contra esa acción, contra ese uso indebido.

Hasta el momento no he visto nada en ningún documento que me lleve a alguna definición o a algún uso indebido del DNS que sea innovador o distinto más allá de lo que ya han enumerado los registros y registradores. Además del acuerdo, no he visto tampoco ningún otro tipo de documento técnico o de uso indebido del DNS técnico que no

se haya considerado. Creo que el problema que tenemos no está realmente en la definición sino que el problema que tenemos es que tenemos diferentes soluciones parciales por un lado y por el otro pero no tenemos un mecanismo de gobernanza coherente que nos permita aplicarlo. Tenemos políticas, las hacemos cumplir bajo la resolución de disputas, por ejemplo. Básicamente ese sería mi comentario.

BRUCE TONKIN: Gracias. Mason.

MASON COLE: Yo quiero hablar sobre los registros y registradores en cuanto a esta cuestión de ir en pos de las acciones. Creo que podemos dedicar mucho tiempo a lo que sería una definición del uso indebido del DNS y mientras tanto el uso indebido se lleva a cabo, se hace un uso indebido del DNS. No solo tenemos que focalizarnos en una definición.

Con respecto a su pregunta, Bruce, el BC publicó una declaración sobre el uso indebido del DNS y creemos que una definición del DNS es en realidad una acción que podría causar un daño sustantivo y que podría incluso ir en detrimento de un propósito legítimo. Además, el recuerdo de registro reciente captura de alguna manera una de las definiciones técnicas que tienen que ver por ejemplo con distribuir el malware, operar botnets de manera negativa, la piratería, el phishing o, por ejemplo, infringir fraudulentamente los derechos de marca o derechos de propiedad intelectual.

La definición de uso indebido también se citó en los compromisos de interés público y en el acuerdo de registro. Durante la transición, la BC hizo lo que pudo con la junta directiva para poder proteger estos PIC. Al comienzo de esta semana escuchamos que hay cierta dificultad por parte de la ICANN para hacer cumplir estas cuestiones. Buscamos seguir debatiendo el tema con la comunidad para ver de qué manera podemos mejorar.

BRUCE TONKIN: Gracias, Mason. ¿Jeff?

JEFF BEDSER: Gracias, Bruce. Esto es simplemente una divulgación. Yo estoy muy gustoso de saber lo que están haciendo los registros y de ver todo. Mi compañía también, por ejemplo, lleva adelante un sistema de informe para la actividad del uso indebido o DAAR. A mí me gustaría abrir el debate para definir lo que es el abuso o el uso indebido. A veces tenemos en cuenta cuando hablamos de uso indebido que hay una víctima que sufre daños financieros o algún otro tipo de problema. Tratar de limitar el uso indebido de manera limitada y decir: “Este es el uso indebido sobre el cual nos vamos a hacer responsables”, es un poco complicado. Es una línea muy delgada que tenemos que tener en cuenta porque tenemos un ecosistema que cuenta con muchísimos operadores de registro, más de 200 o 250 operadores de registro y aproximadamente 2.000 registradores.

La pregunta sería cuántas situaciones podrían darse. Podemos pensar en miles. Es decir, tenemos que continuar hablando de la victimización. Son situaciones en las cuales si no se toma acción, la gente va a seguir siendo víctima de estas otras acciones indebidas. También creo que cuando uno va a nivel de registro y toma acción, hay que decir: "Tenemos que dejar de hacer esto para evitar la victimización pero también tenemos el uso indebido y tenemos que tomar una especie de acción a nivel de registro y también a nivel de la empresa que hace el hosting". Si reunimos todas estas condiciones, esto nos va a ayudar a comprender cuáles son los problemas, las pérdidas y el tema de la victimización.

BRUCE TONKIN: Graeme.

GRAEME BUNTON: Una breve respuesta dentro de la definición del marco. No quiero seguir discutiendo el tema de la definición pero yo escuché a muchas personas esta semana que decían que estábamos avanzando mucho, que era un error. Otros decían que no hemos llegado lo suficientemente cerca para lograr una definición. Para mí, dentro del terreno clásico de la ICANN, quiere decir que ya estamos ahí prácticamente. Con respecto a la declaración del BC, qué es lo que significa la legitimidad. No entiendo, por ejemplo, cómo se puede definir algo legítimo o no. para mí no es una definición que nos permita seguir tomando acción.

BRUCE TONKIN: Quiero abordar otro tema que se mencionó también anteriormente que es el tema de la proporcionalidad. Qué se hace cuando no todo lo que está relacionado con nombres de dominio causa un problema. Por ejemplo, cuando hay una dirección de correo electrónico de una persona en gmail.com o, por ejemplo, si hay un contenido que es malicioso en YouTube, mucha gente va a pensar que no es justo remover el contenido de youtube.com porque ese es el contenido que le pertenece a alguien más. Con respecto al tema de la proporcionalidad, hay que analizar la solución, hay que ver qué dicen los registros y los registradores o si van a hablar con los registrantes.

Al principio de las presentaciones había una solicitud específica para los registradores para que brindaran un contacto para el caso de uso indebido pero esa información cada vez es menos importante para los proveedores de hosting o para los registratarios. Eso solía estar también en el servicio del WHOIS. Es decir, brindaba el dato técnico o dato del contacto técnico o el dato de la compañía. Se daban los detalles pero esa información está gradualmente desapareciendo, probablemente en respuesta a las leyes de privacidad que ahora existen. Cuando ustedes dicen que el registrador tiene que hacer algo, tiene que ir, por ejemplo, a la compañía de hosting, cómo sugieren ustedes que la gente llegue al contexto adecuado para poder abordar estas acciones. Cómo se enfrentan con estos problemas.

BRIAN CIMBOLIC: A ver, siempre hay una pregunta o una cuestión de proporcionalidad cuando se habla de utilizar el sistema de nombres de dominio para, por ejemplo, abordar problemas del uso indebido del contenido web. Dicho esto, creo que este no es el final de la discusión y el final de la ecuación, todo lo contrario. Hay que medir los daños. Muchas veces es desproporcionado hablar del sistema de nombres de dominio para abordar una cuestión de un sitio web pero cuestiones como por ejemplo material de abuso infantil, que causan daño, en esos casos creo que ese análisis de ver la proporcionalidad, sopesar el daño que se causa, es el análisis que tenemos que tomar muy seriamente en cuenta. Sí, hay que trabajar con los proveedores. Hay que trabajar de manera ascendente para poder lograr la solución pero también hay otras instancias en las que tendríamos que tomar acción.

BRUCE TONKIN: La pregunta específica que quiero hacer es la siguiente. Cuando se llega al punto donde ustedes piensan que no hay que tomar acción y que tiene que ser el proveedor del hosting o el registrador el que lo tiene que hacer, cómo reacciona la comunidad, qué hace la comunidad al respecto, cuáles son las herramientas disponibles que tienen, qué pasa, cuál es el próximo paso.

GRAEME BUNTON: Jeff seguramente está en una mejor posición para responder. A veces hay una especie de opacidad entre el dominio y el proveedor del alojamiento. Yo no soy experto en ciberseguridad pero seguramente hay un valor en tener una conversación sobre cómo hacer que esto sea

más transparente. Una de las herramientas que va a ser útil para hacer esto sería esa. Quizá Jeff la conozca.

JEFF BEDSER: Se necesita investigación y también ha habido muchos cambios en los últimos años. Por ejemplo, si ustedes utilizan un proveedor de Internet como Cloudflare, la forma en que el sistema funciona es que oculta el alojamiento. Hay que contactarlos a ellos para probar quién es la empresa de alojamiento para poder contactarla. Si no conocen el término bulletproof hosting, esto significa que a uno lo protegen de ataques de denegación de servicio. Este alojamiento antibalas simplemente implica que a uno le van a ignorar los emails y vamos a tener que tomar alguna medida. En ese proceso, cuántos días pasan entre el primer contacto, el segundo contacto, el tercer contacto antes de que uno pueda realmente tomar una medida de algún tipo. Creo que Graeme tiene razón. Si bien podemos ser responsables por ese contacto y ese problema, tiene que haber un método que haga que sea más fácil encontrarlos y que puedan ser contactados.

GABRIEL ANDREWS: Cuando estamos hablando de las brechas y de los informes del uso indebido debemos tener una conversación honesta sobre lo que sucede cuando los buenos informes tienen que ver también con el cumplimiento. Cuando nos dicen que este informe indica que se usó para una actividad mala mientras que este otro dice que vamos a actuar en este sentido y, al mismo tiempo, vamos a tomar registraciones adicionales quizá de los mismos registratarios de

nuevos dominios que fueron ya reportados por abuso ante la ICANN. ICANN lo vuelve a presentar y permite que el ciclo se perpetúe. Ya sea que haya o no un potencial para hacer más, sin tener un rastreo obligatorio de cuántas quejas de abuso hubo en un solo registrador o registratario, tiene que haber algún tipo de metodología de tres tipos para rastrear el abuso repetido, para que no haya un feedback de informe que se resolvió ad infinitum.

BRUCE TONKIN: Lo que estoy escuchando de estos oradores es que no tenemos una buena solución ya sea que se trate de contactar a la empresa de hosting o al usuario final. Como dijo Jeff, hay muchos servicios que están diseñados para proteger contra los ataques de denegación de servicio. Hay distintas capas de infraestructura de Internet que típicamente se encuentran entre el registro y el usuario final. Hay un registro, hay un registrador que presenta las cuestiones del registro, los registradores al revendedor, luego el revendedor puede utilizar un proveedor de DNS que puede utilizar un firewall de aplicación web que puede utilizar una empresa de servicio de alojamiento diferente.

Estamos hablando de hasta 5 o 10 organizaciones involucradas en la provisión del servicio cuando vemos que estamos tipeando una URL en un navegador. Tomar una medida es cada vez más difícil porque a nivel de los datos de contacto, eso no está disponible. Lo único que tenemos son los datos de contacto para el registrador y los registradores quizá puedan contribuir un poco más y dar mejores formas de contactar a los revendedores o a las empresas de

alojamiento que están asociadas con la registración. Perdón, Farzaneh.

FARZANEH BADII: Cuando hablamos del contenido no estamos hablando de nada que esté vinculado a la ICANN o que la ICANN tenga que tomar alguna medida. Para aquellos que no lo saben, en nuestros estatutos hay disposiciones que evitan que ICANN se ocupe de la regulación del contenido y mezclar las capas del contenido con las capas técnicas es algo muy riesgoso. Creo que hay que dejar muy en claro cuando estamos hablando de regulación del contenido.

En cuanto a los registros y registradores y cuáles son las medidas que toman por fuera de la ICANN, creo que deberían poder tomar medidas. Sin embargo, si quieren hacer que sea más legítimo, quizá puedan ser más transparentes sobre las políticas que tienen y sobre la implementación de aquellas políticas. También tener un proceso para que si por error ellos dieron de baja algo, el usuario pueda disputar eso. Es decir, objetarlo.

BRUCE TONKIN: Esa es una buena pregunta, Farzaneh. Cuáles son los derechos de apelación. Quizá el registro o el registrador pueda hablar de eso. Cómo hace una persona que se borró su nombre, qué puede hacer.

BRIAN CIMBOLIC: Es una buena pregunta. Estamos ahora en el proceso de formalizar un mecanismo de apelaciones para el PIR. Va a haber un proceso formal a través del cual el registratario cuyo dominio fue suspendido como resultado de una política antiabuso, esto va a poder ser revisado por un tercero. Mientras tanto, una persona, que abusaron de su email, va a poder presentar un reclamo de que hubo un caso. Vamos a poder identificar el caso antes de que se tome una medida. Es decir, si un registratario viene y de nuevo tiene que ser un reclamo creíble de que su dominio estaba comprometido, en ese caso podemos revertir la suspensión, lo cual es otro beneficio de suspensión versus borrado, porque lo podemos remover en cualquier momento.

BRUCE TONKIN: Una de las cosas que surgieron en el reporte son un par de sugerencias. Una de esas sugerencias es que ICANN indica que esto debe ocurrir a nivel de la registración. Hay que hacer un análisis profundo. Otra sugerencia es que los registros y registradores deben buscar incentivos financieros diferentes para incentivar la buena conducta. Vamos a ver qué tienen los otros panelistas para decir.

GABRIEL ANDREWS: Lo que yo quiero decir es que la acción es la que está tomando la PIR y requiere de análisis. Cuando estamos hablando de tener un registro que incentive a todos los registradores y les diga: “Si ustedes toman todos estas medidas para combatir el abuso en su plataforma, ustedes van a poder tener un descuento en la registración”. Esto vale la pena explorarlo porque en última instancia debemos recordar que los malos

están incentivando la mala conducta. Ellos están comprando dominios y nosotros debemos establecer alguna política de garrote y zanahoria para que aquel que es inmoral considere hacer lo correcto. Un paso más incluso. Podemos considerar qué podemos hacer para alentar a los registros a alentar a los registradores.

Pensamiento final. Para cada zanahoria puede haber un garrote. Creo que estamos en una curva en términos de conducta de abuso. Cuáles son los garrotes. Cuáles son los desincentivos que se deben emplear para aquellas conductas inadecuadas. Cómo podemos cuantificar quiénes son los malos, quiénes son los buenos. Cómo puede haber una luz para que algunos puedan nutrirse de eso y otros puedan observar qué es lo que ocurre.

GRAEME BUNTON: Esta es una idea nueva, esta de los incentivos. Por lo menos nueva para mí. Creo que hay que tener mucho cuidado en cuanto a cómo lo definimos, cuáles son esas métricas en las cuales se están basando estos programas. Los registradores en general no tienen mucho margen en su negocio y eso es muy interesante quizá para los registradores en general. Quizá se pueda explorar un poco más.

MASON COLE: Yo estaba del lado de las partes contratadas en la mesa. Los incentivos de costo y los incentivos financieros pueden ser una solución atractiva. Yo aplaudiría esta idea. Creo que sería algo inteligente de hacer. También creo que este sería un buen momento para revisar los

contratos y ver si la mejor redacción de los contratos puede tener un impacto en el uso indebido del DNS porque lo que aprendimos en esta última semana es que los contratos no son tan sólidos como creíamos y deberíamos quizá examinar si hay una oportunidad de fortalecerlos y de darle a la ICANN una mejor herramienta para tratar el uso indebido.

BRUCE TONKIN: Lo que yo observo con los contratos es que están muy cerca del lado de los informes. Los registros requieren que se recolecten estadísticas y que se envíen a registratarios, que se tenga en cuenta el contacto, que se hagan investigaciones. Quizá no queda claro lo que sucede con los informes del abuso. Esto quizá está peor expresado en los acuerdos de registro y registradores y podemos mejorar la redacción de esos contratos. ¿Hay alguna otra sugerencia que el panel quiera hacer sobre las cuestiones prácticas que la comunidad o la organización puede hacer?

BRIAN CIMBOLIC: Quería hablar del incentivo. Con nuestro programa de QPI vimos registradores que no están recibiendo un incentivo y que típicamente no fueron agresivos en el uso indebido. Es decir, vienen y nos dicen: “Nosotros no calificamos. Cómo podemos mejorar” y está impulsado por la finanza, lo cual está muy bien pero decir que una conducta puede tener una buena escala implica que debemos incentivar para tener un mejor espacio financieramente y ese espacio lo vamos a ir encontrando.

BRUCE TONKIN: Del lado financiero hay cargos que cobra ICANN, otros que carga el registrador, otros que cobra el revendedor. Podría esto convertirse en una especie de cadena.

FARZANEH BADII: Creo que la discusión de los incentivos, debemos tener mucho cuidado cuando hablamos de esos incentivos y qué es lo que estamos incentivando. Si incentivamos que los registradores retiren más contenido, quizá podrían ser extremadamente celosos en ese sentido y ser injustos con los registratarios. Nosotros estamos muy orientados al resultado. Estamos diciendo: "Vamos a bajar 2.000 dominios", etc. Creo que tenemos que estar más orientados hacia el proceso. Tenemos mecanismos de reversión, etc. Podemos hacer algo por el uso indebido cuando sucede. Creo que esto debe ser más una meta. Para hablar un poco más de la cuestión ambiental, el DNS se utiliza para que estemos conectados por Internet y nos trae prosperidad a la vida todos los días. No se usa solamente para los delitos sino que trae más prosperidad que miseria. Eso es importante de mencionar.

BRUCE TONKIN: Hay que recordar que Internet en general sigue siendo una fuerza para el bien.

BRIAN CIMBOLIC: Para clarificar, yo estaba hablando específicamente del abuso del DNS, no del contenido de los sitios web. En los programas en los que nosotros trabajamos, todavía seguimos hablando sobre una pequeña cantidad comparada con el número general de dominios. En el tercer trimestre hemos suspendido a 28.675 dominios. Es un pequeño número. Lo bueno es que la mayoría están vinculados a CSAM. Tenemos más de 1.100 referencias de una fundación de Internet, lo cual quiere decir que estamos teniendo remediación. No tenemos que actuar a nivel de los nombres de dominio. Estamos tratando de que el problema se resuelva. Si el contenido viene en pequeña cantidad, hay un subconjunto mucho más adecuado para el abuso del DNS.

BRUCE TONKIN: Para aquellos que no lo sepan, CSAM tiene que ver con el abuso infantil.

GABRIEL ANDREWS: Farzi, creo que su comentario en cuanto a los procesos es muy bueno porque sí, hay mucho que se puede hacer y yo no quiero mencionar ciertas buenas prácticas que están dentro del espacio del ccTLD. Algunos de ustedes quizá vieron esto en conversaciones anteriores pero nosotros lo que vimos es que su idea en particular es que ellos tienen procesos por los cuales analizan la registración de los nombres de dominio y tratan de bloquear a esos dominios que se parecen a un mail. Un bad actor puede controlar un dominio que se parece mucho más al de la víctima. Esto es algo que se puede hacer como proceso a nivel del registrador. Eso se está haciendo por algunos pero hay un

proceso adicional con el cual utilizan informes anteriores de abuso como un mecanismo de correlación para identificar el abuso en tiempo real.

El mejor predictor de la conducta futura es el pasado. Esos esfuerzos son algo que se debe aplicar en la medida en que podemos incentivarlos y creo que tiene mucho sentido incentivarlos. De hecho, hay algo que está por detrás de esto.

BRUCE TONKIN: Graeme.

GRAEME BUNTON: Gracias. Brevemente quiero agradecer a Farzi por el comentario porque es muy importante especialmente para investigar los incentivos, que uno no lo puede hacer en un vacío. Hay que tener un mecanismo de apelación y transparencia. Es un proceso robusto el que se necesita para que no se torne problemático.

JEFF BEDSER: Creo que uno de los incentivos primarios tiene que venir de la política de la ICANN. Es un diferenciador del mercado y tenemos puntos de vista asociados. Como dijo Graeme, no hacemos lo suficiente para poder abordar el trabajo. La diferenciación de lo que están haciendo también tiene que ayudar a los clientes porque hay mucha gente que no participa en la comunidad en la ICANN pero sí está en el mismo

negocio. El incentivo podría ser hacer las cosas bien. Ese sería también un premio en sí mismo.

BRUCE TONKIN: Estamos a mitad de camino. Seguramente habrá preguntas. Vamos a comenzar con la lista de oradores.

MARK SEIDEN: Yo tengo una pregunta que quizá nos lleve a saber que estamos en el lugar incorrecto para poder implementarlo. Hay gente que tiene visibilidad sobre el tema del contenido y esto no solamente implica a los proveedores y a las empresas antivirus. Les pido que hagan lo imposible para poder hacer investigación sobre estos informes. Nosotros no tenemos acceso a esos informes y en muchas ocasiones no podemos ni siquiera reproducir los problemas que se informan. Yo los insto a que por favor traten de comprender qué es lo que sucedió, qué es lo que sucede y que no inventen sistemas que sean tan defectuosos y que causen más problemas.

Lo que tenemos que hacer es no entrenar al adversario. Un ejemplo de esto sería la generación o el algoritmo de generación de nombres de dominio. Es decir, esto permitiría evitar que se registren nombres de dominio en la DGA pero también puede causar un problema financiero. Les pido que por favor tomen en cuenta esto. Que no entrenen al adversario o bien que cambien los DGA.

BRUCE TONKIN: Elliot.

ELLIOT NOSS: Elliot Noss, de Tucows. Estuvimos hablando durante unos 45 o 50 minutos y durante más de 20 años sobre este tema. Se ha avanzado mucho. Ahora se ve que hay seis panelistas con seis puntos de vista y todos están en acuerdo. Hay una línea a tener en cuenta que creo que es la línea más importante a tener en cuenta y que tiene que ver con avanzar en el 2019 y en el 2020.

Esto es lo que dijo Mason. Cumplimiento tiene, por ejemplo, problemas para hacer cumplir los PIC. Desde que comenzó este panel me sorprendió. Gabriel dio tres ejemplos muy interesantes sobre el uso indebido del DNS. Cada uno de estos ejemplos está ocasionado por registradores responsables. Ya verificamos los casos, ya verificamos con cumplimiento contractual. Ahora nos encontramos en la época de tener buenos registradores versus malos registradores. Gente que es buena y gente que no. Me cansé de todo esto. Me cansé de haberlo visto tantos años, de estar hablándolo en tantos foros. Tomemos acción.

El miembro más importante de este panel, que podría contribuir a seguir avanzando, no está en el panel. Este es Jamie o John Jeffrey o ambos, porque van a poder explicar por qué el cumplimiento contractual no puede hacer cumplir estas cuestiones y por qué está dentro de los cuatro puntos del contrato existente. Yo me quiero solidarizar con ellos y con esa postura y creo que también tenemos que poner todos los esfuerzos de la comunidad juntos porque tenemos

que estar simplemente de acuerdo. Para bien o para mal, nos tenemos que poner de acuerdo. Es ahí donde tenemos que poner todo nuestro esfuerzo y energía en el corto plazo. Tenemos un marco que nos dio la comunidad y quiero saber, como dije ayer brevemente, en la reunión conjunta con la junta directiva y las partes contratadas, que no es una cuestión de quiénes están y quiénes no. Hablamos de los incentivos. Hoy por hoy existen incentivos financieros claros que fueron propuestos por los registros con buena intención pero que de alguna manera incentivan la mala conducta. Esto también lo vemos de gente que está dentro de nuestra comunidad, gente que está aquí. No es algo que desconozcamos. Necesitamos abordar las cuestiones que tenemos por delante, frente a nosotros.

Si cumplimiento contractual no puede identificar efectivamente que hay elementos específicos del contrato que los van a ayudar a exigir cuestiones claras y también afectar a estos actores malos, hablemos del tema y sigamos avanzando con eso específicamente. El cumplimiento que no esté lidiando con ninguna acción que sea maliciosa sobre la cual todos tenemos que estar de acuerdo y comenzar a actuar.

BRUCE TONKIN: Gracias, Elliot. Vamos a tomar un comentario de la participación remota.

PARTICIPACIÓN REMOTA: Tenemos dos preguntas y dos comentarios. El primer comentario es de Maxim Alzoba: “El DAAR contiene falsos positivos y no hay evidencia de ninguna información accionable para los registros. Nombres de dominio ni números”. El segundo comentario dice que por favor estemos al tanto de los cierres que se hacen y la falta del debido proceso por parte de los registradores y registros y de la terminación de los contratos.

El siguiente comentario viene de Andrew y dice: “Por favor, no nos detengamos únicamente en las definiciones y en los temas del ámbito. Tenemos que comenzar a trabajar en las acciones”. Hay un comentario de Michele Neylon que dice: “El uso indebido impacta, es una cuestión que impacta el ecosistema de Internet y no hay duda de que la industria hoy se encuentra en una mejor posición para resolver el tema y también para agregar más obligaciones en nuestro contrato”. Tenemos una pregunta de Sivasubramanian, de la India, que pregunta lo siguiente: “¿Cuáles son estas cuestiones artificiales de la ICANN? Si la ICANN, por ejemplo, restringe su atención solamente al uso indebido de un nombre de dominio y de su sistema va a ocurrir que esto se va a dar en otros espacios. Van a quedar otros espacios sin atender y va a dejar una larga porción disponible para el uso indebido. La ICANN es la única organización que tiene el entendimiento y la capacidad técnica para poder abordar el uso indebido de manera competente que sucede fuera del uso de nombres de dominio y también los que se originan desde la web profunda”.

La última pregunta es de Andrew Campling: “El ecosistema del DNS ha sido ampliamente descentralizado y colaborativo. Se ha encriptado el

protocolo del DNS a través del protocolo como por ejemplo DoH. Esto va a centralizar a los operadores y va a resultar en la necesidad de inteligencia para seguir trabajando".

BRUCE TONKIN: Esto lleva a los estatutos. La organización es una entidad privada que tiene contratos con registros y registradores y hay ciertas limitaciones dentro de los estatutos que se establecen así.

FARZANEH BADII: Cuando hablamos del ciberdelito en general, parte del delito se facilita a través del uso del DNS. Esto no significa que todo lo que está relacionado con ese delito se tiene que resolver a través de una organización como por ejemplo la ICANN. Es una sugerencia muy riesgosa decir que tenemos que utilizar estos foros que son centralizados para todas las cuestiones o problemas relacionados con el DNS o para abordar todos los delitos que suceden que en cierto punto tienen que ver con el uso del DNS. Estamos poniendo entonces en peligro la Internet abierta, global e interoperable.

BRUCE TONKIN: La segunda pregunta la mencionó un proveedor de servicio de Internet y hace referencia a lo que se decía con respecto a la cadena de suministro. Es necesario también abordar el tema de la cadena de suministro que está más cerca del problema. No quiero hacer un debate muy extenso porque probablemente no todos van a poder tomar la palabra pero adelante, Alan.

ALAN GREENBERG: Mi comentario está relacionado con lo que dijo Elliot pero con una perspectiva distinta. El trabajo que escuchamos que nos cuentan Brian y Graeme es muy alentador. No es que no haya habido acciones anteriormente pero hacerlo de manera pública y alentar a otros registradores y registros a que lo hagan es muy positivo. A mí me interesó escuchar los comentarios de Brian y Mason sobre los PIC. Estuvimos trabajando durante décadas. Escuchamos durante décadas que sí, este es un problema pero no tenemos las herramientas, cumplimiento no tiene las herramientas para hacerlo. En algunos casos yo creo que hasta Elliot tiene razón. Hay cláusulas en el contrato que se pueden incluso interpretar como que se pueden implementar pero cumplimiento no las usa o no las aplica de manera en que se puedan exigir.

También escuché comentarios con respecto a que el informe de DAAR es importante y que OCTO no implica cumplimiento. Lo que tenemos que hacer es sentarnos todos, todas las partes en una misma mesa. Si es necesario hacer cambios contractuales, lo tenemos que hacer todos juntos. Asegurémonos de que la separación artificial entre OCTO y el departamento de cumplimiento contractual no evite que nosotros usemos información que nos resulte valiosa. Podemos hacer algo y, como dijo Elliot, es muy sencillo decir que los malos actores no están en la ICANN. Algunos sí están. Dejemos de simular que no lo sabemos.

BRIAN CIMBOLIC: Quiero comentar algo con respecto a la difusión externa a otros registros y registradores. Estamos trabajando en algo como una especie de marco y esta es una convocatoria abierta a los registros y registradores. Si ustedes piensan que hay un marco que podemos implementar, estamos también agregando gente o buscando gente que esté comprometida o que se quiera comprometer para seguir trabajando en este documento. Hay varios operadores de registro de código de país que están trabajando y ojalá ustedes también puedan hacerlo.

BRUCE TONKIN: Tiene la palabra Stephanie.

STEPHANIE PERRIN: Stephanie Perrin, de la unidad constitutiva de partes no comerciales. Yo quería tomar la palabra para avalar lo que decía Farzi. La palabra que ella no utilizó pero que sí nos interesa en la unidad constitutiva es que la ICANN puede hacer incentivos financieros o incentivar financieramente a aquellos que actúan bien y también sabemos que el OCTO habla del uso indebido técnico y el uso indebido del contenido pero, por favor, les ruego que se adhieran al uso indebido técnico porque tienen que trabajar mucho en ese sentido. También avalo lo que dijo Elliot en relación con que la ICANN no se meta en el negocio y que actúe sobre contratos que están fuera del proceso de desarrollo de política de las múltiples partes interesadas.

BRUCE TONKIN: Probablemente los panelistas quieran abordar los comentarios en general. Voy a dejar que hagan las preguntas y luego el panel va a compartir las reflexiones.

DIRK KRISCHENOWSKI: Soy vicepresidente del grupo de GeoTLD. Quiero hacer un comentario sobre este grupo de los GeoTLD. Los miembros tenemos contratos con los gobiernos, lo cual incluye varias obligaciones de interés público, incluido el uso indebido, como lo define la ley nacional. Hicimos una investigación de GDPR donde se demuestra que hay muy pocos pedidos que son muy buenos. Hoy quisiera decir que estamos haciendo una encuesta de abuso del DNS con 22 TLD geográficos en los últimos 12 meses. Sí, hay abuso en los TLD geográficos pero muy poco. Solamente tres miembros tienen más de 10 casos en el último año. Vamos a publicar los resultados de ese estudio muy pronto pero quisiera decir que más allá de la conversación actual no hay una necesidad de obligaciones contractuales adicionales. Quiero citar a Tucows en ese sentido. Tampoco hay una necesidad de un acceso unificado que, por lo que escuché es el sistema que lo regula todo.

BRUCE TONKIN: Gracias, Dirk. Vamos a volver a las cuestiones online.

PARTICIPACIÓN REMOTA: Mi pregunta es sobre el impacto del DNS no fue entendida. El DNS ha sido muy descentralizado y muy colaborativo. Con el advenimiento de los protocolos de DNS, como DoH, los resolutores descentralizados

van a requerir compartir la inteligencia o en lugar de eso van a ser explotados para una ganancia comercial. Si no, cómo van a hacer los registros y los registradores para saber dónde está ocurriendo el uso indebido.

BRUCE TONKIN: Jeff, ¿quiere comentar? Es una pregunta.

JEFF BEDSER: Lo voy a tener que pensar. No tengo una respuesta directa.

BRUCE TONKIN: ICANN no tiene un contrato con el resolutor del DNS y no le puede decir qué hacer pero es parte del ecosistema. Yo sí entendí la pregunta. Es una pregunta sobre los resolutores.

BYRON HOLLAND: Byron Holland, del operador de ccTLD para .CA. Les agradezco por hacer que esta conversación se inicie. Escuché mucho acuerdo bastante violento, quizá con la excepción de Farzi. Hay al menos un abogado en el podio y hay una persona más del mundo de la política. Quiero que pensemos en la noción de la pérdida de las definiciones. Las palabras importan y, como abogados y pensadores de política, nosotros sabemos que las palabras importan. Si no, vamos a terminar yendo en múltiples direcciones. Vamos a asegurarnos de que reducimos todo a una definición. Como operador, mi perspectiva es que esa noción establece la línea entre el abuso técnico y el abuso de

contenido. Eso importa y cómo lo definimos va a ser crítico para el éxito de crear espacios limpios, que es lo que todos queremos. Quizá podamos a pesar de eso diferenciarnos en la implementación.

Hay que prestar mucha atención a los estatutos de la ICANN que dicen claramente dónde empieza y dónde termina el alcance y el abuso del contenido quizá está por fuera de esa línea. También debemos mirar dónde están los temas y dónde están las reglas o las regulaciones o las acciones que se van a tomar. Si los operadores del DNS en la segunda y tercera capa hacemos algo y el contenido está en otra capa debemos tener mucho cuidado de qué es lo que vamos a regular y dónde vamos a actuar, cuál es la capa de la actividad sobre la cual vamos a actuar. Para muchos de nosotros que estamos en esta sala y que luchamos muchas peleas de la gobernanza, mucho ha tenido que ver con la regulación y la legislación en la capa correcta. A los que estamos en el espacio de gobernanza debemos asegurarnos de que no incumplimos todo esto de lo que venimos hablando desde hace muchos años y en muchos foros globales.

Mi punto final. Muchos de los comentarios tienen que ver con los actores individuales que actúan. Creo que hay espacio para eso claramente. Debemos recordar que el control judicial no es algo malo. En los países donde hay un derecho, el control judicial nos da permiso para hacer estas cosas. Estas no son malas palabras. El control judicial no es una mala palabra y no deberíamos dejarla de lado. Gracias.

BILL JOURIS: Soy miembro de un grupo de partes interesadas. La persona de los registros y registradores estaba hablando sobre lo que hacen para resolver los problemas cuando los identifican. Me pregunto si consideraron qué pueden hacer para que esos problemas no surjan directamente. Hubo aquí un ejemplo que se planteó. Si sabíamos que EZIAET se iba a registrar, quizá el problema nunca habría surgido. Ahora debemos ver qué es lo que causó la confusión. La buena noticia es que la ICANN a través de la internacionalización de nombres de dominio está compilando una larga lista de caracteres que son confusos. De hecho, eso lo podemos agregar. Esta identificación ya está hecha. Quizá no es una lista completa pero claramente los va a permitir dar un paso hacia delante. La mala noticia es que ICANN no puede publicar esa lista y cualquier persona que hace un algoritmo de generación de dominio no tiene ya que adivinar porque nosotros se lo estamos diciendo. Personalmente, yo creo que la obligatoriedad del uso de esas listas debe estar en el contrato pero al hacerlo hay algo que los registros y los registradores deben hacer como a modo de prevención.

BRUCE TONKIN: ¿Algún otro comentario?

GRAEME BUNTON: Hay un sistema para evitar las registraciones. Este sistema es un problema mucho más complicado de lo que pensamos. La idea de hacer un predelito de nombres de dominio tiene que ver con lo que expresó Farzi sobre los programas de incentivo, que quizá no

conozcamos. Creo que hay un verdadero riesgo y tenemos que pensarlo más. Gracias.

BRUCE TONKIN: Algo que hacen los cc es que usan software predictivo para identificar estos temas. Esto no evita la registración pero sí puede identificar lo que requiere más investigación y que quizá requiera de información sobre por qué un nombre se está registrando. Tiene que ver más no solamente con parar una registración sino que tiene más que ver con una investigación.

NEIL SCHWARTZMAN: Hola. Soy Neil Schwartzman. Soy director ejecutivo de la Coalición contra Email No Solicitado. Esta es una discusión interesante. Bienvenidos a Montreal. Esta es mi ciudad. Estamos escuchando la misma discusión una y otra vez. Estoy aquí para darles un poco de contexto desde mi perspectiva personal. Hasta agosto yo me estaba ocupando mucho del abuso del DNS para el DNS para un fabricante de hardware que hace estos aparatos que tengo aquí en la mano.

Nosotros pensamos que 20.000 es un buen número. También pensamos que 30.000 ataques de phishing implican 90.000 activos. Yo personalmente mapeé 50.000. Cuando hablamos de los esfuerzos y que quizá necesitamos una mejor definición, pasaron 50 años desde que se inició Internet y entonces qué es lo que nos impide definir las definiciones efectivamente.

Es tiempo de avanzar. No quiero decir que hay que moverse erráticamente ni irresponsablemente. Entiendo el proceso pero llegó el momento de hacer algún esfuerzo concertado porque esto es una crisis. Cuando vamos a ver la anonimización de IP a IP, cuando efectivamente hay anonimización de quién es el propietario de un activo como un dominio, estamos hablando de un reino libre para los criminales. Ellos están haciendo un enorme uso de ello. El grupo de trabajo anti-phishing ni siquiera tiene una idea de todos los ataques de phishing, con todo el respeto a las personas que están tratando de hacerlo. Hay mucho que no se reporta porque no tenemos el tiempo.

El uso indebido es un costo para los registros y registradores que están aquí. El incentivo es no poner dinero en eso. Ese es el incentivo que hay en este momento. Yo estoy de acuerdo en que no debemos decir a la gente que establezca sistemas falsos, que ponga muchos dominios y que los use indebidamente para tener dinero. Esa no es la forma de hacerlo. La forma de hacerlo es tratar el problema efectivamente con unos informes adecuados y precisos.

Este es otro punto de contacto. Uno de los grandes registradores que tiene un gran problema de phishing, ellos tienen tres personas que trabajan en el equipo de phishing. Uno de ellos acaba de tener un hijo. Es decir, hay dos personas a tiempo completo. Ni siquiera se acerca a lo que es suficiente. Estamos hablando solamente de phishing. No hablamos de DNS, de spam. El spam de una persona es el marketing del otro. Debemos hablar de la erosión de la confianza del consumidor en Internet. Por eso todos estamos aquí, para proteger al usuario final. Gracias.

PIERRE BONIS: Soy Pierre Bonis, de AFNIC, del ccTLD .FR. Quisiera hacerme eco de lo que dijo Byron. Debemos preguntarnos por qué estamos hablando de eso hoy. El uso indebido no es nuevo. El uso indebido técnico tampoco es nuevo. De hecho, eso está en el contrato. Yo creo que estamos hablando de eso hoy porque hay más y más presión legítima de muchas partes interesadas por fuera de la ICANN. Digamos gobiernos pero también miembros de la sociedad civil que están hartos, diría, de los actores digitales que les dicen: "No podemos hacer nada". Hay enormes plataformas, enormes motores de búsqueda que les han dicho eso a los gobiernos y a muchos actores durante años y años. Cuando nosotros tratamos de decir que hay una capa técnica de la cual nosotros estamos a cargo y que hay una capa de contenido de la cual nosotros no estamos a cargo, nadie escucha ya porque escucharon ya este tipo de oración durante décadas. Estas oraciones las dijeron personas que estaban a cargo del contenido. Creo que es muy importante no importar las responsabilidades de los proveedores de alojamiento, las plataformas, hacia la industria del DNS simplemente porque la gente está harta de las explicaciones técnicas. Si nosotros continuamos con el rumbo de tratar de hacer algo con el contenido para asegurarnos de que la gente nos vea como actores responsables a fin de cuentas no vamos a ser responsables porque vamos a hacer el trabajo de los jueces o de la policía, que no es nuestro trabajo. No porque no queremos hacerlo sino porque eso no es democrático.

Este llamado a la acción es muy lindo pero para el bien común y el interés general debemos ser muy cautelosos y debemos decir que podemos hacer algo a la capa técnica pero hay un enorme riesgo de que nos digan qué es una competencia buena o mala. Esto es bueno a nivel nacional para un cc como .FR pero es incluso más verdadero a nivel global para una organización como la ICANN porque, por supuesto, nadie considera que una organización global o de múltiples partes interesadas pueda tener una definición del contenido inadecuado, malo que pueda cumplir con todas las jurisdicciones internacionales y que también pueda cumplir con todas las culturas. Gracias.

BRUCE TONKIN: Gracias. Por cuestiones de tiempo y veo que hay muchos comentarios y me gustaría que todos tomen la palabra, vamos a hacer que las intervenciones sean más breves.

TOM LAM: Soy Tom Lam. Tengo una pregunta y también tengo un comentario para hacer. Me paré dos veces ya. En cuanto al programa de los incentivos, ¿los registrados les van a brindar a los registradores una lista de los nombres de dominio que han sido registrados y borrados dentro de un determinado plazo? ¿Se utilizará esa letra si, por ejemplo, los registradores eligen por ejemplo registrarse en esa lista negra para ver cuáles son esas registraciones? Esto podría ser un incentivo para los registradores de alguna manera y los registradores también tendrían que de alguna manera desarrollar una especie de método

para los que son clientes legítimos y para que después puedan seguir avanzando en el proceso de registración.

Mi comentario tiene que ver con ser impermeables o a prueba de balas. Nosotros brindamos información de contacto del hosting y también brindamos los IP de origen a los informadores o los informantes de confianza. Estamos gustosos siempre de ayudarlos con el debate si nos contactan. Nosotros no compartimos información. Nos encontramos trabajando en abordar el tema del malware con DoH.

BRUCE TONKIN: Gracias. Siguiente orador.

DEAN MARKS: Soy Dean Marks. Soy vicepresidente de la IPC. Además soy abogado. Quiero responder algunos de los comentarios sobre el tema de las regulaciones y el rol, por ejemplo, del sistema de justicia. La idea es recordarnos que para cada registración de nombre de dominio existe un contrato entre el registrante y el registrador. Eso implica obligaciones contractuales, lo cual quiere decir que el registrador está legalmente capacitado para tomar acción. Si el registratario piensa que ese contrato ha sido violado, por supuesto también es posible hacer una revisión judicial. Corresponde que así se haga.

Farzi, quiero decir que estoy de acuerdo con usted. Si usted piensa que hay marcos implementados para que los registradores y los registros suspendan un nombre de dominio, me parece que es una opción pero también se puede decir que se está cometiendo un error porque se

está suspendiendo un nombre de dominio. Me parece que tenemos que seguir avanzando con este marco para seguir abordando el tema del uso indebido. No me parece que toda la responsabilidad esté en el sistema de nombres de dominio sino que también tenemos que ver que somos una plataforma de operadores pero que es un paso muy importante y quiero también expresar mi gratitud al IPC. El marco habla, por ejemplo, de identificadores confiables. Yo trabajé para la asociación de motion picture y quería decir que todos los que están interesados en esas cuestiones me pueden contactar.

BRUCE TONKIN: Milton.

MILTON MUELLER: Milton Mueller, Georgia Tech. Yo me siento obligado a tomar la palabra porque me parece que el tema fundamental que estamos debatiendo no ha sido identificado claramente. Tenemos que darle un marco totalmente distinto al que se le dio. La pregunta con la que ustedes comenzaron es qué tenemos que hacer sobre el uso indebido del DNS. Eso, por supuesto, nos lleva a preguntarnos qué queremos decir con uso indebido del DNS y empezamos a hablar de cuánto contenido está incluido y la rúbrica o que implicaría el uso indebido del DNS.

La gente que busca una definición más compleja de uso indebido del DNS parece que si no definiéramos el uso indebido, no vamos a hacer nada. Cuando hablamos de cuestiones relacionadas con el contenido, hablamos del ejemplo de la pornografía infantil. Eso es

extremadamente ilegal en cualquier jurisdicción del mundo. Hay muchísimos mecanismos para informar estas cuestiones y para removerlas y que no tiene nada que ver con la ICANN y el sistema de nombres de dominio. Lo mismo con el copyright. Tenemos tratados globales. Si ven lo que se estuvo haciendo, por ejemplo, si nuestro departamento de inmigraciones y aduanas estuvo haciendo, bueno, estuvieron ocupándose de muchas cosas en todo el mundo pero hay otras jurisdicciones que hacen lo mismo. Si no definimos el uso indebido del DNS no vamos a poder avanzar o nos van a atacar legalmente y políticamente.

Creo que la pregunta que se tendrían que hacer es esta. Cuando hay un problema con el DNS que está inmediato, que hay una emergencia, tenemos que pasar por encima de los procesos y hacer que los registros y registradores actúen de manera directa. Esa es la pregunta que hay que evaluar. ¿Queremos que sean los registros y registradores los jueces, jurados y ejecutores de la política? Me parece que esto se ve en algunas cuestiones que están relacionadas con la ciberseguridad y el spam, pero que no veo que haya ningún justificativo para esto en cuestiones que tienen que ver con el contenido.

BRUCE TONKIN: Adelante, James.

JAMES BLADEL: James Bladel, de GoDaddy, una de las otras empresas que están trabajando en el marco para el uso indebido. Quería responder a lo

siguiente. El marco no es tan nuevo. Estas prácticas que se describen aquí han estado implementadas desde hace décadas o años y representan una parte en realidad de lo que sucede dentro de los registros y registradores y tienen como objetivo crear conciencia y educar a la comunidad sobre lo que ya está sucediendo pero quiero hablar de algo específicamente que ya mencionaron.

Ustedes mencionaron algo con respecto a que el proveedor de hosting es la entidad más adecuada para abordar el tema del uso indebido del contenido. Creo que eso es así. Estamos de acuerdo. Ahora bien, qué es lo que van a hacer los registradores para garantiza que estos contenidos estén disponibles para el reclamo. A veces esto es un tema complejo porque muchas veces actuamos sobre la base de nuestro acuerdo de hosting y en términos de servicio pero eso nos da un poco más de flexibilidad. En algunos casos sabemos quién es el que publica. Tenemos ideas y podemos avanzar en esa decisión. Más allá de todo esto creo que es erróneo que los registradores tienen idea de quién es el proveedor de hosting o qué cosas van a funcionar o qué cosas no o cómo vamos a contactarlos o llegar a ellos.

Quizá tendríamos que buscar otros recursos que ya se encuentran implementados, pensando por ejemplo en las SO. Suponiendo que los registros y registradores tienen información privilegiada que no quieren compartir con respecto a los proveedores, me parece que eso es algo que tenemos que corregir.

BRUCE TONKIN: No se dijo exactamente eso sino más bien que la información no siempre está disponible. No se quiso decir eso.

LUTZ DONNERHACKE: Soy Lutz, de EURALO, At-Large. Lo que estamos debatiendo aquí es qué está en el ámbito de la ICANN. Si no me equivoco, si entendí bien, muchas de las cuestiones debatidas aquí tienen que ver con los contratos. Entonces, si existe la posibilidad de ver qué registraciones se hicieron, sería más fácil para las agencias de cumplimiento de la ley descubrir quién es el responsable. Esto es poner mucha energía en los registradores para obtener los datos correctos. Uno también puede ir al contrato y seguir el intercambio porque el contacto se tiene que mantener. No es la registración. Las registraciones deben seguir. Muchas de ellas, por ejemplo, son automáticas. A nadie le importa si tienen detalles o no pero el contrato entre los registros y los registradores, estos contratos están siempre implementados y contienen datos correctos. Mi pregunta es por qué no se publica el cambio al contrato para cada registración. Por ejemplo, si utilizamos el servicio de WHOIS extinto ya, olvidémonos del GDPR. ¿Por qué no lo hacemos así?

KATE PEARCE: Voy a hablar en mi propia representación. Yo quería mencionar algunas cuestiones. Voy a hablar un poco más lento. Tengo acento neozelandés. Entiendo que puede ser complejo. Rápidamente, en primer lugar la mayoría de las cosas que vemos tienen que ver con los nombres de dominio y la mayor parte del daño sucede en nombres de

dominio más antiguos. Los daños tienen menos posibilidad de ocurrir o de impactar en las registraciones que tienen pocos días pero otro punto es que hablamos de las regulaciones compartidas. Esto ya está sucediendo a nivel de los resolutores, particularmente en las empresas y en los espacios gubernamentales. Hay espacios donde ve que hay cierta predicción. Eso ya está teniendo lugar. Quizá sí sea correcto pero el resultado de esto es una organización con menos recursos e individuos que no tienen la protección. Para muchos de ellos, esto quizá sea el único punto de contacto en particular con un hosting que avanza con tanta velocidad.

BRUCE TONKIN: Tiene la palabra David.

DAVID CANE: David Cane, del grupo de partes interesadas no comerciales. Soy profesional también de la seguridad. Mi tema con el término uso indebido del DNS es qué es el uso indebido del DNS. Su definición tiene que ver con algo que le sucede al DNS y que eso que le sucede no es bueno. Sé que seguir debatiendo el tema de la definición nos lleva a una serie de cuestiones que son distintas. Hay algunas que están dentro del ámbito de la ICANN, que tienen que ver con la seguridad y la estabilidad. También hay otras que están asociadas pero que no llevan siempre a los mejores resultados. Me refiero al ejemplo de los botnets. No queremos, por ejemplo, remover o quitar todos los nombres de dominio que probablemente puedan tener un botnet. Eso no se puede hacer simplemente con un mecanismo.

Teniendo en cuenta que esto está claro dentro del ámbito de la ICANN no siempre se obtienen los mejores resultados. También hay otras cuestiones que tienen que ver con el contenido. El hecho de que el contenido puede ser erróneo o ilegal no va a cambiar el hecho de que quizá esté fuera del ámbito de la ICANN. Hay otras cuestiones. Que esté fuera del alcance de la ICANN no significa que no tengamos que hacer algo al respecto. Seguramente haya cuestiones en las cuales podemos aportar. Ambas posiciones están bien establecidas pero hay un esfuerzo también importante para poder tener una respuesta concertada a estas cuestiones.

No tenemos que olvidarnos que estamos en la ICANN. Lo que hemos aprendido de la ICANN y que esto implica muchas cuestiones, muchas cuestiones de sutilezas de política. Hay muchos detalles y creo que incluso cuando lo hacemos podemos decir: “Este es un tema de contenido y hay que responderlo”. ¿Por qué hay que responder este tema? Lo tenemos que hacer fuera de la ICANN y hacemos esto. No tenemos que olvidarnos de lo que aprendimos de la ICANN. A veces los temas de políticas se complican, las personas tienen perspectivas totalmente diferentes. Hay temas que quizá no nos demos cuenta pero tengamos que aprender de las lecciones y de los procesos. Tenemos que tener una respuesta concertada para todas estas cuestiones. Quizá tengamos que pensar en, por ejemplo, cómo podemos hacer un proceso de desarrollo de política que sea un modelo fuera de la ICANN y fuera también de las complicaciones de la ICANN. Gracias.

BRUCE TONKIN: Los últimos dos oradores, por favor.

WERNER STAUB: Soy Werner, de la Asociación CORE. Hablo a título personal. Estábamos hablando sobre cómo atrapar a los malos dominios. Supongamos que estamos hablando de billetes y que estamos hablando de billetes falsos y de imprentas que lo que queremos es que no produzcan una gran cantidad de billetes falsos. Creo que, en ese tipo de reflexión, uno pensaría de una segunda forma. No quiere decir que no haya que hacer la primera pero qué pasaría si mejorásemos, por ejemplo, los billetes originales en lugar de ir casando, ir buscando atrás los billetes falsos. Cómo hacer para mejorar aquellas características que nos permitan reconocer que es un billete bueno, no uno que es malo. El bueno.

Aquí es donde nosotros debemos trabajar. Esto es un valor agregado. Nosotros estamos en una especie de carrera de calidad de registraciones. Todos quieren que sean más baratos, hacer menos verificados y nadie quiere que se verifique nada. Nosotros estamos recibiendo quejas. Hay gente que quiere que sí se lo verifique, que está pidiendo una forma de poder mostrarle a la gente y a las máquinas que se trata de una registración verificada. Esta es una oportunidad comercial para los registradores, también para los registros y también es una manera de que los nuevos gTLD se distingan. Se trata de una manera positiva y de un círculo vicioso de incentivos que nos van a ayudar a realizar una mejora si lo hacemos más fácil. Vamos a poder identificar más fácilmente a los malos.

BRUCE TONKIN: Último orador.

ROB HALL: Hola. Soy Rob Hall. Creo que ya me reconocen. Hace tiempo que estoy aquí. Estoy un poco frustrado porque hablamos del DNS para cubrir todo pero en realidad en esta sala estamos hablando del abuso de un nombre de dominio, no de un sistema de todo el ecosistema. Recuerden que hay muchos otros sistemas y estamos hablando del uso indebido del DNS. Quiero preguntarle al panel, uno de los abusos que nosotros estamos viendo como registros y registradores con los años es el sistema del WHOIS, que también es parte del DNS. Debemos establecer un nuevo sistema el RDAP y quiero ver cómo vamos a parar el abuso de eso. Está también el minado de datos y lo que sucede con nuestros clientes. No quiero que nos focalicemos en que lo que la gente cree que es un cliente que registra un nombre de dominio y abusa ese uso sino que empecemos a hablar sobre todo el ecosistema de nuevo y de los servicios que nos olvidamos normalmente porque no son los importantes.

BRUCE TONKIN: Gracias. Quiero preguntarles a los panelistas si tienen algún comentario final o mensaje que quieran dejar a la audiencia.

GABRIEL ANDREWS: Quiero agradecer todos los comentarios. Es muy interesante ver lo que ustedes piensan. Es educativo también para alguien como yo. Esta es mi tercera reunión de ICANN nada más. Creo que hay un reconocimiento general de que hay un potencial de encontrar un punto común en el tratamiento de algunos de las conductas más nocivas que existen en nuestro ecosistema. Podríamos hablar de definiciones. Podríamos tratar de encontrar esos términos exactos pero quiero advertirles de que los criminales, los delincuentes son inteligentes, son creativos y que si somos muy prescriptivos para identificar cada medio de abuso o de uso indebido que existe podríamos potencialmente caer en un problema. También hay un beneficio, sin embargo, al reconocer que hay buenos impulsores entre nosotros y que se van aplicando las reglas que están establecidas.

BRUCE TONKIN: Farzaneh.

FARZANEH BADII: Dos puntos. Uno es que yo no creo que se esté ocultando al host. Tampoco creo que lo anónimo y la gente que puede realizar acciones y tener sitios web y expresar sus opiniones en Internet sean necesariamente un criminal, un delincuente. No todo el mundo quiere ocultar cosas ni ser anónimo y no hablamos necesariamente de un delincuente pero debemos pensar en eso. No podemos decir directamente que debemos establecer todo un contrato y la cadena de los registradores en Internet e identificar a los registratarios. Hay libertades civiles que están en juego aquí también.

Lo otro que quiero mencionar, quizá no fui clara al principio, nosotros acordamos con algunas de las entidades que se ocupan del abuso del DNS en ICANN. Usted mencionó el marco pero no estamos de acuerdo con los asuntos de los registros y registradores que están quitando contenido por los opioides, etc. Quería aclarar eso.

BRIAN CIMBOLIC: Hay muchos registros y registradores que están haciéndolo lo mejor que pueden y están tomando medidas, incluso los que no están obligados contractualmente a tratar los asuntos del uso indebido del DNS. Como dijo Farzi, creo que tiene razón. Decir que uno lo hizo simplemente no es el enfoque adecuado. Hay que pensar más y ser un poco más transparente.

GRAEME BUNTON: Cuatro puntos rápidos. Terminamos en una discusión sobre registradores y el abuso. Creo que vale la pena reconocer que nos impacta también. Todos estamos casi siempre bajo un ataque de DDoS como registrador y esto genera cuestiones que son importantes para nuestro interés también. Me sorprende también que estoy de acuerdo con Elliot en que hay muchas herramientas en nuestros contratos. Tenemos que ser un poco más creativos sobre cómo usarlas. A Milton le digo, y a Farzi también respecto del marco sobre el abuso del DNS, que creo que el argumento que se puede decir es que estamos tomando medidas en esas instancias muy específicas a causa de los fracasos en los gobiernos y en las regulaciones globales y en los

lugares en los que vemos ese daño material donde nos parece que no hay herramientas externas.

Lo último que les quiero decir. Esta es una metáfora que uso hace mucho. El abuso del DNS se encuentra en ese documento, que es una especie de polución de la industria. Pretender que esto es una externalidad no es adecuado y debemos hacernos responsables porque eso sea así.

MASON COLE: Hay desconfianza en Internet por el uso indebido. Si ICANN no hace lo suficiente para tratar esa desconfianza, esto reduce la legitimidad de la ICANN. El BC trabaja con herramientas. Aplaude a los registros y a los registradores que lo están haciendo y también aplaude los incentivos. Tenemos que trabajar en conjunto con cumplimiento para que le demos herramientas para que reduzcan a los malos. Espero que podamos sacar algo de esta sesión y que podamos hacer un mejor trabajo.

JEFF BEDSER: Hablamos mucho de esto y seguimos haciéndolo pero me emociona que este tema fue un tema importante en la agenda y en los próximos meses. Todos debemos tener en cuenta que los perpetradores del abuso no ven estas líneas del contenido y de la infraestructura del DNS. No les importa cuáles son las líneas donde dicen cuál es tu problema o tu problema o tu problema. Ellos usan el sistema y el ecosistema para victimizar a la gente y para continuar la victimización.

Hay que tener un lugar para tener la conversación. Yo no soy una persona de política. No creo que sea ICANN donde se deba realizar esto pero debemos iniciar la conversación, mejorar el sistema y tener menos abuso, mejorar la reputación del modelo y con el crecimiento capitalista del modelo, la gente debe confiar en ese modelo. Si no somos nosotros, entonces quién.

BRUCE TONKIN: Para resumir, escuchamos discusiones sobre las definiciones. Las palabras importan. La gente habló sobre tener una línea clara entre lo técnico en cuanto al abuso del DNS versus el abuso del contenido. Tiene que haber una línea clara en esos dos tipos de uso indebido. Algunas de las sugerencias positivas para la mejora son que la gente pueda identificar el contenido que quedó fuera y la gente que es responsable del hosting debe encontrar métodos apropiados para contactar al registratario. También debe haber un método de apelación. Siempre debe haber una forma de apelar una decisión si hay algo que es quitado. También hablamos de los distintos incentivos. Creo que tiene que haber apoyo para una mayor investigación. Aquellos incentivos pueden ser la reputación, tener una mejor reputación y que la gente sepa lo que es bueno y lo que es malo, formas de mejorar eso.

También hubo algunos comentarios sobre resolver el problema en la capa correcta. Creo que este es un buen entorno para compartir las prácticas. A nivel contractual, los contratos deben estar incluidos en el mandato de la ICANN, también en el mandato técnico. En particular,

cómo podemos ayudar al equipo de cumplimiento a ser efectivo para que podamos tomar medidas contra las partes que no están cumpliendo con lo que la comunidad considera que es aceptable.

Quiero agradecerles ahora sí a todos los oradores, tanto en la audiencia como en el panel. Han presentado temas importantes y son todas cosas en las que debemos pensar y avanzar en ese sentido. Gracias a todos.

[FIN DE LA TRANSCRIPCIÓN]