KOBE – Sesión de trabajo de los líderes de At-Large: GCSC y el presidente de la GNSO
Domingo, 10 de marzo de 2019 – 15:15 a 16:45 JST
ICANN64 | Kobe, Japón

OLIVER CREPIN-LEBLOND: … Aquí a la comisión global sobre la estabilidad del ciberespacio que vienen a reunirse hoy con nosotros, y a conversar sobre el trabajo que están haciendo o que han hecho en el pasado, en los últimos dos años… pasa bastante rápido, estoy recordando cuando empezó.

Tenemos nuevos co-presidentes, que han tomado el control que tenía Marina Kaljurand, sigue siendo muy interesante tenerlos aquí a nosotros, le quiero agradecer a Wolfgang Kleinwaechter por estar aquí, tuvimos una reunión con ALAC en un contexto de ICANN, creo que es la primera vez que ustedes están en un contexto de ICANN para discutir el trabajo, por eso es muy emocionante ver a toda esta gente aquí en la sala.

No voy a seguir hablando por siempre, le voy a dar la palabra a quien está aquí a mi lado, para que nos cuente sobre el trabajo en el GCSC. Aquí hay una nota de organización.

GISELLA GRUBER: Disculpen la interrupción, soy Gisella del personal. Quiero recordarles a todos que esta sección tiene traducción al español

y al francés, es posible que ustedes reciban preguntas en esos idiomas, y salvo que los hablen por favor utilicen sus auriculares, tenemos aquí las cabinas de interpretación detrás, les quisiera pedir que por favor digan su nombre cada vez que toman la palabra para que los identifiquen en el canal lingüístico correspondiente y también la transcripción, y quiero pedirles que hablen a una velocidad razonable para que haya una interpretación adecuada. Muchas gracias.

OLIVIER CREPIN-LEBLOND: Gracias Gisella.

LATHA REDDY: Gracias Olivier por invitarme a esta presentación. Mi nombre es Latha Reddy, soy co-presidente de la comisión global sobre la estabilidad del ciberespacio, y nuestra misión es comprometernos con distintos sectores para desarrollar normas y políticas, mejorar la seguridad y estabilidad internacional, y ayudar al comportamiento de estados y no-estados en el ciberespacio.

Como dijo Olivier, nosotros lanzamos esta comisión hace dos años en la Conferencia de Seguridad de Múnich, es una iniciativa conjunta del gobierno de los países bajos, y los últimos dos actores están en la secretaría del grupo.

Éramos tres co-presidentes con Marina, y con Michael y yo como co-presidentes. Marina fue elegida como miembro del parlamento en Estonia, ella renunció entonces como presidente, pero que las reglas no le permiten ser presidente. Michael y yo hemos asumido la presidencia conjunta de la comisión.

Tenemos 25 comisionados, como ya mencioné a la secretaría, somos un grupo de múltiples partes interesadas, tenemos a la sociedad civil, a la industria, a gente con experiencia en el gobierno, yo soy diplomática retirada, jubilada, Michael pertenece al sector de la seguridad interior en Estados Unidos, y tenemos también a un grupo de asesores en investigación, y también una junta de asesoramiento, es decir que tenemos toda una burocracia.

Quería también decir, que mencione brevemente cuál es nuestra misión. Lo que nosotros hemos logrado hasta ahora, es formular y difundir ocho normas en el espacio público que esperamos que puedan llegar a los líderes, a los que generan las políticas en todo el mundo. También coordinamos en conjunto con muchos otros organismos, que incluyen parte de algunos organismos de la O.N.U., Marina también es miembro del panel de alto nivel de la secretaría de la O.N.U. sobre los asuntos digitales.

Lo que nosotros hacemos, porque las normas en sí explican mejor lo que nosotros hacemos, qué tipos de recomendaciones la

comisión se focaliza, y en qué se va a focalizar nuestro reporte final. Así, les vamos a dar una idea de lo que creemos que es importante, para que nuestro ciberespacio sea abierto, seguro, y también que exista una innovación.

Tenemos entonces ocho normas. Quisiera pedirle a uno de mis colegas de la comisión presentarles la primera norma, que es proteger el núcleo público de internet. Quisiera también pedirles entonces a mis colegas, que se limiten a una presentación de dos minutos cada uno para que tengamos suficiente tiempo para el debate.

WOLFGANG KLEINWAECHTER: Cuando empezamos a discutir las normas, la idea de tener una norma especial para proteger al público de internet, inmediatamente tuvo consenso total entre los miembros de la comisión. Por un lado, la estabilidad del núcleo público fue garantizada por un sistema distribuido con unos servidores raíz, servidores SS, y entonces es difícil de hacer que deje de funcionar internet, no es que no hay un botón para que no funcione más, hay varios elementos que garantizan una cierta estabilidad. Por otro lado, lo que hemos visto en los meses y en los año recientes, es que existen ataque continuos a este núcleo público, recientemente secuestro del DNS nos muestra una dimensión que puede socavar la estabilidad y la seguridad de internet.

Pareciera que hay una norma especial para los actores estatales y no-estatales, es decir, que ninguno de los dos debe tocar ese núcleo público, entonces hay una garantía de que queda siendo estable, y que se debe trabajar en conjunto para encontrar a los criminales que planean hacer cosas inadecuadas para ese núcleo público.

También tenemos una discusión sobre los ataques contra este núcleo público de internet, que implicarían una categoría específica, digamos, del ciber-delito, porque hay un derecho penal interno, y hay delitos contra la humanidad, porque si atacamos el núcleo público, el internet es tan importante para tantas actividades en la vida hoy, que realmente esto podría tener una categoría especial.

Estos son temas de discusión, pero nuestro entendimiento de este núcleo público de internet, que debe ser muy cercano a la misión de internet, porque nosotros lo vemos como el sistema de ruteo de DNS, el sistema de números.

Cuando nosotros comenzamos una discusión, en conjunto con ICANN y con la comisión global, ICANN descubrió que el trabajo para la protección del núcleo público de internet, es uno de los elementos claves que tenemos. Nosotros venimos de distintos lugares, ICANN viene de lugar más técnico, nosotros venimos de un lugar más político, pero hay una intersección, y nosotros

estamos aquí para identificar estos temas. Vamos a tener una reunión con el Comité Asesor de Estabilidad y Seguridad hoy, y también va a ser muy bueno tener retroalimentación de la comunidad de los usuarios, de la comunidad de At-Large, para ver cuáles son los pasos políticos que se deben dar para proteger el núcleo público.

LATHA LEDDY: Le voy a pedir ahora a Marietje Schaake que presente la norma sobre el llamado para proteger la infraestructura electoral.

MARIETJE SCHAAKE: Gracias. En mi vida diaria soy miembro de parlamento y soy de los países bajos. Lo que tratamos de hacer con las normas es anclarlas en leyes internacionales, donde podemos hacerlo para no reinventar la rueda, sino más bien construir a partir de un conjunto de acuerdos. Estas normas están ancladas en dos principios jurídicos internacionales.

Uno es el de la no interferencia entre las naciones, que es parte de la carta de la O.N.U., y por supuesto es clave. La carta de la O.N.U. dice que todos los estados miembros deben evitar el uso de la fuerza o de las amenazas contra la territorialidad integral de cualquier estado o su independencia, en cualquier manera que sea inconsistente con el propósito de la O.N.U.

Cuando uno lee la declaración universal de los derechos humanos, se encuentra allí que el derecho a elegir sobre la base del sufragio universal y el voto secreto también está protegido en esta declaración universal.

Claramente, cuando miramos los procesos electorales, ya sea que sean con papel o con votos electrónicos, cada elección tiene ahora una parte digital, un componente de TI, y por supuesto hay mucha tensión en el debate al público sobre esta información, y nosotros nos focalizamos mucho en los asuntos que tienen que ver con la infraestructura técnica.

La norma que proponemos es la siguiente, y cito, la pueden leer allí en la pantalla, “los actores estatales y no-estatales no deben perseguir, apoyar o permitir las ciber operaciones que tiene la intención de interrumpir la infraestructura técnica que es esencial en las elecciones, referéndum o plebiscitos.”

Eso es todo.

LATHA REDDY: Gracias. También debemos decir que, cuando miramos la interrupción, también estamos analizando la infraestructura de las elecciones, es decir que no estamos teniendo en cuenta la desinformación o la mala intención, porque esencialmente

miramos como la infraestructura o la estabilidad de internet puede ser afectada.

Para la tercera norma le voy a pedir al señor Bill Woodcock que hable de esta, es una norma para los actores estatales y no-estatales que deben evitar manipulación de las distintas partes.

BILL WOODCOCK: Estamos hablando de los distintos ataques al DNS, que son similares a los que tienen los gobiernos que han intentado corromper la cadena de abastecimiento, introducir compromisos en productos en el proceso de fabricación. Por ejemplo, [missed] compromete la criptografía de la curva eléctrica, recomendada para muchas fábricas en la introducción de esos productos. No es un compromiso intencional por parte de los gobiernos de la seguridad de las partes centrales de internet, sino que se compromete porque las cantidades de fabricación terminan afectando a distintas porciones de internet, distintas partes, y no han sido seleccionados específicamente y no son proporcionales.

La norma entonces. Aquí, tiene la intención de proteger a los clientes de la corrupción de los dispositivos y el software que están comprando, por parte de los gobiernos, y también por los actores no-estatales, pero es más hacia el otro lado donde está orientado. Los actores estatales y no-estatales no deben

manipular, y tampoco se debe permitir que sean manipulados, si se amenaza la estabilidad de la ciber-seguridad, del ciberespacio.

Hay muchos políticos que están involucrados en este proceso y no tantos ingenieros. Le sedo ahora la palabra a usted.

LATHA REDDY: Vamos a pasar a la norma siguiente, que es la norma en contra del secuestro, o la apropiación de los dispositivos ICT.

OLAF KOLKMAN: Trabajo para la sociedad de internet. La norma anterior tenía que ver con un proceso de fabricación, esta norma es sobre los dispositivos que están abiertos. La norma entonces tiene que ver con dispositivos que se utilizan en ataques, y que están inspirados por ejemplo, que ocurrieron hace un par de años, y el hecho de que tenemos una gran cantidad de dispositivos IoT inseguros en el campo, que si se utilizaran conjuntamente, y se utilizaran como armas, causarían inestabilidad.

No solo eso, sino que si eso sucede, los usuarios de estos dispositivos podrán encontrarse comprometidos también, podrían verse como beligerantes, podrían haberse visto como a quienes conscientemente forman parte de los ataques, y también pueden ser visto como quienes están involucrados en operaciones militares.

Entonces, para poder capturar esto en una norma, hablamos de actores estatales y no-estatales que no deben utilizarse para botnets. El apoderamiento de estos dispositivos indica una desproporción de la naturaleza en masa de este uso. Y por supuesto los botnets y otros propósitos similares, porque no todos los ataques pueden estar instigados como un botnet, puede haber otro tipo de ataques, que son capturados allí también. Exactamente dos minutos.

LATHA REDDY: Gracias, Olaf. Vamos ahora a pasar a la norma para que los estados creen una vulnerabilidad en un proceso.

CHRIS PAINTER: Esto es a reacción a una atención que mucha gente está viendo entre los estados que tienen acceso a unas vulnerabilidades públicas, hay una atención entre mantenerla para la aplicación de la ley, o para las cuestiones de seguridad nacional, o divulgarlas en forma más general, y reconocemos que hay problemas en ambos lados.

Hay países que han creado un marco transparente con todos los actores del gobierno, no solamente los organismos nacionales sino otros organismos económicos y otros. Y tomaron decisiones,

la decisión de divulgarlos con una parte importante, que es que hay una presunción de que se deben divulgar.

Estados Unidos ahora tiene este proceso, lo mismo al Reino Unido, y al leer el artículo creo que vi también a Canadá, anoche, Canadá también lo está haciendo. Cuantos más países lo hagan, estamos sugiriendo que todo el mundo lo haga así, pero cuantos más países puedan ver estas equidades, va a haber un equilibrio, y va a haber una presunción respecto de la divulgación, o en favor de la divulgación.

LATHA REDDY: Gracias, Chris. Quisiera pasar a la norma siguiente que es la de reducir y mitigar las vulnerabilidades significativas. Jeff Moss es quien va a presentar.

JEFF MOSS: Gracias por tenernos aquí. Esta es la primera norma… aquí todas las normas hablan del rol del gobierno, entonces esta es la primera que se focaliza en los fabricantes, y quizás en la sociedad civil, los productores de la tecnología. La meta aquí es ser más transparente y reconocer la rendición de cuentas que hay que tener como productor de sistemas críticos, y tratar de reducir las vulnerabilidades que pueden impactar en la internet.

Me disculpo porque esta es una de las normas más largas, quizás la podría haber ampliado si hubiese tenido más tiempo.

La voy a leer para aquellos que pueden decodificarla. Los desarrolladores y productores de los productos y los servicios en los cuales la estabilidad del ciberespacio depende, deben priorizar la estabilidad. Tomar pasos, o dar pasos para asegurar que sus productos y servicios están libres de vulnerabilidades significativas, y tomar medidas para mitigar esas vulnerabilidades que luego se descubren, y ser transparentes respecto a sus procesos. Todos los actores tienen el deber de compartir la información sobre las vulnerabilidades y ayudar a mitigar las actividades maliciosas.

Voy a indicar un par de cosas. Una es que reconoce que los bugs afectan a la vida, no le estamos diciendo a la gente que haga softwares sin fallas, lo que estamos diciendo es que hay que hacer procesos para reducir estas fallas, hay que ser transparente, porque una falla, para una persona, o para un fabricante puede ser muy insignificante, pero ellos no se dan cuenta que el software está siendo utilizado en otro lugar del mundo, y hace que esta vulnerabilidad o esa falla sea muy significativa. Como no tenemos un conocimiento global sobre a dónde va a ser usada esa tecnología, se debe asumir que tiene impactos más allá del conocimiento y por eso debe ser transparente, cuando finalmente encontramos como remediarlo.

Esta norma está entre otras dos, entre la norma de no manipulación, y también va a haber una norma sobre higiene, que va a estar en el medio, entre cómo se deben comportar los fabricantes.

LATHA REDDY: Vamos a pasar ahora a la siguiente norma, que es la norma sobre la ciber higiene básica, como defensa fundacional. La va a presentar Abdul-Hakeem Ajijola.

ABDUL-HAKEEM AJIJOLA: Damas y caballeros, el éxito de la sociedad digital solamente se va a poder lograr cuando la confianza pública en su plataforma sea mejorada. Los datos de hoy son el componente fundacional de ciber poder, que influyen en la supervivencia. A medida que crece nuestra sociedad cada vez dependemos más de las fortalezas y las debilidades del ciberespacio. Corremos el riesgo de crear un futuro sobre la capacidad de que no hemos aprendido completamente como proteger.

La clave de dar una protección efectiva, es que nuestras defensas fundacionales sean adecuadas, por lo tanto, la norma del GCSC sobre la ciber higiene básica como una defensa fundacional, debe incluir medidas adecuadas que incluyen leyes y regulaciones para garantizar que hay una ciber higiene básica.

La norma del GCSC es, como fundación, adopta la implementación verificada de un régimen fundacional, que representa, prioriza, las tareas esenciales para defender, prevenir y mitigar rápidamente los daños del ciberespacio que se pueden evitar. Nosotros creemos que esta norma tiene un interés muy particular para los registros y registradores relacionados con los ISP y entre muchos, muchos otros.

Damas y caballeros, los régimen de ciber higiene deben incluir medidas de implementación, deben establecer cómo se comparte la información técnica y las buenas prácticas, y debe estar sujeto a un control adecuado. Si nosotros utilizamos este ejemplo, una polución podría impactar a los usuarios que consumen servicios hacia abajo, y no hacia arriba. Los dispositivos que cada vez son más inteligentes requieren leyes inteligentes, y al crear más rendición de cuentas para este ciber cuidado, los gobiernos no deben restringir la innovación que se encuentra en las propiedades básicas de internet.

La ciber higiene y las buenas prácticas ya existen en muchas maneras, y han sido, o han tenido mucha atracción y aceptación internacional. Sin embargo, nosotros debemos entender la importancia de adoptar medidas para demostrar, y ayudar a prevenir, y rápidamente mitigar los daños del malware, facilitar la conciencia, sigue siendo un obstáculo que debe ser atravesado en los desafíos y en las capacidades.

Bill Clinton una vez dijo, que si nosotros podemos curar el SIDA con un vaso de agua, no debemos dar esa cura a la mitad de la gente de Africa Sub-Sahariano, de donde yo vengo, y esa gente necesita ayuda.

En enero del 2019, solo en Nigeria, tiene más de 108 ciudadanos online, y por supuesto hay muchos otros ciudadanos online en India. Tristemente, hoy nosotros vemos que lo que dijo Bill Clinton está sucediendo en gran parte del mundo subdesarrollado, y se debe aplicar entonces esta norma del GCSC sobre la ciber higiene.

Además, la ciber higiene se aplica a los desafíos de las tecnologías emergentes y automatizadas, y a determinar a aquellos que tienen una responsabilidad sobre el impacto de esas tecnologías. Los rondas potenciales, y los avances en el beneficio humano están siendo perdidos porque nosotros no estamos pudiendo tener recursos disponibles para un mayor futuro, un mejor futuro. Por lo tanto es importante, damas y caballeros, que los estados aprueben leyes, incluidos leyes y reglamentaciones, para asegurar una buena ciber higiene. Gracias.

LATHA REDDY: Gracias, Abdul. Y la última norma que queremos presentar es la norma contra las ciber operaciones ofensivas por parte de actores no-estatales, y la presentará Frederick Douzet.

FREDERICK DOUZET: Gracias. Esta norma dice que los actores no-estatales no debieran participar en ciber operaciones ofensivas, y los actores estatales deberían prevenir y responder a estas actividades si ocurren.

La razón por la cual hicimos esta norma, es porque algunos actores no-estatales realizan acciones contra operaciones ofensivas en forma transfronteriza, y aducen que lo hacen para defensa propia, porque los estados no tienen la capacidad de protegerlos adecuadamente contra los ciber ataques, y estas operaciones ofensivas en general se llaman ciber defensa activa, y en su forma externa, represalia, es dejar que, son actividades que no se pueden controlar, o por lo menos no se pueden monitorear estas prácticas, entonces a veces deciden ignorarlas activamente.

En otros estados parece ser que no están ni claramente prohibidas, ni físicamente autorizadas, y además algunos estados han decidido, o proponen leyes, para permitir las operaciones ofensivas por parte de actores no-estatales en sus legislaciones nacionales.

EL GCSC cree que estas prácticas pueden socavar la seguridad de la estabilidad del ciberespacio, y resultar en disrupciones y daños graves, y también disparar disputas legales internacionales complejas y escalar los conflictos.

Basamos esta norma en el derecho internacional, y en particular en dos principios que fueron claves en la elaboración de la norma, y que emergen del principio de la soberanía de las naciones, por un lado los derechos que tienen los estados del monopolio y el uso ilegítimo de la fuerza, que está restringido estrictamente y objetivamente por los derechos internacionales, y también los derechos de las responsabilidades de los estados, el principio de diligencia de vida, que los estados no deben sabiendas, permitir que se use su territorio para actos que son contrarios a los intereses de otros estados.

LATHA REDDY: Gracias, Frederick. Bien, ustedes han escuchado la presentación de nuestras ocho normas, y antes de concluir nuestra presentación, le voy a pedir a mi presidente Michael Chertoff, que les cuente un poquito sobre nuestra definición y los principios que seguimos el GCSC, y la cuestión de la ciber estabilidad, ¿por qué? Por nuestro nombre ustedes ven que somos una comisión global sobre la estabilidad en el ciberespacio, esto entonces lo vemos con nuestra misión fundamental. Michael entonces hará una conclusión, de resumen.

MICHAEL CHERTOFF: Gracias, Latha. Nuestra definición de trabajo en este momento es algo así, la estabilidad en el ciberespacio, es la condición en la

cual los actores estatales y no-estatales, pueden tener confianza en su capacidad de usar el ciberespacio de manera segura, porque la disponibilidad de la integridad de los servicios en el ciberespacio está asegurada de manera general.

Permítanme desglosar esta definición un poquito. Aquí no estamos intentando decir que no hay que hacer nada malo en la internet, estamos hablando de cosas que afectan la estabilidad de la internet, incluyendo la percepción de la estabilidad, por el reconocimiento de que la gente no tiene confianza en la estabilidad de la internet, esto significa que la internet es inestable, sea estable o no esta percepción.

En segundo lugar, las lesiones o las amenazas a la estabilidad son de naturaleza general, no somos ingenuos los que reconocemos que razones legítimas, a veces, para que los estados naciones específicamente se focalicen en un rango muy específico, y eso no afecta la estabilidad general.

Pero si analizamos las normas, verán que están focalizadas en aquellas actividades que socaba las actividades generales de la internet, pueden ser los protocolos, o la infraestructura, o incluso los puntos de extremo. La idea es que, si estas puntas, si estas áreas se ven comprometidas y afectan la estabilidad, el sistema se ve realmente afectado.

Nuestra esperanza es que estas normas sean adaptadas por el gobierno, y por el sector privado, los fines de crear un entorno en el cual se tenga la confianza de que la internet sea funcional en el futuro.

LATHA REDDY: Gracias, Michael. Ahora, le devuelvo la palabra a Olivier, y le voy a pedir que por favor modere las preguntas.

OLIVIER CREPIN-LEBLOND: Gracias. Ahora vamos a abrir el piso a preguntas, para los que están en el panel, pueden levantar la tarjeta, y también tenemos micrófonos volantes, creo que están, si alguien ahí atrás quiere hacer un comentario, quiere hacer una pregunta, o hacer comentarios. Por favor, levanten la mano, y Gisella se acercará con el micrófono.

Empecemos primero con Hadia Elminiawi, que levantó la tarjeta primero. Vamos a ir entre los que están sentados en la mesa y los que están centrados en el público.

HADIA ELMINIAWI: Mi comentario se refiere a la norma, no recuerdo qué número era, era la que hablaba de la manipulación de los productos en su fabricación. Las leyes que surgen, que requieren a las empresas

entregar dados encrestados de extremo a extremo, esos de alguna manera ablega a las empresas a abrir puertas traseras al interior de su criptografía, de su encriptación. De hecho, no es una manipulación estatal o no-estatal, es la misma ley la que fuerza esta manipulación. A ver. O hace que los fabricantes incorporen esto en sus productos. ¿Cómo manejan este tipo de situaciones ustedes?

OLIVIER CREPIN-LEBLOND: ¿Quién va a responder?

JEFF MOSS: Dos observaciones generales. Primero, hablamos mucho ya de lo siguiente. Si los gobiernos proponen este tipo de cosas, como una entrada trasera en la criptografía, las empresas en el mundo comercial, no significa que la compañía va a dejar de ganar dinero, compañías como Apple, en general, resuelven este problema a través de su ingeniería. No tienen mucho personal luchando contra los requisitos regles, no me sorprendería entonces si los fabricantes específicamente diseñan sus productos para evitar estos problemas.

Y otro comentario, es este reconocimiento general de que la gente recopila datos, que básicamente, no se recopilan datos si no se los pueden proteger, y esto está relacionado con la norma

de transparencia. Si uno está obligado a incorporar estas backdoors, estas puertas traseras, por ejemplo, los productos australianos, los usuarios, los consumidores, van a evitar los productos australianos.

O sea, hay fuerzas que se alguna manera minimizan, a mí me parece que los gobiernos no van a conseguir lo que quieren. Inicialmente los mercados eran competitivos, eran otros lugares donde haya menos retos jurídicos, entonces en total, debemos reconocer que la comunidad internacional no está totalmente agrupada detrás de estos conceptos.

BILL WOODCOCK: Creo que el problema que usted está describiendo, es uno que bueno, reconocemos, entendemos. El abordaje que hacen los gobiernos que plantean este requisito en los fabricantes es incorrecto, y es contradictorio del espíritu de la no manipulación y de la vulnerabilidad, las normas no son explicitas hasta el último detalle, no pueden explicar todas y cada una de las posibles violaciones, lo hace desde una forma conceptual. Considera así el ataque del lado del lado de la oferta, y también la vulnerabilidad de los productos.

OLIVIER CREPIN-LEBLOND: Gracias, Bill. Él era Bill, para la transcripción. Usted tiene que decir su nombre por la transcripción y la interpretación. Pasemos atrás, y después tenemos más preguntas.

RICARDO HOLMQUIST: Si les parece voy a hablar en español. Los intérpretes deben trabajar. Yo quería, aquí las diferentes normas lucen bastante bien, pero hay diferentes actores involucrados, porque están compañías muy grandes, cuando hablamos por ejemplo de la norma que tenemos en pantalla, hablamos de gobiernos en muchos de los casos, pero en alguno de los casos, como el caso de las aplicaciones, van a ser compañías muy pequeñas las que vayan a estar allí. ¿Cómo espera este grupo que esto sea implementado a nivel de los gobiernos, a nivel de las compañías?, algo como la Convención de Budapest de Ciber Seguridad, ¿cómo se plantea el próximo paso?, las normas están muy bien, ¿cuál es el próximo paso? ¿Cómo ir a reforzar esto de alguna manera? Gracias.

CHRISTOPHER PAINTER: Eso es exactamente lo que estamos trabajando en la comisión en este momento, tenemos una serie de normas, que debo decir van a suplementar otras normas que saldrán de la O.N.U., y una de las cosas que habla la comisión ahora es la responsabilidad y la aplicación posible, representa muchos problemas. Debemos

reconocer que las normas solas no alcanzan, porque si no hay manera de rendir cuentas es solo un trozo de papel. Hay muchas maneras de manejarlo pero es precisamente lo que estamos trabajando ahora, que es parte del marco general.

FREDERICK DOUZET: En el documento de Paris, hay otras normas. No me acuerdo, varios gobiernos han respaldado el documento de Paris, muchas empresas también, así que espero que esto contribuya.

MARIATJE SCHAAKE: Uno de los motivos por los cuales estamos aquí, agradecidos de estar aquí, es que no solo se espera que ustedes, la sociedad civil y varias otras partes abracen estas normas, que consideren que son útiles, y convenzan a los gobiernos, a las empresas del sector privado y a otras partes. Que empiecen a avanzar hacia la aceptación, y después de la aceptación vendrá la responsabilidad.

Si existe alguna violación, no se ha pretendido que esto sea un proceso monopólico de la gente que está aquí a la mesa. Somos personas de distintas maneras de pensar, venimos de distintos lugares del mundo con distinto expertise, e intentamos elaborar algo que pensamos que puede ayudar a la estabilidad del

ciberespacio, y también dar confianza a la gente que está en el ciberespacio en el mundo.

OLAF KOLKMAN: Bueno, a ver, hubiera sido de otra forma. Nosotros esto no lo podemos hacer solos, necesitamos a las compañías, necesitamos a los estados, pero también a todos los otros actores. Esto es una convocatoria.

ABDUL-HAKEEM AJIJOLA: Voy a hablar desde otra perspectiva. Hay algo en los diez mandamientos que dice, "no cometerás adulterio", y así es que hay que tener una sola esposa, eso es para los católicos, pero para los musulmanes tampoco podemos cometer adulterio, pero nosotros podemos tener cuatro esposas. Entonces, la pregunta de una empresa grande, una empresa pequeña, bueno, aquí la norma se aplica por igual. Gracias.

OLIVIER CREPIN-LEBLOND: Bueno, vamos a pasar de la mesa al piso, uno y uno. John Laprise.

JOHN LAPRISE: Quisiera preguntarle al panel, ¿por qué no hay una norma para proteger a la estructura eléctrica? Y lo pregunto con el conocimiento, y acá hablo como académico, que hace 40 años en

los Estados Unidos, durante la guerra fría, el comité asesor de telecomunicaciones nacional dijo que el sistema de telecomunicaciones y el sistema eléctrico eran co-dependientes, porque dependían uno del otro para su control, si se caía uno no había manera de mantener el otro activo en funcionamiento, entonces, aquí la situación no es tan distinta, entonces la pregunta es: La internet es co-dependiente de la infraestructura eléctrica, entonces, ¿por qué no hay una protección?

CHRIS PAINTER: Yo diría que en naciones unidas en el comité de expertos también hubo una recomendación sobre la protección de la infraestructura eléctrica, también estamos respaldando estas normas. Tenemos que definir si estamos hablando de la red eléctrica como la infraestructura principal.

Tenemos primero que definir cuál infraestructura es más importante que otra, pero nadie ha hablado del núcleo de internet. Algunos dicen que estamos añadiendo algo al debate, hay quienes dicen que el núcleo de internet debe ser considerado también infraestructura crítica, como la infraestructura eléctrica. Esto no es que queríamos decir que no nos importaba, simplemente que queríamos tratar algo que no estuviera ya cubierto.

BILL WOODCOCK: En 2017, hicimos un relevamiento exhaustivo entre expertos de cuáles eran las estructuras que había que proteger, y la red eléctrica era de alto riesgo, se mencionó así. Y elegimos entre todos nuestros hijos solo cuatro, numeración en rotamiento, criptografía y cable. Ahí está lo eléctrico, pero no fue uno de estos cuatro elegidos. Hay otras cosas que se pueden proteger.

MICHAEL CHERTOFF: Tratamos de focalizarnos mucho en aquellas cosas que sean singulares de la operación de la internet. Por supuesto que es bueno proteger la infraestructura crítica, pero esto ya está cubierto por reglas existentes, como la DHS que conozco muy bien, pero quisimos focalizarnos y centrarnos en algo que no estuviera cubierto por reglas o normas ya existentes.

OLIVIER CREPIN-LEBLOND: Voy a pedir que las respuestas sean breves, porque tenemos siete u ocho personas. Olaf Kolkman.

OLAF KOLKMAN: Es importante que aquí, lo importante no es solo la infraestructura física, los cables y los puntos de intercambio. Sino también, lo lógico, el rotamiento, los estándares. Entonces, en ese sentido, esto es bastante nuevo. Es muy novedoso pensar en las estructuras intangibles que no queremos que se violen.

OLIVIER CREPIN-LEBLOND: El caballero en el frente, me parece que el micrófono se le acerca.

ABDULKARIM OLOYEDE: Yo soy Abdulkarim, permítame felicitarles por estas normas. Y creo no obstante que hay algo que falta, y me pregunto, ¿por qué? Que es el tema de la privacidad. ¿Hay algún motivo por el cual lo hayan dejado afuera?

LATHA REDDY: Debo decir que si usted lee la misión, dice que es mantener el ciberespacio estable. La privacidad y demás, es un gran tema, pero no afecta el funcionamiento o no-funcionamiento de la internet.

O sea, no es que no somos conscientes del problema, sabemos que es un problema muy serio, afecta cómo usamos la internet, pero creo que no es algo que vaya a hacer que el ciberespacio pierda estabilidad, si se manipula la privacidad. Es un tema importante, muy importante.

OLIVIER CREPIN-LEBLOND: Wolfgang?

WOLFGANG KLEINWAECHTER: Los derechos humanos tienen un efecto sobre la estabilidad del ciberespacio, y existe sin duda una inter-relación. La violación masiva de los derechos humanos tiene efectos negativos sobre la estabilidad del ciberespacio. Todavía no tenemos en claro cómo traducir este punto en un texto, pero existe una inter-relación entre el respeto de los derechos humanos y la estabilidad del ciberespacio.

OLIVIER CREPIN-LEBLOND: Suen Ojedeji.

SEUN OJEDEJI: Muchas gracias. Es una audiencia pública esta, me pregunto, ¿por qué no hay una norma sobre la infraestructura de internet que causa lo que nosotros llamamos shutdown de la internet, o baja o caída de la internet? ¿Por qué no está reflejado en la lista? Si está ya cubierta en alguna de las normas, quisiera saber en cual.

Además quiero decir que es muy bueno que exista una manera de ver los efectos de estas normas, entonces quizás puedan considerar una manera de hacer un seguimiento, un rastreo de los efectos. Gracias.

OLIVIER CREPIN-LEBLOND: ¿Alguna respuesta?

JEFF OSS: Todos estamos de acuerdo, si entendí bien su pregunta, un ataque en contra de la infraestructura del routing. Cómo funcionalizamos algunas de nuestras normas, la comunidad de certificados, quizás el observatorio de la internet, o quizás un observatorio de normas. ¿Qué países o compañías han aceptado estos principios? ¿Qué compañías parecen estar violándolos? ¿Qué compañías siempre lo harán?

Porque lo primero que pasa cuando se intenta socializar estas normas, es que surgen en la identificación de quienes son los buenos y los malos. Entonces, esperamos, no nosotros sino a través de socios adecuados, quizás tener algún tipo de observatorio, o manera concreta de poner en funcionamiento estas normas.

BILL WOODCOCK: Aquí, estamos hablando… dos ejes tenemos, uno es si un país o una organización ha expresado que va a adoptar una norma, y el otro es el aspecto de cumplimiento o adición. Creo que podemos hacer un rastreo de ambos, es fácil decir quien dijo que esta norma representa su visión, su entendimiento del comportamiento.

Ya tenemos varios países, básicamente todos los países europeos, media docena de Las Américas, media docena de África, y otros tantos de la región hacia Pacífico. Luego, tenemos que ver si los países hacen cosas que violan estas normas, porque alguien puede decir que apoya una norma y después no sé, la agencia de inteligencia o los militares las violan, entonces tenemos que manejar estas dos cosas a la vez.

OLIVIER CREPIN-LEBLOND: Creo que vamos a tener que ir a las preguntas, todavía hay cuatro personas, y nos quedan solo diez minutos.

ELLIOT NOSS: Quiero felicitar a todos ustedes por este trabajo, yo estaba esperando públicamente lo que yo llamo un proceso de múltiples actores sobre la ciber seguridad, y esto pareciera ser que es la génesis. En ese sentido, quisiera alentarlos a que hagan un par de cosas.

Una, por favor asegúrense de que queden separados de éste proceso. Y quiero decir con esto, que ICANN tiene un mandato específico, ustedes tienen el suyo propio, y ustedes son igual de importantes y separados, y el modelo de múltiples partes interesadas va a florecer cuando exista un foco vertical.

Dos, aprovechen esta comunidad y este trabajo. Y lo pueden hacer de un modo muy específico, primero tendrían que venir a estas reuniones en forma regular. Uno de los beneficios que ustedes pueden tener de eso, es tratar de que exista una presenta significativa de aplicación de la ley aquí, y en todo el mundo.

Al menos, de acuerdo con el diagrama de la parte principal, ustedes no son parte principal del modelo de partes interesadas, ustedes también generan un efecto real, en como el mandato de ustedes va cambiando, y también van a tener que tener aplicación de la ley, como una parte necesaria de aplicación de la ley, quizás para ustedes en términos de ciber seguridad va a ser lo que el GAC ha sido para la comunidad de la ICANN, es decir, primero empezó con unas reuniones privadas y muy lentamente se fue convirtiendo en algo más integrado.

Va a ser un proceso largo, y quiero alentarlos a que aprovechen la mayor cantidad de lo que puedan.

LATHA REDDY: Quiero agradecerle, usted puede ver que hay seis de nuestros comisionados que en algún punto han tenido interacción muy amplia con la ICANN, y nosotros somos muy conscientes de lo que hace la ICANN, lo conocemos muy bien.

Creo que tenemos la atracción suficiente, y tomamos nota de lo que usted nos dice, que no debemos ser subsumidos dentro de los procesos de la ICANN. Gracias. Olaf.

OLAF KOLKMAN: Uno de nuestros comisionados es un líder, y eso lo hemos capturado en la comisión. Nos queda muy claro a nosotros que nuestro enfoque es hacia el modelo de múltiples partes interesadas. También nos queda en claro, que esta es una comunidad que tiene un mandato muy específico, y nosotros creemos que ese núcleo público se acerca a este otro.

Lo que hemos tratado de hacer con la comisión es ir a distintos lugares, donde las unidades constitutivas están presentes. Eso no constituye necesariamente la aplicación de la ley, pero sí incluye por ejemplo el lado más militar de la ciber estabilidad, y el lado más político de la ciber estabilidad. Por eso estamos tratando de posicionar las normas, tener retroalimentación, en mi propia comunidad de la sociedad de internet, que estamos tratando de hacerlo también.

Y por eso estamos aquí. El problema es que tenemos un mandato que dura un año más, y por lo tanto, involucrarse profundamente en los procesos de ICANN sería un desafío.

OLIVIER CREPIN.LEBLOND: Tenemos que terminar a las y cuarto, quizás las preguntas puedan venir después. Tiene la palabra Jonathan Zuck, Holly Raiche y el caballero que se paró. Vamos a ir alternando. Adelante Jonathan.

JONATHAN ZUCK: Estábamos hablando de la interacción, creo que usted va a decir cuál es la aplicación de la ley, y sería interesante qué significa eso, pero dar nombres puede ser un poco complicado. Mi preocupación sobre las normas es algo que nosotros compartimos, y luego esto se convierte en una carrera armamentista, donde todo el mundo está diciendo que, "usted vino primero", etcétera, y se convierte en algo difícil.

Estoy tratando de pensar en ejemplos de la historia, como Los Principios de Sullivan, que podrían ser un ejemplo donde habría una presión pública de que la gente cada vez participe más. Mi idea es tratar de que estas normas sean tomadas por una organización que ya tiene una infraestructura de cumplimiento.

Hay organizaciones como la WTO, que ya tienen una membresía, y entonces hacer que estas cosas puedan ser interpretadas de maneras diferentes. Hay organizaciones que ya tienen una infraestructura para monitorear la aplicación de la ley, una organización donde la gente ya siente que la inversión puede ser una buena salida.

OLIVIER CREPIN.LEBLOND: El señor que está al lado de Nigel Hickson, preséntese por favor.

NANO DORWICH: Hola, mi nombre es Nano Dorwich, vengo de Serbia. Quisiera dirigir mi pregunta a Frederick Douzet. Hasta donde yo sé, la ICANN participó en al menos una, o más operaciones para identificar una gran cantidad de dominios y darlos de baja, que fueron utilizados para botnet o extorciones cibernéticas.

La pregunta es si la inclusión en esa operación va en contra de la norma que usted presentó.

OLIVIER CREPIN.LEBLOND: Le vamos a dar a Frederick algunos minutos para pensar en la respuesta y vamos a ir a Holly Raiche.

HOLLY RAICHE: De Australia. Quisiera preguntarles, ¿qué hicieron con la ley de acceso y asistencia del año 2009? Si hicieron alguna declaración, quisiera que me lo cuenten.

OLIVIER CREPIN.LEBLOND: Habla Holly, en Australia.

FREDERICK DOUZET: No quisiera ir a esta invitación de nombres, porque eso sería atribución y eso es muy político. La meta de modificar normas, y la violación de normas es más para entender las tendencias. Es decir, está viendo algún progreso con la ciber estabilidad, y también está dando un análisis legal sobre los casos anteriores para poder ir construyendo casos que ayuden a entender cómo se aplica nuestro derecho internacional al ciberespacio, y monitorear cuales son las normas que están siendo respetadas o violadas.

En cuando a dar de baja los botnets, y las operaciones líderes, de nuevo, la idea es que los estados tienen los monopolios, y ellos son legítimos de la fuerza, por lo tanto todo depende si eso se hace porque el estado pide que se haga, o si uno lo hace propio.

Pensamos que si los estados los autorizan a ustedes a hacerlo, porque hay una necesidad de hacerlo, en ese caso se considera un organismo del estado, y por lo tanto, en el derecho internacional, el estado se considera responsable.

MICHAEL CHERTOFF: Creo que usted está hablando de la ley de Australia que requiere la encriptación. Todavía no llegamos al punto en el que tenemos que hacer presentaciones, porque no hemos votado las normas plenas, pero creo que se puede tener un buen argumento de que hay vulnerabilidades que abarcan este tema.

Yo creo que esto va a estar pendiente durante bastante tiempo. Una de las cosas que hacemos una vez que finalicemos nuestro informe final, es hacer defensa, y hay situaciones en donde las cuestiones que nosotros hacemos son incompatibles con las normas.

OLIVIER CREPIN.LEBLOND: Le damos la palabra a Chris Painter.

CHRIS PAINTER: Quisiera agregar algo de lo que dijo Frederick. Lo que hace Microsoft tiene que ver con órdenes judiciales, ellos hacen esas bajas y trabajan con los gobiernos. Creo que no estaría prohibido con nuestra norma.

En cuanto al sin nombres y culpabilizar, creo que tenemos que pensar que esta no es una comisión que lo pueda hacer en sí. Pero tiene más que ver con las expectativas que tenemos, porque yo creo que la mayoría de nosotros vemos una tendencia que empeora y no mejora, incluso con estas normas no pareciera que esto mejore, así que tenemos que ver cómo los cambiamos.

OLIVIER CREPIN.LEBLOND: Gracias por esto, Chris.

MARIT JESHAAKE: Quisiera referirme a lo que usted dijo, sobre buscar instituciones existentes donde la aplicación de los estados ya existe. Esta es la línea de pensamiento en la que nosotros estamos, pero no hemos trabajado plenamente aún la adherencia, las normas, la atribución, la rendición de cuentas, la responsabilidad, pero tomamos notas de su punto.

Definitivamente es la línea que nosotros adoptamos. Es decir, que nosotros podemos ver a partir de mi respuesta que no consideramos que hayamos terminado todo esto que está siendo profundizado y trabajado. Trabajamos muy intensamente para consultar con la gente, para que haya mejores respuestas, resultados, y para mejorar las normas y la implementación que ustedes están viendo hoy.

OLIVIER CREPIN.LEBLOND: Me dicen que está viniendo el próximo orador, que todavía no llegó, así que tenemos dos minutos más. Ustedes tienen que irse a otro lado. Algunas. Bueno, Wolfgang entonces no va a poder hablar porque acaba de poner de pie. Vamos a ir entonces a la pregunta del caballero de barba atrás.

DIEGO CANABARRO: Hola. Mi nombre es Diego y vengo de Brasil. Trabajo para la comisión directiva de internet de Brasil. Quiero tener una

información, todos se van, pero se mencionó algo con respecto a la capa lógica del ciberespacio. Quisiera poder entender un poco más la concepción que tienen ustedes del núcleo público, porque hay mucha literatura que discute qué es lo que es público, qué es lo que es privado, en la gobernancia de internet.

Aparentemente, gran parte de lo que ustedes dicen tiene que ver con el núcleo público, es decir, el ciberespacio que está en menos de actores privados, los cables submarinos, la infraestructura de ruteo, y otras infraestructuras que están 80% en manos del sector privado. ¿Cuáles serían las implicancias de publicitar estas cuestiones, al aplicar el concepto que tienen ustedes del núcleo público a esos activos privados?

LATHA REDDY: Yo creo, que si miramos las explicaciones que nosotros presentamos sobre el núcleo público, dijimos que la tecnología que está por detrás de la internet global es imperfecta. Si nosotros consideramos el núcleo público como una infraestructura pública, la tecnología puede dejar de funcionar, y la existencia de los actores maliciosos y las vulnerabilidades, y el desarrollo de capacidades que pueden crear condiciones de inestabilidad que puedan beneficiar, o puedan poner en peligro el beneficio del ciberespacio.

Nosotros tratamos de delinear cuales son los elementos técnicos que nosotros consideramos, que pueden afectar esencialmente el núcleo público, es decir, que evitan que el internet deje de funcionar. No creo que haya uno que sea más importante que el otro, nosotros esencialmente estamos mirando, o analizando, cualquier asunto que pueda evitar que internet deje de funcionar como tiene que funcionar, y nosotros claramente decimos que esto se aplica a los actores estatales y no-estatales.

OLIVIER CREPIN.LEBLOND: Gracias, Latha. Anriette también es parte de la comisión así que adelante.

ANRIETTE ESTERHUYSEN: Gracias, Olivier. Quiero agregar a la pregunta de Diego, porque me parece que es una pregunta fundamental. El punto sobre la norma del núcleo público, es que no importa si esa parte de internet que constituye el núcleo público está gestionada por una entidad privada o no. Lo que importa, es que está gestionada en el interés público como uno diría en ICANN, o para la estabilidad y flexibilidad general de internet.

Esa es la razón por la cual nosotros abordamos los actores estatales y no-estatales. Es decir, no es publicitarlo más, sino que todo esto ya es público.

CHRIS PAINTER: Una cuestión más. Nosotros redactamos esta norma durante mucho tiempo, y gastamos el tiempo. Porque entendemos que hablamos de interrupciones sustanciales de internet, interrupciones breves. En la medida en que los actores y los gobiernos digan, "tenemos que hacer ciertas cosas de internet para la aplicación de la ley", etcétera, nosotros no estamos prohibiendo nada, estamos siendo claros, y entendiendo qué es lo que ellos tienen que hacer.

Pero, si hacen algo que tiene una interrupción sustancial que afecta a todos en la comunidad, o a una sección de ese grupo, ahí es donde tratamos de actuar.

OLIVIER CREPIN.LEBLOND: Muchas gracias, Chris. Si hay más preguntas sobre este tema, quisiera sugerir que se las envíen al personal, por e-mail staff@at-large.icann.org y se las vamos a responder. Muchas gracias por haber venido a vernos, es un verdadero placer.

LATHA REDDY: En representación de la comisión global, quisiera agradecerles por su tiempo, atención y paciencia. Ha sido un placer tener esta consulta pública junto con la ICANN, con el Comité Asesor de At-Large, y le agradecemos a Olivier por su presidencia aquí.

OLIVIER CREPIN.LEBLOND: Tenemos ahora a Keith Drazek que está llegando a la sala, y le voy a dar la palabra a Cheryl Langdon-Orr. Por favor no se vayan, porque todo esto continúa.

MUJER NO IDENTIFICADA: Damas y caballeros, estamos por empezar la siguiente sesión con el presidente de la GNSO, miembros de regionales de ALAC y enlaces, por favor acérquense a la mesa. Muchas gracias.

CHERYL LANGDON-ORR: Damas y caballeros, por favor tomen asiento. Si son ALAC o At-Large líder regional, y si hay asientos de sobra, por favor vengan los de atrás, porque nosotros somos individuos paranoicos y preferimos verlos. Siéntanse en libertad de venir aquí en frente, sentarse en la mesa si así lo desean.

Con esto, vamos a ver si lo digo en voz baja a ver si funciona. Muchas gracias.

Para quienes no me conocen, prefiero hacerlo así. Soy Cheryl Langdon-Orr. Es un privilegio para mí ser enlace de ALAC ante el consejo de la GNSO, creo que es el privilegio de Keith, el presidente recién llegado del consejo de la GNSO. Esperemos que él no vuelva a disfrutar de un café.

Tenemos también cosas que son muy importantes y que están sucediendo con lo que nosotros estamos haciendo como comunidad de At-Large, en respuesta a nuestra propia revisión de las regiones en At-Larga.

Lo que queremos hacer, es estar más involucrados en política, y estar involucrados más directamente y obviamente. Queremos diseñar el 3.0, así que queremos escuchar un poco más cómo funciona la GNSO, porque cuando hacemos muchas unidades constitutivas, y grupos interesados, que piensan que ALAC somos todos nosotros. Un poco sobre la estructura y la función, yo sé que usted no es la GNSO, sino que es una cara distinta. Y que luego nos cuente qué es lo que va a suceder con el PDP 3.0, porque lo que estamos haciendo, es que estamos tratando de que más gente participe en el proceso de desarrollo de políticas. Adelante Keith.

KEITH DRAZEK: Gracias, Cheryl. Gracias por la invitación de estar aquí con todos ustedes hoy. Mi nombre es Keith Drazek, soy el presidente actual y nuevo del GNSO. El consejo de la GNSO tiene un proceso de desarrollo de políticas, para el desarrollo de las políticas. El consejo de la GNSO está haciendo este desarrollo, no solo yo.

Me complace venir a hablarles sobre la infraestructura de la GNSO, y de la evolución de la participación de los consejos en el

proceso de PDP. Primero, quiero decir que estamos muy contentos de tener miembros de ALAC que participen en el proceso de la GNSO, particularmente los ejemplos más recientes están en los procedimientos posteriores en la Vía de Trabajo 5. Usted es co-presidente de ese PDP y le agradecemos por ese sacrificio.

También el EPDP habrá reemplazado las especificaciones temporarias, le agradecemos a Hadia, a Alan, por el enorme sacrificio y la gran cantidad y de intensidad que se requiere ahí. Ha sido titánico realmente este informa que se ha presentado dentro de los plazos establecidos por la especificación temporaria, esto es algo que se debe tener en cuenta. Sé que todavía hay frustraciones, con el trabajo que no se hizo en la fase 1, pero como gerente de los procesos de política de la GNSO, nosotros queremos asegurar que esto se va a iniciar, que haya los recursos adecuados, el alcance adecuado, y que se declare la urgencia para el acceso estandarizado y la divulgación de los datos de registro no públicos. También esto se llama el modelo de acceso unificado.

Desde la perspectiva del consejo, nosotros estamos plenamente comprometidos a asegurar la carta, creemos que todavía es adecuada y estamos preparados para soportar, o apoyar al EPDP a que desarrolle un plan de trabajo y establezca cuáles son las expectativas hacia adelante.

El consejo de la GNSO continúa brindando lineamientos al grupo de trabajo de EPDP durante las próximas semanas, todavía la pelota está del lado de la cancha del EPDP y tenemos que encontrar un nuevo presidente. Como ustedes saben, Kurt Pritz indicó que el trabajo después de la fase 1, él iba a retirarse y no estaba preparado para la fase 2. El consejo de la GNSO no ha hecho el llamado a personas de interés para un nuevo presidente para el trabajo de la fase 2. El plazo para esto será el 22 de Marzo, esperamos poder recibir suficientes declaraciones de interés, para luego pasar el proceso de selección y que sea aprobado por el consejo de la GNSO que se va a reunir el 18 de Abril.

Quiero dar un paso hacia atrás. La estructura del consejo de la GNSO, y la GNSO en general, para aquellos que no están familiarizados, es una estructura bicameral, tiene dos cámaras efectivamente dentro del consejo de la GNSO.

Está la cámara de las partes contratadas, que consiste en registros y registradores en dos partes interesadas. Y la cámara de partes no-contratadas, donde tenemos el grupo de partes interesadas y no-interesadas, y no-comerciales, donde se tratan todos los intereses, desde la propiedad intelectual, la unidad constitutiva de usuarios no-comerciales, el ISPCP, los intereses sin fines de lucro, así que hay varios intereses en los grupos no-contratados.

A nivel del consejo hay un presidente que es seleccionado dentro de los consejeros en el grupo, y luego hay dos vicepresidentes, uno de cada una de las cámaras, la contratada y la no-contratada. Ese es esencialmente el equipo de liderazgo del consejo de la GNSO, y luego tenemos a los consejeros en cada uno de estos grupos.

Hay una buena gráfica en el sitio web de la ICANN en GNSO.ICNN.org que tiene una representación visual, si alguien quiere hacerle un seguimiento a esto.

Entonces, en breve tenemos una interacción continua con ALAC, con el GAC y con otras partes de la comunidad, y tenemos un trabajo de PDP continuo. Hablamos entonces de los procedimientos posteriores, Vía de Trabajo 5, del EPDP, y a medida que miro hacia adelante, y hablo del PDP 3.0, creo que hay una expectativa de que va a continuar habiendo una oportunidad.

Una de las cuestiones que experimentó la GNSO durante los últimos seis o siete años, o incluso antes, que creo que apreció en la última ronda del desarrollo de políticas de la GNSO que culminó en la guía del solicitante del 2012, fue que teníamos una política de la GNSO dentro de una burbuja, y después el GAC vino con un asesoramiento de la junta, como un ejemplo. Creo que hubo un reconocimiento en ese punto de que íbamos a tener que

ser más efectivos en nuestro trabajo de políticas si hubiésemos tenido los aportes como parte del proceso.

Remontándonos a muchos años atrás, la GNSO, y me pareció que esto tiene que ver con Jonathan Robinson que era el presidente en ese momento, es decir que eso fue hace tres o cuatro presidentes. Hubo una difusión activa hacia el GAC, ahora nosotros reconocemos que cuanto más podamos hacer participar el interés de la gente en los comités asesores en nuestro proceso de desarrollo de políticas lo más temprano posible, mejor va a ser para que no terminemos con sorpresas al final, donde hay un asesoramiento que entra en conflicto con las recomendaciones de políticas, y creo que lo que estamos viend0 hoy es prueba de que eso efectivamente es útil, es bienvenido y es cumplir.

Creo entonces ciertamente que, durante mi tiempo como presidente, yo estoy comprometido a garantizar de que tengamos unos procesos inclusivos en el trabajo de PDP, en el que regularmente invitamos a cualquiera que quiera participar, y estar en esos grupos.

Específicamente sobre el PDP 3.0, el año pasado, el consejo bajo la presidencia de Heather Forrest, hubo un reconocimiento en el que tuvimos PDPs que siguieron durante años y años, y en algunos casos algunos años más. Tuvimos PDPs que continuaron

durante cuatro años. Tuvimos incluso algunos como el grupo de trabajo de PDP del RDS que se acaba de cerrar después de trabajar durante tres años, y por supuesto eso fue en parte por el GDPR por las especificaciones temporarias, por el reconocimiento de que el mundo cambió desde el momento en que se creó ese grupo.

Creo entonces que haya un reconocimiento del consejo del año pasado, en el que nosotros teníamos que hacer un mejor trabajo como gerentes del proceso para PDPs, y garantizar que haya un alcance adecuado, que los grupos se creen de un modo que sean efectivos y eficientes, y esas son las palabras centrales que tenemos que tener en cuenta, efectividad y eficiencia en nuestra gestión de estos PDPs.

Incluyo el reconocimiento de que nuestros enlaces del concejo a los grupos tenían que ser más participativos, activos y tenían que estar disponibles para que se recuerde qué es lo que sucedió, en caso de que hayan desafíos en el proceso, o cómo un presidente pudo haber operado por fuera de las normas y los procedimientos.

El año pasado atravesamos un proceso que resultó en aproximadamente 16 recomendaciones para mejorar nuestra capacidad en el consejo de ser mejores gerentes del proceso, y asegurarnos que no terminemos con PDPs que duran cuatro

años, y terminemos con PDPs que funcionan bien, y que si hay un problema para cumplir a tiempo, o si la dinámica en el grupo, y en el liderazgo, que tengamos una alerta temprana para prepararnos para tomar medidas para que todo esto funcione adecuadamente.

También reconocemos que el ancho de banda digamos, de los voluntarios, es limitado, al igual que del personal. Si tenemos reuniones presenciales, ese costo, bueno, la imitación de presupuestos de ICANN, tenemos que priorizar mejor. Esa es una de las palabras claves, priorizar el trabajo. Cuando surge algo nuevo, el EPDP, por especificación temporaria, bueno, hay que reconocer en algún momento que hay otra cosa que hay que poner en pausa, porque es un límite de lo que podemos hacer, y esto se aplica en especial si son varias las partes de la comunidad que participan, no es solo la lente de los recursos de la GNSO, sino una consideración comunitaria.

Aquí están las recomendaciones que surgieron del año pasado, en este momento estamos implementándolas. No es que a partir de ahora todos los PDP van a ser iguales, vamos a ir evaluando a medida que avancemos, y a medid que surjan nuevos procesos de desarrollo de políticas, o que consideremos nuevos PDP, veremos si hay maneras de ajustar, si es necesario hacer algunas modificaciones de las cartas orgánicas de los grupos, a fin de garantizar que se haga una entrega efectiva y oportuna de los

resultados finales, y del informe, porque eso es lo que dice la recomendación.

Y lo último, y después las preguntas. Les doy un ejemplo, en este momento se está hablando de qué pasa con el grupo de trabajo del EPDP sobre las medidas de protección de derechos de todos los gTLDs. Hay un trabajo de fase 2 que va a hablar solo del UDRP.

Se está discutiendo si el consejo tiene que redefinir la carta para tener un proceso más eficaz, es un ejemplo de cómo queremos implementar estos cambios. Gracias.

CHERYL LANGDON-ORR: Muchas gracias. Les pido disculpas al equipo de traducción. Vamos a bajar un poquito la velocidad para poder decir todo lo que hay que decir. Bueno, gracias Keith. Tenemos que permitir que Keith se vaya a su próxima reunión, para que no llegue tarde. Así que rápidamente las preguntas breves, y breves las respuestas. Jonathan primero.

JONATHAN ZUCK: Con respecto a los PDPs más cortos, un par de historias de éxitos, tiene que ver con este CCWG con el marco de responsabilidad y el EPDP. Ambos fueron externalidades que crearon plazos, parte de su priorización tiene que ver con limitar los tiempos de un PDP,

establecer plazos para los PDPs y luego ajustar los PDP a los plazos.

KEITH DRAZEK: La respuesta corta es, sí. Es una de las cosas que estamos discutiendo, y sin duda es una consideración. Hay retos, en esto de establecer tiempos arbitrarios en algunas instancias, pero en otros casos puede ser muy eficaz, y sin duda uno de los componentes que se está considerando para el PDP 3.0, y pido disculpas a los intérpretes.

CHERYL LANGDON-ORR: ¿Holly?

HOLLY RAICHE: Volviendo atrás a la revisión, una de las recomendaciones que parecía estar enterrada, era una colaboración entre la GNSO y el ALAC, por ejemplo a través de webinars, desde el día uno, ICANN tuvo la oportunidad de este tipo de asesoramiento, de mejorar la participación. Sería muy útil, y sería bueno también hacerlo en dos husos horarios.

KEITH DRAZEK: Muchas gracias, Holly. Tomo nota. Algo similar nos dijeron en la última reunión con el GAC, en especial respecto de la carta del

EPDP. Había interpretaciones o entendimientos o expectativas que quizás no se entendieron bien, y no hubo oportunidad para participar en una etapa temprana, así que tomo nota de sus sugerencias, es sin duda algo que vamos a considerar, y en dos husos horarios.

CHERYL LANGDON.ORR: La costa. Tiene que ser los husos horarios correctos, ¿no? La costa este y oeste de los Estados Unidos. Bueno, ahora aprovechemos para agradecerle a Keith por su presencia, tuvimos poco tiempo con usted pero muy valioso. Ahora, nos gustaría saber si en el futuro tendremos tiempo con usted, quizás no con usted, sino con su equipo, o algunos de los otros líderes del consejo de la GNSO para poder compartir y comprender un poco más.

Damas y caballeros, tenemos otra sesión que empieza en tres minutos. Keith se va, muchísimas gracias Keith.

KEITH DRAZEK: Muchísimas gracias a todos, anhelo volver a reunirme con ustedes, y la próxima vez prometo tener más tiempo para preguntas. Gracias.

[FIN DE LA TRANSCRIPCIÓN]