ICANN | منتدى السياسات الافتراضي – العروض التقديمية لبرنامج NextGen اليوم 1
الاثنين، 14 يونيو/حزيران 2021 – من 14:30 إلى 16:00 بالتوقيت الصيفي لوسط أوروبا

ديبورا إسكاليرا: حسنا، أشكركم جميعا على حضوركم معنا اليوم. طابت أوقاتكم أينما كنتم. أهلا ومرحبا بكم إلى عرض ICANN71. اسمي ديبورا إسكاليرا، وأنا أعمل في قسم دعم المسؤولية العامة، وأسير برنامج NextGen@ICANN. وسأكون مسير المشاركة عن بعد في هذه الجلسة. يرجى العلم بأنه يجري تجيل هذه الجلسة وأنها تتبع معايير السلوك المتوقعة في ICANN. أثناء الجلسة، سيتم قراءة الأسئلة أو التعليقات فقط بصوتٍ عالٍ إذا ما تم تقديمها في صندوق الأسئلة والأجوبة. وسأقرأها عليكم بصوتٍ عالٍ في الوقت الذي يحدده رئيس هذه الجلسة أو مديرها.

ستتضمن الترجمة الفورية للجلسة عدة لغات. انقروا فوق ترجمة ICANN في Zoom وحددوا اللغة التي ستستمعون إليها خلال هذه الجلسة.

وإذا أردتم التحدث، فيُرجى منكم طلب الكلمة في غرفة Zoom، وبمجرد مناداة مسير الجلسة على اسمكم، سيساعدكم فريق الدعم الفني على إيقاف كاتم صوت الميكروفون عندكم. وقبل التحدث، تأكدوا من تحديد اللغة التي ستتحدثون بها من قائمة الترجمة الفورية. يُرجى ذكر اسمكم للتسجيل واللغة التي تتحدثون بها إذا كنتم تتحدثون لغة أخرى غير اللغة الإنجليزية.

وعند التحدث يتعين التأكد من كتم صوت جميع الأجهزة والإشعارات الأخرى. ويُرجى التحدث بوضوح وبسرعة معقولة للسماح بالترجمة الدقيقة. يمكن لجميع المشاركين في هذه الجلسة تقديم تعليقاتهم في الدردشة. للقيام بذلك، يرجى استخدام القائمة المنسدلة في مربع الدردشة أدناه وتحديد "Respond to All Panelists and Attendees" (الرد على جميع أعضاء اللجنة والحضور). فسيتيح ذلك للجميع الاطلاع على تعليقك.

ويُرجى ملاحظة أن الدردشة الخاصة ممكنة فقط بين أعضاء اللجنة بتنسيق ندوات Zoom عبر الويب. أي رسالة يرسلها عضو في اللجنة أو حاضر عادي إلى حاضرين عاديين آخرين سيراها أيضًا مضيفو الجلسة والمضيفون المشاركون وأعضاء اللجنة الآخرون.

حسنا، أريد أن أتقدم بشكر خاص لمرشديَّ الذين كانوا يساعدونني مع الطلاب، كانوا يساعدونهم في التحضير خلال الأسابيع التي تسبق ICANN71. لقد قاموا بعمل رائع. شيري ستابس وأريس إجناسيو وديسالين يهوالا. شكرًا جزيلًا. لقد كانوا مصدر دعم لا يصدق لي، لقد ساعدوا

الطلاب في التحضير ل ICANN71، لقد كانوا مرشدين مذهلين يساعدونهم على الاستعداد لـ ICANN 71، يقودونهم خلال العملية ويعدونهم لهذا اليوم.

أول مقدم عرض معنا هو دانيال غولوبف، ونأمل أنه موجود ومستعد للانطلاق. فرناندا، زميلتي في العمل، تساعدني في تشغيل الشرائح اليوم. شكرا جزيلا لك يا فرناندا، على مساعدتك لي اليوم. دانيل، هل أنت في غرفة الدردشة؟

دانيل غولوبف: نعم، أنا كذلك، وأنا مستعد للانطلاق. مرحباً بكم جميعاً.

ديبورا إسكاليرا: حسنًا. إذن، أذكر جميع مقدمينا بأن يتكلموا ببطء وبوتيرة معقولة لأن مترجمينا سيترجمون كل ما تقولونه. وأذكركم أيضا أن تقولوا "الشريحة التالية، رجاء" لفرناندا. شكرا جزيلا يا دانييل، يمكنك أن تبدأ.

دانيل غولوبف: حسنًا. مساء الخير لكم جميعاً يا زملائي الأعزاء. أود أن أتحدث عن قضية محددة نوعا ما، حول مواقف جمعية التكنولوجيا الرقمية الروسية من تنظيم الإنترنت والوضع العام لحرية الإنترنت في روسيا. إن هذه بطبيعة الحال قضية محددة إلى حد ما، ولكن من الممكن عكس هذه القضية من روسيا على بلدان أخرى. الشريحة التالية، من فضلك.

إن في روسيا جمعيات تهدف إلى تطوير صناعة الإنترنت، وتسمى جمعيات الإنترنت. و[غير مسموع] وجودهم وطبيعة [غير مسموع] تختلف. وكان المعيار الرئيسي لاختيار الجمعيات التي سيشملها هذا العرض هو أن تكون مستقلة عن الدولة. ولكن، إذ قمت بتحليل عمل هذه الجمعيات، فقد لا يبدو ذلك صحيحا تماما، وقد حاولت في هذا العرض تحديد مواقف الجمعيات من لوائح الإنترنت التي يتم التعبير عنها بوسائل مختلفة.

لقد فكرت في استخدام هذه الجمعيات و المنظمات الروسية في هذا العرض: رابطة حماية حقوق التأليف والنشر على شبكة الإنترنت واتحاد وسائط الإعلام والاتصالات والمركز العام الإقليمي لتكنولوجيات الإنترنت والرابطة الروسية للاتصالات الإلكترونية، ومعهد تطوير الإنترنت.

بطبيعة الحال، هناك عدد أكبر بكثير من الجمعيات في روسيا، ولكنني اخترت أكبر وأهم الجمعيات على شبكة الإنترنت في روسيا. الشريحة التالية، من فضلك.

أود أن أقدم لكم مقدمة عن حالة حرية الإنترنت في روسيا. تحاول السلطات الروسية السيطرة على الجزء الروسي من الإنترنت قدر الإمكان، وهناك بعض الحالات تبين كيفية ارتباط الإنترنت بالحكومة في روسيا و[كيفية] تنظيمها هناك.

هناك هيئة تنفيذية روسية تدعى "روسكومندزور"، تقوم بمراقبة قطاع الإنترنت الروسي وحجب العديد من المواقع التي تعتبر انتهاكا للقانون الروسي وفقا للسلطات الروسية. وقد تم حجب الكثير من المعلومات في روسيا بسبب هذه الهيئة التنفيذية.

ومرة أخرى، من الممكن معاقبة المواطنين الروس بسبب إدلائهم بتصريحات مهينة للسلطات على شبكة الإنترنت. كانت هناك مؤخرا احتجاجات ومظاهرات في روسيا، وغالبا ما تم اكتشاف عمليات إغلاق شبكة الهاتف المحمول، [مع] مشاركة الحكومة.

هناك محاولات لجعل الجزء الروسي من الإنترنت معزولا عن بقية العالم، أو ما يسمى بالإنترنت السيادي، أو شبكة الرونيت RUnet كما نسميها في روسيا. والشركات الدولية العاملة في صناعة تكنولوجيا المعلومات ملزمة بتخزين بياناتها عن المستخدمين الروس على أراضي روسيا حتى تتمكن السلطات الروسية من الوصول إلى بيانات المستخدمين الروس. الشريحة التالية، من فضلك.

حسنا، أول جمعية أريد الحديث عنها هي جمعية حماية حقوق النسخ على الإنترنت، أو AZAPI باللغة الروسية. إنها شراكة غير ربحية تهدف إلى مكافحة الوضع غير القانوني للكتب والمنتجات الصوتية على الإنترنت. إذن فهي مرتبطة غالبا بمشاكل حقوق الطبع والنشر. ويشارك موقع AZAPI في مناقشة مشاريع القوانين المتعلقة بحماية حقوق الطبع والنشر في القطاع الروسي من الإنترنت، ومن بين زبائنه كبار ناشري الكتب الروس الذين يسعون إلى الدفاع عن حقوق النشر الخاصة بهم. ومن المؤسف أن هذه الرابطة لا توفر وسائل مرضية لتلبية هذا الطلب. الشريحة التالية، من فضلك.

كيف تفاعل AZAPI مع الحكومة الروسية؟ في عام 2015، قدم AZAPI استئنافا إلى محكمة مدينة موسكو بطلب لمنع شركة RuTracker التي تقوم بتخزين بيانات حقوق النشر لعملاء شركة AZAPI. إذن لم يسعوا فقط إلى إرضائهم، بل طلبوا حجب الموقع بأكمله، أي متتبع التورنت بأكمله، وهذا ليس أمرا جيدا بالنسبة للإنترنت للأسف.

وفي عام 2016، قدم AZAPI استئنافا إلى محكمة مدينة موسكو بطلب لإلزام محرك البحث Yandex - الذي يعد ثاني أكثر محركات البحث شعبية في روسيا بعد غوغل- بإزالة الروابط إلى الكتب المتعلقة بـ RuTracker من نتائج البحث، والتي كانت موجودة هناك.

وفي عام 2019، قدم AZAPI التماسا إلى محكمة مدينة موسكو بشأن سلسلة من الدعاوى القضائية ضد Archive.org، الذي كان يخزن نسخا رقمية من الكتب السمعية للكاتبين ديمتري غلوكوفسكي وداريا دونتسوفا في الذاكرة المؤقتة، وهذان الكاتبان أيضا من زبائن AZAPI.

وفي عام 2020، ناشد AZAPI المفوضية الأوروبية أن تقوم بمساءلة غوغل بسبب رفضه إزالة تطبيقات من غوغل بلاي تسمح بـ "انتهاكات كبيرة لحقوق النشر والتوزيع" للكتب الإلكترونية. هذه المواقع هي Ok.ru وMail.ru وTelegram وYouTube وWattPad. الشريحة التالية، من فضلك.

الرابطة التالية هي اتحاد وسائل الإعلام والاتصالات، أو MKS باللغة الروسية. وقد تم تشكيلها عام 2014 من قبل أكبر اللاعبين في ميدان صناعات الإعلام والاتصالات. إنها شراكة غير ربحية لشركات الإعلام الروسية وشركات الاتصالات التي تعمل كوسيط بين شركات الاتصالات وسوق الإعلام. الشريحة التالية، من فضلك.

وقد اقترحت نقابة الإعلام والاتصالات على الحكومة الروسية مسودات لعدة قوانين في سنوات مختلفة، وكان معظمها تحت إشراف بافيل ستيبانوف الذى كان رئيسا لـ MKS من 2016 إلى 2018. وقد اقترحت MKS مثل هذه [غير مسموع] مثل منع المرايا لمواقع القراصنة خارج نطاق القضاء، ومنع التورنت على مستوى بروتوكول UDP، وتقييد تشغيل وظائف VPN، وتنظيم تطبيقات المراسلة، وتنظيم عمليات السينما على الإنترنت. الشريحة التالية، من فضلك.

وهناك رابطة أخرى، وهي المركز العام الإقليمي لتكنولوجيات الإنترنت، أو ROCIT باللغة الروسية. وقد تأسست في عام 1996. ويضم أعضاء مجلس ROCIT ممثلين عن الوكالات الحكومية والشركات التجارية. وهي تتلقى تمويلا من صندوق المنح الرئاسية الروسي. وبالتالي فهي ممولة بشكل غير مباشر من الحكومة، على الرغم من أنها جمعية غير حكومية. وتهدف إلى خلق بيئة إنترنت ودية وتعميم تكنولوجيات الإنترنت. وقد تم وضعها كمنصة للتفاعل بين المستخدمين والشركات والدولة، وكذا لحل القضايا المتعلقة بصناعة تكنولوجيا المعلومات. الشريحة التالية، من فضلك.

وترتبط ROCIT برد فعل السلطات الروسية على الاحتجاجات. في عام 2021، شهدت روسيا احتجاجات واسعة النطاق ضد الحكومة، وكانت الحكومة تقمع هذه الاحتجاجات بشدة ماديا ورقميا. وقد وصفت ROCIT توزيع مثل ذلك المحتوى عبر الشبكات الاجتماعية بأنه ترويج لأعمال متطرفة، كهذا التصريح مثلا:

"يلاحظ خبراء ROCIT زيادة حادة في مواد المحتوى الموجهة ضد السلامة العامة على الإنترنت." ففي هذا التصريح، كانوا ينتقدون المحتوى الذي يخبر الناس ببساطة عن الأنشطة الاحتجاجية. ويطلقون على المواد المتعلقة بأعمال الاحتجاج مصطلحات مثل "التطرف" بل حتى "الإرهاب".

وناشدت ROCIT الشبكات الاجتماعية وقف توزيع مثل هذه المحتويات المتعلقة بالنشاط الاحتجاجي. وتوافق هذا الموقف مع موقف الحكومة. الشريحة التالية، من فضلك.

وهناك رابطة أخرى هي الرابطة الروسية للاتصالات الإلكترونية، أو RAEC باللغة الروسية. وقد تأسست في عام 2006. وهي مدرجة في قائمة المستفيدين من دعم الدولة في مجال الإعلام الإلكتروني، وتمولها الحكومة هي الأخرى. ومن بين المشاركين الرئيسيين في هذه المجموعة مجموعة Mail.ru وKaspersky Lab وVKontate وRostelecom، وهي أكبر شركات تقنية المعلومات في روسيا.

وهناك أيضا شركات تملكها الدولة، مثل وكالة "روسيا اليوم" ووكالة أنباء TASS. وهي عبارة عن جمعية غير ربحية لممثلي سوق الاتصالات الإلكترونية الروسي، تهدف إلى تعزيز آراء قادة الصناعة والتفاعل مع الوكالات الحكومية. الشريحة التالية، من فضلك.

ويمكن التعبير عن الموقف من تنظيم RAEC على الإنترنت من خلال جائزة رونيت. وهي جائزة نظمتها شركة ""RAEC، وهي تمثل الإنجازات التي تحققت في صناعة القطاع الروسي من الإنترنت، ومنذ عام 2011، امتلأت جائزة "رونيت" بترشيحات تتعلق بتنظيم القطاع الروسي من الإنترنت، مثل الرونت الآمن، والإنترنت بدون تطرف، والمشاريع الاجتماعية المهمة، وخاصة حماية الأطفال، وتعزيز الحصانة الرقمية للرونت.

وفي أغلب الحالات، كانت الشركات المملوكة للدولة هي الرابحة الوحيدة في هذه الفئات، وكانت تهدف إلى فرض الرقابة على القسم الروسي من الإنترنت. وفي الفئات المتصلة بمحتوى المعلومات في الإنترنت، تعطى الأفضلية في معظم الحالات لموارد الدولة. الشريحة التالية، من فضلك.

آخر جمعية أود الحديث عنها هي معهد تطوير الإنترنت، أو IRI بالروسية. تأسست عام 2015 بدعم من الإدارة الرئاسية. ومع ذلك فلا زالت تهدف أن تكون جمعية غير حكومية. وهي منظمة مستقلة غير هادفة للربح نشاطها الرئيسي هو إنتاج محتويات ذات أهمية اجتماعية على الإنترنت والعمل على مشاريع قوانين خاصة بكل صناعة. وهي تعمل وسيطا بين أعضاء الصناعة الرقمية والأجهزة الحكومية، وتعلن مسابقات لإنتاج أشرطة الفيديو حول موضوع الدعاية الاجتماعية والمحتوى الوطني. وهي في الأساس مثل سوق للمحتوى على الإنترنت، في الجزء الروسي من الإنترنت، من حيث الحركية الاجتماعية. الشريحة التالية، من فضلك.

كيف شاركت IRI في تنظيم الصناعة الرقمية عبر الأعوام؟ لقد اقترحت قائمة بالبرامج الروسية للتثبيت المسبق على أجهزة الكمبيوتر المحمولة والهواتف الذكية. واقترحت برنامجا للتأمين على الكهرباء. واقترحت وضع مذكرة بشأن الإعلان الاجتماعي. واقترحت إنشاء بيئة رقمية آمنة للجيل الجديد. واقترحت وضع برامج تعليمية حول التكنولوجيات الرقمية. واقترحت أيضا تنظيم أجهزة تجهيل الهوية في روسيا، بما في ذلك شبكة VPN. الشريحة التالية، من فضلك.

كيف ترتبط هذه الجمعيات؟ بالنسبة لهذه الرابطات، لا توجد هيئة تعاونية تعنى بقضايا إدارة الإنترنت. غير أن أعضاء هذه الجمعيات موجودون في الجمعيات الأخرى أيضا. في الأساس، أعضاء MKS حاضرون في ROCIT أيضا، والحكومة الروسية عضو أيضا، أو لها بعض التأثير في بعض القدرات في كل جمعية مدرجة.

ما علاقة هذا بـ ICANN؟ تعد شركتا ROCIT وIRI من مؤسسي مركز التنسيق للمجالات عالية المستوى في روسيا، والذي يحافظ على وظائف المجالات الروسية عالية المستوى مثل .ru و.rf. إذن في الأساس، من خلال هذه الجمعيات غير الحكومية، وعلى الرغم من أنها مرتبطة بالحكومة، فإنه يمكن للحكومة التأثير على سياسة المستويات العليا وعمل كل جمعية. الشريحة التالية، من فضلك.

وخلاصة القول؛ أولا، إن العديد من جمعيات الإنترنت، وإن كانت مسجلة كجمعيات غير ربحية وغير حكومية، مرتبطة بهياكل الدولة في روسيا، وتتلقى تمويلا من ميزانية الدولة، وتعمل بناء على أوامر من الدولة، كما أن ممثلي الحكومة موجودون في الجمعيات ويؤثر ذلك على التعبير عن آراء هذه الجمعيات.

ويتم التوصل إلى ردود فعل الرابطات عن طريق الأغلبية، ومن بين المشاركين في ذلك السلطات الروسية. وهي إيجابية في معظم الحالات، وتدعم تنظيم الإنترنت. وفي حالات نادرة جدا، تنتقد ردود الفعل هذه بعض القضايا المعينة بشكل معتدل.

والنقطة الثالثة هي أن الجمعيات نفسها تستفيد من التنظيم لأنها تعمل على تنفيذ أوامر الدولة وتنفيذ القوانين المعتمدة. وهم يضغطون لتحقيق مصالحهم عند مناقشة أو تقديم مشاريع القوانين، ويحاولون احتكار مجالات تجارية معينة من خلال تركيز جوانب العمل حول جمعية واحدة وإضعاف المنافسين.

وفي الختام، فإن الحكومة الروسية تحاول السيطرة على أكبر قدر ممكن من الإنترنت، وإن الجمعيات هي إحدى الطرق التي تمكّن الحكومة، والسلطات الروسية، من تحقيق أهدافها، وإن كانت الجمعيات ليست حكومية، اسميا على الأقل، فإن الحكومة تسيطر عليها نوعا ما. شكرًا لكم على اهتمامكم.

ديبورا إسكاليرا: رائع. شكرا لك يا دانيل. هل هناك أية أسئلة موجهة إلى دانيل؟ يمكنكم رفع أيديكم أو كتابة أسئلتكم في الدردشة.

دانيل غولوبف: لدينا سؤال من بابلو.

ديبورا إسكاليرا: حسنا يا بابلو، يمكنك إلغاء كاتم الصوت وطرح السؤال.

بابلو بورديك: نعم. مرحبًا بكم جميعًا. بادئ ذي بدء، أشكرك كثيرا يا دانيل، على هذا العرض الرائع والتثقيفي جدا. أنا مهتم جدا بهذا الموضوع لأني أبحث جزئيا في القضية الروسية، وكنت أتساءل ما إذا كان يمكنك أيضا تقديم المزيد من التفاصيل حول ما إذا كانت هناك جمعيات للإنترنت غير مرتبطة مباشرة بالحكومة أو مرتبطة بشكل غير مباشر بالحكومة، وأعني جمعيات الإنترنت المستقلة.

دانيل غولوبف: شكراً لك على سؤالك الرائع يا بابلو. لسوء الحظ، كان الوقت محدودا، وقد سُمح لي تقديم العرض في عشر دقائق فقط. نعم، هنالك جمعيات مستقلة تماما، لكن لا يسمح لها بالتسجيل قانونيا في معظم الحالات، لأنك، لكي تسجل بالكامل، يجب أن تتقيد بالقوانين والتشريعات الروسية. وعليك أن تجد بعض حلولا وسطا، وفي معظم الحالات، لا ينجح الأمر.

هناك جمعية تدعى روسكومسفوبودا Roskomsvoboda. وهي تعمل في ميدان حرية الإنترنت، وهي فرع معتمد من ICANN في روسيا من بعض النواحي. وهي تسعى في سبيل حرية الإنترنت وتحاول أن تجعل حرية الإنترنت في روسيا متوفرة بأكبر قدر ممكن. ولكن للأسف، في معظم الحالات، لا يسمح لهم بالعمل على المستوى الرسمي.

ديبورا إسكاليرا: حسنًا. شكرا لك. ولدينا سؤال من ريكاردو ناني. تفضل يا ريكاردو.

ريكاردو ناني: شكرا لك يا ديبورا، وشكرا لك يا دانيل، على عرضك المثير للاهتمام، وهو عرض ذو قدر عال من الوضوح، لأنه أحيانا عندما نسمع معلومات عن Runet، فإننا نميل إلى التعامل معها وكأنها عبارة شعبية، ومن الصعب جدا قياس ما تمثله في الواقع.

كان هناك مؤخرا بعض الكلام عن إمكانية قيام روسيا بإنشاء DNS روسي. هل هذا مجرد خطاب عام، أم أن هناك شيئا أكثر واقعية يمكن أن يحدث؟ هل لديك نظرة حول ذلك؟ شكرا لك.

دانيل غولوبف: شكرًا لك على سؤالك يا ريكاردو. نعم، هناك محاولات لإنشاء ما يسمى بالإنترنت السيادي، Runet، بـ DNS روسي. وكان هناك كلام حول هذا المشروع منذ 2010 تقريبا، على ما أظن. وقد حاول أخصائيو تكنولوجيا المعلومات والحكومة الروسية تأسيس ما يسمى بموقف الإنترنت المستقل في روسيا.

غير أن مؤهلاتهم غير كافية. في عام 2017، حاولت روسيا حجب Telegram. ولم ينجح هذا المقترح. فإن Telegram لايزال يعمل في روسيا. وقد حاولوا حجب Twitter هذا العام. ولم ينجح ذلك أيضا، والآن هناك محادثات حول حجب موقع YouTube، وهو أمر... لا أعتقد

أن ذلك سيكون ممكنا، لأن مؤهلات أخصائيي تكنولوجيا المعلومات الذين يعملون في الحكومة ليست مرضية ببساطة.

نعم، هناك كلام حول جعلها أكثر سيادية، لكنني لا أعتقد، نظرا لحالة للإنترنت المنتشرة في روسيا حاليا، أنه من الممكن جعل الوضع مثل الصين. فالمجتمع العالمي ببساطة مندمج جدا مع الجزء الروسي من الإنترنت، ولا أعتقد أن هذا سيكون ممكنا على نطاق واسع.

ديبورا إسكاليرا: شكرًا جزيلاً على هذا العرض التوضيحي الرائع يا دانيل. حسنا، سننتقل إلى مقدم العرض التالي، فيرونيكا سليومينسكا.

فيرونيكا سليومينسكا: مرحباً.

ديبورا إسكاليرا: وللتذكير، لديك عشر دقائق، وإذا تجاوزتِ الوقت المحدد فسأنبهك لذلك. وأرجو مرة أخرى أن تتحدثي ببطء وبوضوح. شكرا لك.

فيرونيكا سليومينسكا: حسنًا. شكرا لك. مرحبًا بكم جميعًا. شكرًا لك يا دانيل على العرض الشيق. أنا فيرونيكا، وأدرُس الإدارة العامة الدولية، وأريد اليوم أن أحدثكم عن أمن الفضاء الحاسوبي والتحديات ذات الصلة لصناع السياسات في هذا المجال، والحاجة إلى تحسين الوعي بهذه المسألة. الشريحة التالية، من فضلك.

شكرا لك. إن أمن الفضاء الحاسوبي موضوع يستمر في النمو من حيث النطاق والتردد في جميع أنحاء العالم. إن الأنواع الجديدة من التهديدات الإلكترونية تظهر باستمرار، ويمكن أن تكون للهجمات الإلكترونية عواقب وخيمة جدا على المنظمات وجميع الناس، مما يعني أن المسألة تحتاج حقا إلى عناية مركزة مع استخدام نهج من أعلى إلى أسفل.

إن أمن الفضاء الحاسوبي مسألة متعددة الأوجه وهي بحاجة إلى تعاون من كلا الطرفين؛ أي من يتعامل مع جوانبها التقنية وكذلك من يتقلد مناصب الحكم، وهذه هي الزاوية التي سأناقش منها هذا الموضوع اليوم.

في عالم "إنترنت الأشياء"، لكثير من الأجهزة الآن عنوان بروتوكول إنترنت (IP) خاص بها للاتصال بالإنترنت، ويعني ذلك أن المجتمع يعتمد بشكل أكبر على الفضاء الإلكتروني. ولكن على الرغم من أن إدارة الفضاء الإلكتروني أمر بالغ الأهمية، إلا أنه يبدو أن الحكومات لا تفعل ما يكفي لضمان سلامتها والحفاظ على أمن الإنترنت، ولا يسترعي ذلك منها القدر الكافي من الاهتمام. الشريحة التالية، من فضلك.

وذلك لأن صناعة السياسات في مجال أمن الفضاء الحاسوبي تواجه العديد من المفارقات، أولها أن الحكومات تريد ضمان أمن الفضاء الحاسوبي، ولكنها تريد من ناحية أخرى الحصول على بيانات المواطنين لأغراض المراقبة. فمن ناحية أولى، تريد الحكومات من المواطنين حماية أنفسهم، ولكن من ناحية أخرى، لا يريدونهم أن يستخدموا التشفير وغيره من تدابير الأمن الإلكتروني، لأنه يمكن للمجرمين والإرهابيين استخدام ذلك أيضا.

وثمة مفارقة أخرى تتمثل في أن أمن الفضاء الحاسوبي ظاهرة عالمية ولا يمكن التعامل معها داخل الحدود الوطنية، ويحتاج ذلك إلى التعاون بين الدول. لكن بعض الحكومات لا تثق ببعضها البعض وهي غير مستعدة للتعاون. بل وربما يخترقون بعضهم البعض. وهذا يجعل الأمر معقدا.

وثمة مفارقة مهمة أخرى تتمثل في عدم وجود مبلغ مناسب معين من الإنفاق الحكومي على أمن الفضاء الحاسوبي، لأن الإنفاق القليل جدا لا يضمن الحماية الكافية، ولكن الإنفاق الزائد يمكن أن يرسل رسالة مفادها أن هناك شيئا مهما جدا هناك، وأن هناك مؤامرة خطيرة تحاك، مما من شأنه أن يخلق الخوف. ولذلك فإن ضمان التوازن أمر بالغ الأهمية. الشريحة التالية، من فضلك.

وعلى هذا فقد تم تحديد أربعة أسباب رئيسية تفسر لماذا يشكّل صُنع السياسات في مجال أمن الفضاء الحاسوبي تحديا كبيرا للغاية، أولها محدودية الرؤية. وبما أن تأثير انتهاكات الأمن الحاسوبي لا يظهر ماديا في الغالب، وأنه ليس من السهل شرح الموضوع للجمهور، فإن الجمهور لا يشعر بخطورة المشكلة وتأثيرها. لذلك من الصعب وضع سياسات لتنظيم شيء جديد يتعلق بشيء غير مرئي.

المشكلة الثانية هي التعقيد التكنولوجي الاجتماعي لأمن الفضاء الحاسوبي، لأنه على الرغم من أهمية البنية الأساسية لتكنولوجيا المعلومات وسياساتها في ضمان أمن الفضاء الحاسوبي، فإن الإنسان المسؤول عن الحفاظ على الأنظمة وتنفيذ السياسات يقوم بالدور الرئيسي في ذلك، لكن الكثير من الأفراد والمنظمات يفتقرون إلى الوعي أو ليست لديهم حتى الموارد اللازمة لاتخاذ الإجراءات.

المشكلة الثالثة هي الطبيعة المتنازع عليها لأمن الفضاء الحاسوبي. معظم المهاجمين مجهولو الهوية، فلا نعرف حقا من هو العدو. والتحدي الرابع هو التأثير الغامض. إذن من الصعب الحكم مسبقا على مخاطر أمن الفضاء الحاسوبي، ومن الأصعب أيضا قياس تأثير السياسات الجديدة لأمن الفضاء الحاسوبي، مما يجعل من الصعب الدعوة للاستثمار. الشريحة التالية، من فضلك.

وكما نرى، هناك الكثير من الغموض وعدم الوعي حول أمن الفضاء الحاسوبي، مما يؤدي إلى تحديات يواجهها صناع السياسات. إذن، ما الذي يمكن فعله لمعالجة ذلك؟ الشريحة التالية، من فضلك.

لقد توصل الباحثون إلى مفهوم صياغة الرسائل، وهو عملية طرح مشكلة معقدة بطريقة بسيطة ومقنعة. ونظرا لأن صناع السياسات والمختصين كثيرا ما يُنتقدون لأنهم لا يستطيعون تقديم رسالتهم وشرحها للجمهور، ولأن أمن الفضاء الحاسوبي ظاهرة معقدة جدا، وطويلة جدا، وصعبة التفسير، فإنه يتعين طرحها في رسالة بسيطة تأسر جوهر الأمن الحاسوبي وتوضح أهميته للناس. الشريحة التالية، من فضلك.

يقترح الباحثون استراتيجية لاستخدام آلية تكوين رسالة أمن الفضاء الحاسوبي من أجل رفع وعي الناس بشأن أمن الفضاء الحاسوبي، وتتكون من ست خطوات أو قواعد، أولها ألا تؤدي إلى تفاقم أمن الفضاء الحاسوبي، وعدم المبالغة في التعريف بمخاطره، ووضعها في منظور واقعي، لأن المبالغة لن تزيد المشكلة إلا سوءا.

والقاعدة الثانية هي أن تبين من هم الأشرار، ومن هم الأطراف الذين نحاربهم، ومن قد يكون من الأعداء، ومن يمكن أن نتوقع تهديدا منه.

والقاعدة الثالثة هي تسليط الضوء على الأبطال، عن طريق تحديد من يقوم بحماية أمن الفضاء الحاسوبي في بلد ما مثلا، وما هي قدراتهم، وعرض نجاحاتهم.

والقاعدة الرابعة هي إظهار أهمية أمن الفضاء الحاسوبي للمجتمع، وربط الحاجة إلى تحسين أمن الفضاء الحاسوبي مع النمو الاقتصادي أو الرخاء الوطني.

والقاعدة الخامسة هي إضفاء طابع شخصي على أمن الفضاء الحاسوبي وربطه بالحياة اليومية للناس، وذلك لتوضيح كيف يمكن أن يؤثر ذلك على حياتهم اليومية، بأية طرائق.

والقاعدة السادسة والأخيرة، هي ربط القضيتين الأخريين المتصلتين بأمن الفضاء الحاسوبي، مثل السياسة.

والشريحة التالية هي شكر لكم جميعا. هذا كل ما لدي. شكرا لك.

ديبورا إسكاليرا: شكرا لك، فيرونيكا. أحسنت في العرض التقديمي. هل لدينا أي أسئلة لفيرونيكا؟ هل هناك أي سؤال في الدردشة أو أي شخص يريد أن يرفع يده؟ حسنًا، شكرًا جزيلاً. إذا كانت لديكم أي أسئلة متابعة لفيرونيكا، فيمكنكم مراسلتنا عبر البريد الإلكتروني أو إرسالها مباشرة. يمكننا أن نعطيكم بريدها الإلكتروني، أو يمكنكم مراسلتنا على العنوان engagement@icann.org.

حسنا، الشخص التالي، الذي لم يتمكن من تقديم العرض مباشرة اليوم، هو أنترونوس مولوجيتا، فهو لم يتمكن من الحضور اليوم، لكنه قدم عرض فيديو. لم أفعل هذا من قبل، هذا جديد علي، لذلك سأشارككم شاشتي وأرى كيف تسير الأمور، ونأمل أن تسير الأمور على ما يرام. هل يمكنكم رؤية هذا؟

أنترونوس مولوجيتا: مرحبًا بكم جميعًا. أنا أنترونوس [غير مسموع]. أريد فقط أن أخبركم بأنه إذا كان لديكم أي سؤال أو أي اقتراح أو تعليق، فأرجو منكم استخدام عنوان البريد الإلكتروني الخاص بي للاتصال بي [غير المسموع]، لذا إذا كانت لديكم أية أسئلة حول هذا العرض التقديمي، فأنتم موضع ترحيب.

إذن، عندما يتعلق الأمر بموضوع سيكون [غير مسموع] كيف يمكننا مساعدة ICANN بالذكاء الاصطناعي؟ [غير مسموع] لجعله أكثر تحديدا والقول إنه يطبق ذكاء اصطناعيا على أمن نظام أسماء النطاقات. لذلك [حاولت أن أرى لاحقا] عندما تم ابتكار نظام أسماء النطاقات هذا. تم ابتكاره عام 1980 دون أي حماية لضمان البيانات أو [غير مسموع].

وحينئذ لم تكن الإنترنت على نفس القدر من الاتساع كما هي عليه اليوم، أو كبيرة كما هي اليوم، لذلك لم يهتموا بمسألة الأمن أو لم يهتموا كثيرا بالحماية، وقاموا بحفظها دون حماية. لكن في هذه الأيام، ومع اتساع شبكة الإنترنت وكبرها، [غير مسموع] وأيضا، يسمح ذلك للمهاجم بتحويل المستخدمين من الوجهة المقصودة إلى الوجهة التي يختارها المهاجم.

ولما قامت فرقة عمل هندسة الإنترنت بالنظر في هذه المشكلة لأول مرة، حاولوا تقديم حل، ولذلك قاموا باختراع DNSSEC، وهو امتداد أمان نظام أسماء النطاقات، وهدفه تقوية مصادقة أصل البيانات، وضمان سلامة البيانات في نظام أسماء النطاقات باستخدام التوقيع الرقمي بناء على مفتاح التشفير العام.

دعوني أقل 'مصادقة أصل البيانات' [غير مسموع]، سلامة البيانات، فعندما أقول 'مصادقة أصل البيانات'، فهذا يعني - عندما أقول أن نظام اسم المجال في المقام الأول لا يوفر مصادقة أصل البيانات، فهذا يعني أن نظام اسم المجال لا يوفر تأكيدا بأن البيانات المرتبطة [غير مسموع]. وعندما نقول في المقام الأول أنها ليست [غير مسموع] لسلامة البيانات، فهذا يعني أنها لا توفر [غير مسموع] إذا كانت البيانات في استجابة نظام أسماء النطاقات قد تم تعديلها أو تغييرها. في المقام الأول، لم يكن نظام أسماء المجالات هذا مؤمنا كما نرى. ولكن بعد تنفيذ DNSSEC، يوفر امتداد نظام اسم المجال هذا سلامة بيانات مصادقة أصل البيانات [غير المسموعة]، بحيث تصبح أكثر أمانا.

ولكن عندما نرى كيف يعمل ملحق نظام اسم المجال هذا، فإننا نجد أنه ليس تلقائيا. من المفترض أن يتم تمكينه من قبل المشغل، وأيضا من قبل مالك نظام اسم المجال. وهذا يعني أن على كل مالك اسم مجال أن يعرف ملحق نظام اسم المجال هذا لجعل الإنترنت أكثر أمانا.

هناك أصحاب أسماء مجالات مختلفون، وهناك رجال أعمال على سبيل المثال، لاستخدام مثال لشرح هذا، موقع [غير مسموع] له اسم مجال، موقع أعمال يستخدمه لبيع منتجاته. هذا الرجل، كما قلت، هو رجل أعمال مثلا، وليس لديه هذا القدر من المعرفة حول الجانب التقني، وهذا يعني أنه لا يستطيع تمكين DNSSEC [غير مسموع] لأغراض أمنية. وهذا يعني أنه يمكن للمخترقين استخدام نفس الصفحة التي [قام بإنشائها وتعامل بها مع زبائنه].

وفكرتي هي حماية هؤلاء الناس، لماذا لا نجعل هذا النظام آليا؟ أعتقد أنه علينا أن ندرج الذكاء الاصطناعي ونجعل هذا النظام آليا.

وعندما يتعلق الأمر بهذا الجزء، أعتقد أن هناك أشخاصا خارج [الجزء] التقني، فعندما تحاول شرح ماهية الذكاء الاصطناعي وما هو التعلم الآلي، فإن الذكاء الاصطناعي هو مثل فرع واسع من علوم الكمبيوتر يهتم ببناء آلات أو أنظمة يمكنها القيام بمهام تتطلب قدرة تفكير بشرية أو قدرة منطق بشرية.

لذا من هذا [غير مسموع]، أريد فقط أن أقدم جزءا محددا حول هذا المجال، ولذلك اخترت الآلة التي تتعلم الذكاء الاصطناعي. فعندما ترى ما يفعله تعليم الآلة وكيف يعمل، أي هذا التعلم الآلي، وهذا الجزء من الذكاء الاصطناعي، فهو يعمل عن طريق تدريب الآلة [لأداء هذا التعلم الآلي لجزء معين] الذي هو التعلم تحت المراقبة. التعلم تحت المراقبة هو جزء من تعلم الآلة الذي يستخدم لتسمية البيانات أو تعريف البيانات، أي تدريب الآلة عبر البيانات المعرفة.

أعلم أن هذا موضوع تقني للغاية وموضوع معقد جدا، ولكن دعوني أحاول شرح ذلك في بضع كلمات، أي كيف يمكننا تطبيق هذا التعلم الآلي أو الذكاء الاصطناعي؟ أعتقد أنه يمكننا تدريب جهاز على [الاستشعار عند] تسجيل نظام اسم مجال جديد، ثم [تمكين] DNSSEC تلقائيا لتحسين أمان نظام اسم المجال.

لذا فإن فكرتي هي أن أجعل الآلة تستشعر تسجيل نظام اسم مجال جديد وتمكين DNSSEC تلقائيا بدون الحاجة إلى تمكينه من قبل مالك اسم المجال والمشغل. أعتقد أن هذا سيحسن أمن الإنترنت.

إذن بحثي هو — لم أتوصل إلى نتيجة، لكني مازلت أعمل عليها، لذا بحثي هو ما إذا كنا نستطيع جعل هذا ممكنا آليا باستخدام هذا التعلم الآلي أم لا. لذلك أريد أن أرى ما يفعله الآخرون في هذه القضية، في مجال أمن الإنترنت لجعل الإنترنت أكثر أمانا. يعمل خبراء مختلفون على كيفية تطبيق تعلم الآلة للكشف عن [غير مسموع].

أعلم أن هذا معقد بعض الشيء وأن هذه الخوارزمية أكثر تقنية [غير مسموع] مثل الخوارزمية [غير مسموع] والتي تستخدم للتسجيل والتصنيف [غير مسموع] وهم يستخدمون أيضا معلومات إضافية، كما يستخدمون بايثون كقاعدة للتشفير.

أعلم أنه لا يمكننا تغطية هذا الموضوع الواسع في عدة دقائق، ولكن هذا كل ما لدي اليوم. إذا كان لديكم أي سؤال، كما ذكرت في البداية، فأنا أرحب باتصالكم بي عبر بريدي الإلكتروني. شكرا جزيلا لكم على [غير مسموع] وأيضا، لدي [غير مسموع] خاص، وأنا أقوم بإعداد عرضي. شكرًا لكم جميعا، وأتمنى لكم يوما رائعا.

ديبورا إسكاليرا: حسنًا. أعتقد أن ذلك كان صعبا بعض الشيء على المترجمين الشفويين، ولذلك لن يكون هذا جزءا من النص المسجل. وأعتقد أن هناك بعض الأسئلة الموجهة لفيرونيكا التي لم أنتبه لها. إذن، هل لأحدكم سؤال موجه لفيرونيكا لم أنتبه له؟ هل يمكنك رفع يدك؟ هل من أحد؟ حسنا، إذا لم يكن هناك شيء آخر، فسوف أواصل.

مقدم العرض التالي هو فيرونيكا بيكولو. فيرونيكا هل أنتِ متصلة بالشبكة؟

فيرونيكا بيكولو: نعم، أنا هنا.

ديبورا إسكاليرا: حسنًا يا فيرونيكا. أذكرك مرة أخرى بأن لديك عشر دقائق، وأرجو أن تحدثي ببطء وبوضوح. تفضلي يا فيرونيكا. شكرا لك.

فيرونيكا بيكولو: شكرا لك. مرحبًا بالجميع. سأتحدث لكم عن السوابق القضائية التي صدرت من قبل محكمتين إيطاليتين في 2019 و2020 تتعلق بحماية حقوق الملكية الفكرية، وبالتحديد حول إمكانية إعاقة تلك القرارات لسلامة الإنترنت والممتلكات الحرجة لما يسمى بطريقة الإنترنت للتواصل. الشريحة التالية، من فضلك.

هذا هو جدول الأعمال. سأعطيكم مقدمة بسيطة، وسأتحدث عن طريقة التواصل عبر الإنترنت، وأشرح لكم ما هي التلميحات الديناميكية وتأثيرها على خاصية الإنترنت الحساسة، وعلى طريقة التواصل عبر الإنترنت، وبعدها سأقدم ندائي لكم. الشريحة التالية، من فضلك.

إذن أقدم لكم مقدمة صغيرة. في عام 2019، سعت شركة إعلامية إيطالية إلى الحصول على تخفيف إلزامي ضد Cloudflare.Cloudflare موفر لخدمات شبكة تسليم المحتوى، والتخفيف من قيود DDoS، وأمان الإنترنت، وخدمات خادم أسماء المجالات الموزعة.

ادعت الشركة الإيطالية أن عملاء Cloudflare كانوا ينتجون بشكل غير قانوني العديد من عروضها التلفزيونية، ووجه هذا طلب إلى Cloudflare لإزالة أو تعطيل الوصول إلى تلك المواقع.

وفي مثل هذه الحالات، تنص اللائحة الإيطالية على أنه لا يجوز لمقدم خدمات الإنترنت الوسيط أن ينهي أو يمنع التعدي إلا عندما تطلب منه ذلك محكمةٌ وطنية أو سلطة إدارية.

في عام 2020، كانت لدينا شكوى مماثلة صادرة عن الدوري الوطني لكرة القدم وSky Italy بسبب العرض الحي غير القانوني لمباريات كرة القدم. في هذه الحالة، كان العلاج صعبا لأن شركة CloudFlare أمرت بتعطيل خدمات شبكة تسليم المحتوى الخاصة بها تجاه بعض عملائها. الشريحة التالية، من فضلك.

إذن، ما هي طريقة الاتصال بالإنترنت؟ طريقة التواصل عبر الإنترنت تنص على أنها مشروع تعده جمعية الإنترنت وينص على أن الإنترنت لا يدين بنجاحه فقط للتكنولوجيا نفسها بل أيضا بالطريقة التي يعمل بها ويتطور بها.

عندما نفكر في الأمر، نجد أنه يمكننا القيام بالعديد من الأنشطة عبر الإنترنت. يمكننا أن ندرس، ونتواصل، ونتشارك، وننظم أعمالا بفضل الإنترنت. ونحن نفعل ذلك لأن الإنترنت تنمو بهذه الطريقة، ونحن بحاجة إلى التعرف على ما يجعل الإنترنت مفيدة للجميع حتى الآن. لذا فقد طور مجتمع الإنترنت خمسة حقوق مهمة والتي هي مبادئ أخلاقية أكثر من كونها خصائص فنية. الشريحة التالية، من فضلك.

حسنا، الخاصية الأولى هي إمكانية الوصول. بعبارة أخرى، أيا كانت الدولة التي تنتمي إليها، ستتمكن دائما من الاتصال بالشبكة العالمية. ما تحتاجه هو جهاز ونقطة وصول وستجد نفسك على الإنترنت. يمكنك التواصل أو العمل مع كل شخص في العالم.

الخاصية الثانية هي الانفتاح وقابلية التشغيل المتبادل. يجب أن نفكر في الإنترنت كمنزل LEGO. يمكن أن يكون لدينا كتلة فوق البنية التحتية، ونحن نعلم أن هذه الكتلة سوف تلائم القاعدة دائما، مما يسمح بابتكار غير دائم وفي أي مكان.

والملكية الثالثة هي اللامركزية. نعلم أن الإنترنت عبارة عن شبكة مكونة من شبكات أخرى. وتختار كل شبكة مستقلة أن تتصل ببعضها البعض وتستفيد كل شبكة منها من الانتماء إلى نفس الشبكة.

الخاصية الرابعة هي معرفات عمومية شائعة. وبعبارة أخرى، هناك لغة مشتركة لفهم عناوين بروتوكول الإنترنت والطريقة التي يتم بها تسليم حزم البيانات من النقطة ألف إلى النقطة باء.

الخاصية الخامسة لا تحتاج للتعريف، وهي الحيادية. الشريحة التالية، من فضلك.

في بلدي، هناك ممارسة واسعة النطاق لمكافحة القرصنة على الإنترنت، والتي تتألف من مطالبة المحكمة ليس فقط بإغلاق مواقع القرصنة النشطة حاليا ولكن أيضا المواقع المستقبلية التي قد يكون لها نفس المستوى الثاني. ونسمي هذه المواقع الأسماء المستعارة.

وبعبارة أخرى، إذا كان هناك مجال مستوى أعلى يتبع نفس مجال المستوى الثاني، سواء كان موجودا أو سيتم تنشيطه، فإنه سيكون عرضة للإيقاف. هذا غريب أيضا لأن الأوامر الديناميكية ذاتية الإنفاذ. عند نسخ المحتوى المخالف في موقع ويب بديل بنفس اسم مجال المستوى الثاني،

لن يحتاج مالك حقوق الملكية الفكرية إلى أي أمر قضائي آخر. سيذهب مباشرة إلى خدمة وسيط الإنترنت وسيطلب منهم أن يغلقوا ذلك.

ويؤثر هذا الأمر القضائي الدينامي على حالات لم يتم فيها انتهاك بعد، وربما حتى على المواقع التي تعرض محتوى قانونيا. وقبل كل شيء، إذا لم يمتثل مشغلو البنية الأساسية للأمر، فيمكن اعتبارهم مسؤولين عن الأضرار. الشريحة التالية، من فضلك.

وفي هذه القضية، أمرت المحكمة شركة Cloudflare بتعطيل خدمة شبكة تقديم المحتوى التابعة لها بطريقة محددة، مما يستهدف عناوين بروتوكول الإنترنت أو أسماء النطاقات المحددة.

لذا، ما أقوم به في هذا الموضوع هو استكشاف أي خاصية من الخصائص الخمس الحرجة التي تتأثر بموجب هذه القضية. وقد قمت أيضا بالتحقيق في الخاصية الثانية والثالثة، لكني أعلم أن هذه الحالة تؤثر بالتأكيد على الخاصية الخامسة، و هي الحيادية، لأن مشغلي البنية التحتية لا يمكن اعتبارهم مسؤولين عن المحتوى الذي يرسله زبائنهم عبر الإنترنت، و لا ينبغي أن يطلب منهم التحكم في البيانات و تنفيذ توصيل مستهدف للمحتوى.

ويصدق هذا كثيرا عندما نفكر فيما حدث الأسبوع الماضي مع مزود خدمة شبكة تسليم المحتوى Fastly. كانت الكثير من المواقع في حالة تعتيم لمدة ساعة. الشريحة التالية، من فضلك.

حسنا، ندائي لكم. تستحق هذه القضية المناقشة على كل المستويات، في منتدى سياسات ICANN، وفي مجتمع ICANN، وفي منتدى إدارة الإنترنت، أيا كان المجتمع أو أصحاب المصلحة الذين يتأثرون بمثل هذا القرار أو قانون السوابق القضائية الذي هو واسع الانتشار في بلدي، ولكني أعرف أن هناك ولايات قضائية أخرى تحاول بدورها الاقتداء بقانون السوابق هذا.

إذن، ما سأقوم به هو البدء في ملاحظة ما إذا ما تمت مناقشة بعض القضايا ذات الصلة في GNSO وتحديدا من قبل جمهور مزودي خدمات الإنترنت ودائرة الملكية الفكرية، لفهم ما يقومون به، وما يفكرون به، وما إذا كانوا يعرفون هذه الأمور. وإن لم يكن كذلك، إن كان هناك أي ممثل من مجموعات أصحاب المصلحة تلك، فيرجى منهم الانتباه إلى هذه المسألة.

أعتقد أن وقتي انتهى، ولذلك سأطلب من ديبورا أن تنتقل إلى الشريحة التالية لنختم. شكرًا لكم على الاستماع.

ديبورا إسكاليرا: شكرا يا فيرونيكا. أحسنت. هل لدينا أية أسئلة لفيرونيكا؟ أنا لا أرى أي أيادٍ أو أسئلة في الدردشة. أحسنت يا فيرونيكا. حسنا، أريد أن أتأكد من أنني لن أتخطى أية أسئلة هذه المرة. حسنًا. رائع. عمل رائع. سننتقل إلى شيفام شارما، مقدم العرض التالي. مرحبا شيفام، تفضل. حسنا، لديك عشر دقائق، وأذكرك أن تتحدث ببطء وبوضوح. شكرا لك.

شيفام شارما: سأناقش الأمن السيبراني لأجهزة IoMT. الشريحة التالية، من فضلك. ما هو IoMT؟ مصطلح IoMT يعني إنترنت الأجهزة الطبية. إنها مجموعة فرعية من IoT أي إنترنت الأشياء. وهي مجموعة من أجهزة الرعاية الصحية التي تشمل أجهزة الاستشعار وتطبيقات الرعاية الصحية [غير مسموع] المتصلة بالإنترنت والتي ترسل بيانات المرضى إلى سحابة يمكن الوصول إليها عن بعد من قبل الموظف الصحي أو الطبيب مما يمكنه من تقليل فرص [غير مسموع]. الشريحة التالية، من فضلك.

إذن هذه بعض أجهزة IoMT: أجهزة الرفاهية الشخصية، والساعات الذكية، وشرائط اللياقة البدنية الإلكترونية، وبعض الأجهزة السريرية التي يرتديها المرضى مثل أجهزة مراقبة السكري أو أجهزة قياس ضغط الدم. هذه إذن بعض الأجهزة السريرية الملبوسة.

ثم هناك الأقراص الرقمية. هذه أقراص تحتوي على أجهزة استشعار بداخلها وتوصل إلى بطن المريض [غير مسموع] وتبدأ في إرسال البيانات خارج الجسم، والتي يمكن عرضها من خلال جهاز مثل الهاتف الذكي أو جهاز يمكن من خلاله للموظف الصحي معرفة المزيد من التفاصيل حول ما يحدث داخل الجسم بالضبط.

وهناك الكراسي المتحركة التلقائية. وهي كراسي المقعدين الآلية التي يتم التحكم بها آليا. والنوع التالي هو telehealth أو الصحة عن بعد. وتعني telehealth زيارة طبيب لا يحتاج للفحص البدني. في هذه الحالة أساسا، لا يحتاج المريض إلى زيارة الطبيب جسديا. ولهذا الغرض، هناك بعض الخدمات المختلفة التي يقدمها [kiosks] أو أي نوع من خدمات التداول بالفيديو التي يمكن للطبيب أن يرى تفاصيل المرضى وأن يقدم المشورة الصحية عن بعد.

النوع التالي هو كاميرا شبكية العين للجوال. هذه بعض عدسات الأعين التي يمكن ارتدائها في الثلج، وهي توفر كل البيانات للهاتف الذكي أو أي نوع من الأجهزة المحمولة. ثم لدينا بعض الأدوات الجراحية الآلية. وتستخدم هذه الأجهزة أساسا في جراحة المناظير وجراحة تنظير جوف

البطن. يقوم الموظف أو الطبيب بعرض مباشر لما يحصل داخل الجسم حتى يتمكن الجراحون من الحصول على رؤية أوضح لأجزاء الجسم من خلال هذه الكاميرات.

التالي هو مختبرات الأمراض المتنقلة. ليس علينا زيارة المختبر من أجل الاختبار، لذا يمكننا استخدام بعض الأجهزة في المنزل لجمع البيانات من المرضى. ففي حال أردنا القيام بإجراء فحص دم، فيمكننا أخذ عينة في منزلنا وتقوم الأجهزة بجمع كل البيانات وتحميلها إلى سحابة حيث يمكن للطبيب الوصول إليها.

التالي، هذه بعض [غير مسموع]. الشريحة التالية، من فضلك.

ديبورا إسكاليرا: عذرًا على المقاطعة يا شيفام. هل يمكنك ضبط مستوى الصوت على الكمبيوتر أو سماعة الرأس؟ فالصوت غير واضح. لا أدري ما السبب في ذلك.

شيفام شارما: آسف لذلك. دعوني أغير سماعات الرأس.

ديبورا إسكاليرا: حسنًا، شكرًا جزيلاً. هل تستخدم سماعة رأس يا شيفام؟

شيفام شارما: نعم، أنا أستخدم سماعة الرأس.

ديبورا إسكاليرا: حسنًا، هذا يبدو جيدًا. شكرا لك.

شيفام شارما: أنا [غير مسموع].

ديبورا إسكاليرا: نعم، يرجى المتابعة. شكرا لك.

شيفام شارما: الآن، هذه بنية IoMT، إذن كيف تعمل أجهزة IoMT هذه. فهي أساسا أجهزة استشعار مختلفة [غير مسموع] في جسم المريض، مثل بعض أجهزة الاستشعار [الحيوية]، مثل ضغط الدم أو مثل ارتفاع السكري أو بعض شرائط اللياقة الذكية التي تجمع البيانات من خلال أجهزة الاستشعار ثم تنقل تلك البيانات إلى جهاز ينقلها عبر الواي فاي أو أحد أنواع وسائل الاتصال مثل 4G أو 5G ويقوم بإرسال البيانات إلى السحابة بحيث يستطيع الطبيب الوصول إلى جميع البيانات وتقديم استشارات صحية إلى المريض عن بعد. الشريحة التالية، من فضلك.

لذلك، عندما ننظر إلى نمو أجهزة IoMT، وفقا لتقرير أعدته شركة AllResearch، في عام 2018، كانت قيمة سوق IoMT تصل إلى 44,000 مليون، وهو ينمو الآن بمعدل 24.4% سنويا منذ 2016 إلى 2026. ومن المتوقع أن تصل إلى حوالي [254 مليار دولار] في عام 2026.

لذا فمن المرجح أثناء العام المقبل أن تهيمن الأجهزة الذكية الملبوسة على السوق. ففي عام 2018، كانت الأجهزة الذكية الملبوسة تهيمن على سوق IoMT في العالم، وشكلت حوالي 27% من السوق. وكانت لوازم نقاط الرعاية تمثل أكبر عدد من مجموعات أدوات الرعاية الصحية الشاملة، بما يبلغ 30 في المائة من سوق IoMT العالمي، ويتوقع أن يزيد تطبيق الرصد الآني بنسبة [25 في المائة]. سيزداد CAGR تطبيقات التتبع والتنبيه بنسبة تبلغ [21%]. وCAGR في الأساس هو معدل النمو السنوي المركب. الشريحة التالية، من فضلك.

لأجهزة IoMT فوائد مثل خفض التكاليف الطبية. لنفترض أن المريض يعاني من نوع من الأمراض الشائعة أو التي لا تتطلب أي دخول فوري للمستشفى، بحيث يمكن للطبيب تقديم استشارة عن بعد عبر الإنترنت. ستتم إعادة توجيه كافة البيانات إلى السحابة. وعندئذ سيطلع الطبيب على التقارير ويقدم استشارات صحية عن بعد. إذن، من شأن هذا أن يقلل من حالات العلاج في المستشفيات وأن يقلل أيضا من التكاليف.

بالإضافة إلى أنه سيحسّن تجربة المريض، لذلك لا يوجد شيء لـ... ليس على المريض أن يقلق، وليس عليه الذهاب لزيارة الطبيب. والفائدة التالية هي سهولة إدارة الأدوية الطبية والالتزام الطبي. فسوف يوفر ذلك إدارة صحيحة، بحيث تكون الأجهزة الذكية قادرة على إدارة كل الأشياء آليا وتوفير تجربة جيدة، كما تقلل هذه الأجهزة أيضا من احتمال حصول أخطاء، لأن لهذه الأجهزة دقة جيدة، وبالتالي فسوف توفر نتيجة جيدة، وستوفر أيضا تحكما أفضل في مقدار الهدر في قطاعات الرعاية الصحية لأن الكثير من الموارد تضيع بلا فائدة. إذن فستساعد أيضا على تقليل

[غير المسموع] وستوفر خدمات أكثر كفاءة مما سيسفر عن نتائج أفضل في ميدان العلاج الطبي. الشريحة التالية، من فضلك.

إن بعض عيوب IoMT تشبه عيوب الإنترنت مثل ما يطلق عليه بالتجديف، حيث تظهر فرص للخروقات الأمنية أو الهجمات الإلكترونية الجديدة يوما بعد يوم، كما تتزايد بعض الهجمات الإلكترونية. وهذه الهجمات تعدي الأجهزة.

تشكل إدارة السجلات الطبية الإلكترونية تحديا أساسيا، لأننا إذا كنا نجمع بيانات المرضى فسيتعين علينا أن نتبع قانون امتثال مثل HIPAA، أو FHIR، ولذلك فإن الالتزام بجميع المعايير يتطلب وقتا طويلا. وفي أوروبا، هناك بعض القوانين مثل GDPR، وعلينا أن نتأكد من أننا نمتثل لهذه القوانين. وهناك معايير طبية مثل FHIR وSMART. ويتطلب تنفيذ هذه وقتا أطول. الشريحة التالية، من فضلك.

ومن أمثلة المخاطر المرتبطة بأجهزة IoMT: كون تطويرها يتطلب مدة طويلة، فإذا قمنا بتصميم جهاز مثلا، فيجب أن نتأكد من أننا نقوم بتحديثه باستمرار عبر برنامج تصحيح ما، وإضافة بعض التحديثات لجعله أكثر أمانا.

إن الهدف الرئيسي من هذه الأجهزة هو سلامة المرضى، ويدخل أمن الأجهزة في ذلك، وفي الوقت الحاضر، ومع تغير التكنولوجيا يوما بعد يوم، فسيتحسن أمن هذه الأجهزة أيضا. وهناك بعض الأجهزة، مثل Fitbit مثلا، والتي تستخدم تقنية البلوتوث للتواصل، والتي يمكن أن يتم اختراقها من قبل قراصنة الكمبيوتر. ويمكننا جمع كل بيانات المريض، بما في ذلك مكان تواجدهم وجميع التفاصيل الصحية والمعلومات التي يمكن أن تؤثر على المريض.

ولبعض هذه الأجهزة كلمة مرور مشفرة، وهي تمثل خطرا كبيرا آخر يمكن أن يسمح للقراصنة باختراق تلك الأجهزة بسهولة إذا كانوا قادرين على الوصول إليها، ويكونون قادرين عندئذ على جمع كل البيانات من الجهاز بسهولة.

والتواصل غير المشفر. يجري الاتصال بشكل غير مشفر، ولذلك سيكون من المحتمل أن يقرأ من طرف ثالث مثل عمليات 'الهجوم من الوسط' التي تمكن المخترِق من قراءة كل البيانات.

ومن المخاطر الأخرى نقص إدارة الأجهزة. فلإدارة هذه الأجهزة، يجب أن نتأكد من أننا نتبع جميع المتطلبات، ونقوم بتحديث جميع الأجهزة باستمرار، كما أن الموظفين لدينا مدربون بشكل

صحيح على كيفية التعامل مع ما إذا كان هناك اختراق عبر الإنترنت أو نوع من الهجمات الإلكترونية، وبالتالي لديهم معرفة بكيفية التعامل مع هذا الوضع. الشريحة التالية، من فضلك.

هذه أنواع من الهجمات المرتبطة بهذه الأجهزة.

ديبورا إسكاليرا: شيفام، لقد تجاوزت الوقت، أرجو أن تختم بسرعة. شكرا لك.

شيفام شارما: حسنًا. إذن في الأساس، هذه هجمات، لذا لن أفسر هذا، فالوقت محدود. إذا هذه هجمات مثل استنساخ العلامات، التلاعب والتنصت، وهي هجمات يمكن أن تؤثر على أجهزة IoMT. الشريحة التالية، من فضلك.

كيف يمكن تحسين أمان هذه الأجهزة؟ يجب ألا نستخدم كلمات مرور جهاز [غير مسموع]، بل يجب أن نقوم بتحديث كلمات المرور هذه وتقويتها، ويجب أن نوفر عمليات تصحيح في الوقت المناسب بحيث إذا كانت هناك أية نقاط ضعف أمنية، فسيتم إصلاحها في الوقت المناسب، والتأكد من أن شبكتنا أكثر أمانا حتى يمكنها تجنب أي وصول غير مصرح به. وقد تكون هناك فرص بأن تكون لموظفينا إمكانية استخدام هذه الأجهزة لأغراض سيئة، ولذلك علينا أن نسمح بالدخول لأشخاص محددين وفقا للمتطلبات. إذن لنفترض أن الموظف لا يستخدم جهازا ما، فعلينا حينئذ التأكد من عدم السماح لهم بالوصول إلى تلك الأجهزة، والتأكد من أن هذه الأجهزة تخضع للمراقبة [7/24] بحيث إذا بدأ أي نشاط خبيث، فسيتم إيقافه فورا.

ومن المخاطر الأخرى غياب الاحتواء. [ليس من المهم فقط صد الهجمات.] علينا التأكد من أننا قادرون على التعامل مع الهجوم قبل حدوثه، ولذلك علينا التأكد من أن بنيتنا التحتية آمنة. الشريحة التالية، من فضلك.

وفي المستقبل، قد تكون هناك تحديات مثل تحسين البنية التحتية للرعاية الصحية، ولذلك فسيكون هناك المزيد من الأجهزة في السنوات القليلة المقبلة. هذا كل شيء. شكراً جزيلاً على وقتكم. إن كانت لديكم أي أسئلة، فقوموا بطرحها رجاءا.

ديبورا إسكاليرا: شكرا لك يا شيفام. يبدو أن ريكاردو يرفع يده. ما هو سؤالك يا ريكاردو؟

ريكاردو ناني: شكرا لك. شكرا يا شيفام على عرضك الجيد. أنا لست خبيرا في أنا لست خبيرا في IoT، ولكني مهتم بها، وقرأت أن IoT قد تسببت في قدر كبير من التطور في أنواع التواصل التي تعمل دون عنوان IP. هل تدخل في ذلك نفس مشكلات الأمان التي تواجه الاتصالات المستندة على IP بالنسبة لـ IoT، أم أنها مختلفة نوعيا؟ شكرا لك.

شيفام شارما: هل يمكنك نشر سؤالك على الدردشة؟ أعتقد أن سماعات الرأس لا تعمل.

ديبورا إسكاليرا: حسنًا. شكرا لك. دانيل، هل يمكنك فعل ذلك أيضا؟ لأننا تجاوزنا الوقت المحدد قليلا، ولم يتبق لنا إلا بضع دقائق وأنا أريد أن أتأكد من أن يحصل ريكاردو على فرصة لتقديم سؤاله وتلقي الإجابات. إذن يا دانييل، هلا تفضلت بنشر سؤالك في الدردشة مشكورا.

إذن مقدم العرض الأخير هو ريكاردو ناني. ريكاردو، أنت التالي، و ضع في اعتبارك أن مدة العرض عشر دقائق و بعدها سنستخدم الخمس دقائق الأخيرة في الإجابة على الأسئلة. شكرا لك يا ريكاردو.

ريكاردو ناني: شكرا على الكلمة وشكرا لاستضافتكم لي. أنا آسف، ليست عندي سماعة رأس لكنني أرتدي هذه لتقليل الضجة الخارجية. سأتحدث عن تجزؤ الإنترنت بصفة عامة، ثم سأنتقل إلى دراسة حالة، وأختم بالآثار العامة. الشريحة التالية، من فضلك.

حسنا، فلنبدأ ببعض التعاريف لما نقصده بمصطلح التجزؤ. [بدأ البعض] بتعريفه بطرق مختلفة مثل: التوافر المختلف للمعلومات والخدمات في أماكن مختلفة تحت قواعد مختلفة. وهذا بالطبع تعريف واسع جدا ويتعامل مع التجزؤ كمصطلح واضح جدا. على سبيل المثال، هل سنقول أننا نواجه تجزؤ الإنترنت إذا لم نستطع الوصول إلى نفس محتوى Netflix في إيطاليا والولايات

المتحدة؟ هناك آثار تنظيمية، هناك نوع من التجزؤ في السوق، ولكن إطلاق تجزؤ الإنترنت على هذه الحالات قد يكون بعيدا عن الصواب.

وقد حاولت بعض التعريفات أن تنشئ تصنيفا للتجزؤ، فقسمته إلى حكومي وتجاري وتقني على سبيل المثال. وحاول آخرون دمج مفهوم حياد الإنترنت في ذلك والتحقق مما إذا كانت له أية علاقة بتجزؤ الإنترنت. وبعد هذا، تأتي هنا تعريفات أكثر صرامة لتجزؤ الإنترنت على أنه عدم توافق مع المعايير الأساسية والبروتوكولات وبروتوكولات الإنترنت المختلفة وبروتوكولات النقل المختلفة غير المتوافقة، بينما تأخذ [غير مسموع] اسما آخر، أو تسمية أخرى.

إذن هذه هي كل التصنيفات، ولدينا العديد من التعاريف المختلفة للتجزؤ. وأنا أميل إلى التركيز على الجانب التقني، وإعطاء كل الظواهر الأخرى اسما مختلفا. الشريحة التالية، من فضلك.

ولتوضيح ما أعنيه عندما أتحدث عن التجزؤ، ولتوضيح أنه، على المستوى الفني على الأقل، يمكننا أن نكون متفائلين بشأن بقاء الإنترنت موحدة بشكل عام. أود أن أعرض عليكم دراسة حالة أجريت عن أصحاب المصلحة الصينيين وانخراطهم في شركة ICANN و انخراطهم بشكل عام في إدارة المعرفات الفريدة.

بطبيعة الحال، عندما نتحدث عن التجزؤ، فإننا نميل إلى الحديث عن العديد من القوى العظمى، وليس عن الصين فقط. قد نتحدث عن روسيا مثلا — وقد تحدثنا عن روسيا اليوم بالفعل — لكن بعض الناس اتهموا بعض المشاريع في الولايات المتحدة أيضا بأنها تفضل تجزؤ الإنترنت. أنا أتحدث عن الصين فقط لأن هذا البلد هو مجال خبرتي الجغرافية، وهو المجال الذي لدي إحاطة كافية به.

ونحن نراقب أصحاب المصلحة الصينيين، ونرى أنه في بداية تاريخ ICANN، بدا أن الصين تتخذ موقفا تصداميا جدا تجاه ICANN. فعندما يتعلق الأمر بالاعتراف بتايوان كعضو في المجلس الاستشاري لـ GAC، وقد توقفت الحكومة الصينية عن المشاركة في أنشطة ICANN عندما يتم استخدام هذا الاسم. غير أن المنظمات الخاصة أو المنظمات العامة، حتى تلك التي ترعاها الدولة، لازالت موجودة.

ومن ثم، ولسنوات عديدة، واصل أصحاب المصلحة الصينيون والحكومة الصينية المشاركة في ICANN وأصبحوا مروجين كبارا لأسماء النطاقات الدولية، والتي تحظى بالطبع بالكثير من الاهتمام، من الناحية الاقتصادية والسياسية والثقافية في مساحة الأسماء الصينية.

في البداية كان هناك خلاف بين ICANN والصين حول من يجب أن يكون صاحب الصدارة في اسماء النطاقات الصينية. لذا فقد كان هناك خوف حتى من أن تنشئ الصين نظام أسماء عالمي منفصل. ولكن هذا لم يحدث، وفي الواقع، فإن أصحاب المصلحة الصينيين يشاركون بشكل كامل في ICANN، وفي عمل IDN.

وهنا عندما نرى [غير مسموع] بين ICANN والصين. تعود الصين إلى المشاركة الكاملة في اللجنة الاستشارية الحكومية، وتستضيف اجتماعا كبيرا لـ ICANN في بكين في عام 2013، وفي عام 2014، أيد رئيس إدارة الفضاء الإلكتروني في الصين آنذاك مبدأ تعدد أصحاب المصلحة في اجتماع ICANN50. الشريحة التالية، من فضلك.

وكان لهذا بطبيعة الحال تداعيات على موقف أصحاب المصلحة الصينيين من الجوانب المرتبطة بتجزؤ الإنترنت وإدارة محددات الهوية الفريدة. ونحن نرى على سبيل المثال أنه بعد انتقال IANA، أصبح ممثل GAC الصيتي نائبا للرئيس، مما يشير أيضا إلى مشاركة أقوى للحكومة الصينية. ومن ناحية أخرى، أصبح أصحاب المصلحة في الصين، وحتى القطاع الخاص مثل هواوي، أكثر نفوذا في مجالات أخرى مرتبطة بموارد الإنترنت الحرجة ومعرفات فريدة، مثل IETF.

ومع ذلك فقد ظهرت ثغرات جيوسياسية جديدة في ITU، وهو [مكان] متعدد الأطراف، عندما قدمت هواوي، ووزارة الصناعة وتكنولوجيا المعلومات وغيرها من الجهات الفاعلة الصينية ما يسمى اقتراح IP الجديد.

ولكن على الرغم من وجود هذا النوع من الغموض، فإننا نرى أن أصحاب المصلحة الصينيين أصبحوا أكثر انخراطا في ICANN. وسأريكم الآثار المترتبة على هذا في الشريحة التالية. الشريحة التالية، من فضلك.

حسنا، ما لدينا الآن هو أنه بعد كل تلك السنوات من المواجهة، أصبح أصحاب المصلحة الصينيين، بما في ذلك الحكومة الصينية، أكثر مشاركة في ICANN. وقد استخدمت هذه البلدان نفس DNS ونفس البروتوكولات التي تستخدمها بلدان أخرى. وهي تشارك في ICANN. ولها تأثير في IETF. وسأتخطى هنا جميع ما يتعلق بالمنهج الذي اتبعته، لكنني استخدمت بشكل رئيسي أساليب نوعية، بما في ذلك مقابلات الخبراء، في جمع هذه البيانات.

والسبب وراء حدوث هذا هو أن الشركات العالمية القوية، والجهات الفاعلة العالمية القوية تريد فوائد الشبكة. إن تقسيم المعايير من شأنه أن يرغم شركات مثل هواوي على إنتاج أجهزة مختلفة

لأسواق مختلفة، حيث ينبغي أن تكون قادرة على الاتصال بمعايير مختلفة غير قابلة للتشغيل البيني، في حين أنه من الأسهل بكثير لشركة عالمية أن تكون قادرة على إنتاج نوع واحد من الأجهزة على نطاق عالمي. فهذا أكثر ربحية بكثير.

لذا، ما يمكن أن يحدث هو أن الدول، مثل الصين، ومثل روسيا، قد تميل إلى أن يكون لها تأثير أقوى في التنظيم المحلي، وفي ما يمكن أن يحدث في الإنترنت، في أي نوع من الأنشطة يمكن للمواطنين القيام به على الإنترنت من أجل مد نفوذهم السياسي بحيث تصبح المعايير في حال يسمح للشركات المحلية بالازدهار. وهذا هو نوع الخطوات التي اتخذتها الصين في انخراطها في ICANN، وIETF، و [موارد الإنترنت] الحرجة وAt-large، إن صح التعبير. الشريحة التالية، من فضلك.

فما نراه الآن هو أن تجزؤ الإنترنت التقني هو سلاح الضعفاء، بينما يفضل الفاعلون الأقوياء احتكار فوائد الشبكة. ربما يريدون السيطرة على حركة المرور على الإنترنت، وخاصة عندما يتعلق الأمر بالمعلومات وتنظيم المجتمع المدني. ولكنهم، عندما يتعلق الأمر بالمعايير التقنية، يريدون أن يكونوا قادرين على إنتاج نفس الأجهزة في كل مكان، وتسويقها في كل مكان، والاحتفاظ بفوائد الشبكة [غير مسموع].

فماذا يخبرنا هذا عن تجزؤ الإنترنت؟ يخبرنا بأن الجهات الفاعلة الأكثر قوة لديها مصلحة في الحفاظ على وحدة الإنترنت وأن أضعف الجهات الفاعلة فقط هي التي قد تحاول تجزئة الإنترنت على المستوى الفني. وهذا يجعل الإنترنت، مرة أخرى، وIP، وبروتوكول TCP/IP، وهي محور الإنترنت التقني، مرنة جدا. ذلك أن الصين تفرض رقابة قوية، ولكن على المستوى الفني، لا تحتاج إلا لشبكة VPN للتغلب على ذلك. بالطبع، يمكن أن يكون هذا خطيرا جدا من الناحية السياسية في بعض السياقات، فيمكنك أن تستخدم الشبكات الخاصة إذا كنت تنتمي لبعض المجموعات على سبيل المثال، وهذا هو حال من ينتمي للسكان الأويغور على سبيل المثال. ولكن على المستوى الفني، كل ما يتطلبه الأمر هو شبكة الاتصال الافتراضية VPN.

إذن هذه أخبار جيدة لبقاء الإنترنت موحدة في جوهرها التقني نوعا ما. وفي حين أنه لا تزال هناك حالات تنافس، وحالات تتسم بالغموض، وحالات من الاشتباكات الجيوسياسية على جوانب أساسية جدا من الإنترنت، وحتى على المستوى التقني، فإن النظام كما يبدو يظهر بعض المرونة. الشريحة التالية، من فضلك.

وبهذا أختم. شكرا على انتباهكم. ويسعدني أن أجيب على تساؤلاتكم.

ديبورا إسكاليرا: حسنًا. شكرا لك يا ريكاردو. هل هناك أسئلة لريكاردو؟ هل من يد أو أي سؤال في الدردشة؟ تفضل يا دانيل.

دانيل غولوبف: شكرا لك يا ريكاردو، على عرضك الرائع. لقد كانت مفيدة ومتماسكة للغاية. أريد أن أسأل عن توقعاتكم المحتملة حول حالة التجزؤ في المستقبل. هل تعتقد أن توحيد الإنترنت ستكون له الغلبة، أو أنك متشائم نوعا ما، وترى أنه سيكون هناك تجزؤ في بعض الأجزاء بحيث تصبح معزولة. شكرا لك.

ريكاردو ناني: شكرًا لك على سؤالك. هذا في الواقع شيء ذو صلة. سأقول أنه سيكون هناك شكل من أشكال تجزئة السوق، كما هو الحال في العديد من الدول الغربية التي لا ترغب، على سبيل المثال، في وجود ممثلين صينيين في بنيتها التحتية المحلية، حتى تلك المتعلقة بالهاتف مثل 5G على سبيل المثال والعكس صحيح. لذا فقد يحدث تجزؤ في السوق. ولكن عندما يتعلق الأمر بالمعايير، فإنني أرى احتمالا للتقارب، وكان هذا هو الحال على كل من بروتوكول الإنترنت ونظام أسماء النطاقات، ولكن أيضا على 5G على سبيل المثال.

وعندما يتعلق الأمر ب 3G، فقد كانت هناك معايير إقليمية أو معايير وطنية أكثر تنافيا. وحتى لو كان ITU يعترف بها، فإنها لم تنشر إلا على المستوى المحلي ولم تكن قابلة للتشغيل البيني مع معايير الجيل نفسه المنتشر في أماكن أخرى من العالم، ولا يزال ITU يعترف بها، حيث أصبح لدينا الآن تقارب أقوى بكثير بهذا المعنى. لدينا ثلاثة معايير 5G، لكنها قابلة للتشغيل البيني، هذا ما قاله الاتحاد الدولي للاتصالات عندما وافق عليها.

لذا هناك تقارب في المعايير لأنه كما قلت، تفضل الشركات الكبيرة أن تكون قادرة على إنتاج الأجهزة عالميا، وبدلا من أن يكون لديها معاييرها الخاصة بطريقة ما، فإنها تريد أن يكون لها [فرصة] كبيرة من حيث براءات الاختراع للتكنولوجيا العالمية ومن ثم تكون قادرة على تسويق الأجهزة والشبكات في كل مكان مستفيدة من الاقتصادات العالمية [على النطاق العالمي].

ولكن في الوقت نفسه، ما يمكننا أن نراه، هو تجزئة تجارية تقودها الحكومات، ويمكننا أن نرى أن الأمور تتجه نحو تنظيم أقوى. وهذا صحيح في روسيا والصين حيث نرى أن الحكومة تصبح أكثر تأثيرا من حيث الرقابة، وفي قوانين توطين البيانات، ولكن أيضا في أوروبا والولايات

المتحدة، كانت إدارة ترامب شديدة التدخل - انظروا إلى مشروع الشبكة النظيفة على سبيل المثال، ولكن انظروا أيضا إلى الاتحاد الأوروبي. إن GDPR عبارة عن نظام متطور للغاية لحماية البيانات، ولكنه يخلف أيضا تأثيرا قويا خارج الحدود الإقليمية.

الآن، بالطبع، بالنسبة لي كمواطن من الاتحاد الأوروبي، هذا مرغوب جدا. أشعر أنني محمي من قبل GDPR، لذا أنا داعم لها تماما ولا أنتقدها. كل ما أقوله هو أن الاتحاد الأوربي يحاول أيضا أن يكون له بعض الثقل في السوق الرقمي وفي ميدان التطوير المستقبلي للتقنيات الرقمية، وهذا يشمل أيضا معايير الإنترنت المستقبلية لأن معايير الإنترنت سيكون لها تأثير على التطوير المستقبلي للذكاء الاصطناعي، على سبيل المثال، والعكس بالعكس، والذكاء الاصطناعي أيضا [راسخ بعمق في] 5G، فكلاهما يعمل مع 5G لتمكين الذكاء الاصطناعي والعكس بالعكس، فالذكاء الاصطناعي مدمج في شبكات 5G.

لذا إذا كان لديك سيطرة قوية على البيانات، فلديك أيضا تأثير قوي عندما يتعلق الأمر بأي شكل من أشكال تطور الذكاء الاصطناعي، لأن البيانات هي المادة الخام هنا.

باختصار، هناك تدخل أقوى من الدول على المستوى التنظيمي، وربما أيضا من حيث التحكم بالمعلومات، هذا على الأقل ما نراه في الصين، وعلى حسب فهمي، في روسيا أيضا، لكنني لست خبيرا في روسيا. ولكن هناك تقاربا بين المعايير. آمل أن يجيب هذا على سؤالك. وكان هناك لف ودوران في بعض النقاط.

دانيل غولوبف: نعم. شكرًا جزيلًا.

ديبورا إسكاليرا: حسنًا. رائع. لقد وصلنا إلى رأس الساعة. شكرا لك يا ريكاردو. عرض رائع. ولكل من قدم اليوم، ولكل من عمل على موضوع NextGen، لقد قمتم بعمل رائع. ممتاز. أنا فخورة بكم جميعًا. لقد قمتم بعمل رائع.

أود أن أشكر كل من حضر اليوم. شكرا لفيرناندا إيونيس التي قامت بعرض الشرائح اليوم. شكرا لمترجمينا الفوريين، وبالطبع، لفريقنا التقني الرائع الذي يدعمنا خلال الاجتماعات، في كل اجتماع. ويرجى الانضمام إلينا في الجزء الثاني من العروض التقديمية التي سيتم تقديمها حول NextGen غدا، والتي ستتم في الساعة 8:30 بالتوقيت العالمي، 10:30 بتوقيت CEST.

شكرًا لكم جميعًا. أقدر دعمكم وأقدر حضوركم اليوم في الجزء الأول من العرض الذي سيقدمه الجيل التالي. أحسنتم جميعًا. رائع. شكراً لوجودك معنا. إذا كانت هناك أي أسئلة، فالرجاء إرسالها إلى—

شيري ستوبس: شكرًا يا ديبورا.

ديبورا إسكاليرا: شكرا لك.Engagement@icann.org إذا كانت لديكم أية أسئلة إضافية أو أسئلة متابعة لمقدمي البرامج. شكرًا جزيلاً لكم على حضوركم معنا اليوم.

شيري ستوبس: إلى اللقاء.

[إنتهاء التدوين]