اجتماع ICANN72 | الاجتماع السنوي العام الافتراضي – عروض برنامج NextGen للجيل التالي التعريفية
الإثنين، الموافق 25 أكتوبر/تشرين الأول 2021 – من الساعة 10:30 إلى الساعة 12:00 بتوقيت المحيط الهادي الصيفي

ديبورا إسكاليرا: أهلاً ومرحبًا بكم جميعًا في عروض برنامج NextGen للجيل التالي في ICANN رقم 72. أنا اسمي ديبورا إسكاليرا وأنا أدير برنامج NextGen للجيل التالي في ICANN. وأنا مدير المشاركة عن بُعد لهذه الجلسة.

يرجى العلم بأنه يجري تسجيل 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.

وتتم الترجمة الفورية للجلسة باللغة الإنجليزية والفرنسية والإسبانية. انقر فوق رمز الترجمة الفورية وحدد اللغة التي ستستمع إليها أثناء 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. والرجاء التكرم بذكر الاسم للتدوين في السجل وتحديد اللغة إذا كنتم ستتحدثون بلغة أخرى غير 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" أو 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. علمًا بأن أي رسالة يرسلها عضو في اللجنة أو حاضر عادي إلى حاضر عادي آخر لن يراها إلا مضيفو الجلسة المساعدون والمضيف وأعضاء اللجنة الآخرون.

وبهذا، أود أن أرحب بكم وأشكر مشركينا في برنامج NextGen على ما بذلوه من عمل شاق في إعداد هذه العروض التعريفية. وأود أيضًا أن أتوجه بالشكر إلى معلمينا، آريس إغناسيو وديسالين ياهوالا اللذين دأبا على العمل بلا كلل طوال الأسابيع الثمانية الماضية في توجيه وتعليم الطلاب وتوجيههم خلال هذه العملية ومساعدتهم على الاستعداد لاجتماع ICANN72. لقد كانوا يعملون بجهد حقيقي، ولم أكن لأقوم بهذا لولا مساعدتهم.

بالإضافة إلى ذلك، أود أن أتوجه بالشكر إلى زميلي، سيرانوش فاردانيان الذي سيدير شرائح العرض لي اليوم. لك بالغ التقدير والامتنان على ذلك، سيرانوش. وبهذا، ولأن أمامنا 90 دقيقة فقط ومعنا ستة عروض تقديمية، ونحن ننوي البدء على الفور وسوف أحيل الكلمة إلى أول متحدث لدينا وهو سارة السمّان. سارة، الكلمة لك، وبعد ذلك سوف نتبع كلمتك بالأسئلة.

سارة السمّان: مرحبا. شكرًا جزيلاً لكِ، ديبورا. مرحبًا، شكرًا لكم على استضافتي. أريد أن أتحدث اليوم حول نظام أسماء النطاقات وانتهاك المحتوى، وبالأخص المعلومات المضللة. الشريحة التالية، من فضلك.

بالنسبة لمن قد لا يعلمون بالفعل، فإن DNS أو نظام أسماء النطاقات عبارة عن نظام متكامل يدعم ويقوي الإنترنت في توصيل مستخدميه والأجهزة المتصلة به. وكما هو الحال بالنسبة للأنظمة الأخرى، رغم ذلك، فإنه عرضة للانتهاك. ووفقًا لما أكدت عليه اللجنة الاستشارية الحكومية التابعة لـ ICANN، فإن من يتولون مهمة إدارة البنية التحتية لنظام أسماء النطاقات يجب عليهم اتخاذ تلك الخطوات من أجل ضمان أن هذا المصدر العام يتسم بالسلامة والأمن معًا.

وهذا الأمر من الأهمية بمكان بالنسبة للجمهور لكي تكون لديه القدرة على إيلاء الثقة والاعتماد على الإنترنت في الاتصالات والمعاملات الضرورية. والأهداف التي أسعى لتحقيقها من وراء هذا العرض التقديمي هو التشجيع على الحوار في مجتمع أصحاب المصلحة حول هذه القضية الهامة المتعلقة بالسياسة العامة وأيضًا لتشجيع مجتمع ICANN على مواصلة اعتراض الانتهاكات في نظام أسماء النطاقات وترتكب به وحوله ككل.

لكن قبل أن نتمكن من التعامل على النحو الصحيح مع انتهاك نظام أسماء النطاقات DNS، ينبغي أن يكون لدى أمناء السجلات والسجلات فهم مشترك حول كيفية تعريف ذلك. الشريحة

التالية، من فضلك. وطبقًا لإطار عمل انتهاك نظام أسماء النطاقات DNS لدى شبكة سياسة الإنترنت والاختصاص القضائي، فإن هناك خمسة أشكال أساسية للانتهاك تم تعريفها بالفعل. وهي في الحالات الخاصة بكل من البرامج الضارة وبرامج الروبوت والتصيُّد الاحتيالي والاستدراج ورسائل البريد الإلكتروني غير المرغوبة.

كما أن هناك حالة انتهاك المحتوى، وهي ليست ذات طابع فني ويجب أن يكون لها تصنيفها الخاص. ولحماية حرية التعبير عن الرأي، فإن السجلات وأمناء السجلات غير مطالبين دائمًا بالتصرف حيال انتهاك محتوى الويب. وعلى الرغم من ذلك، يوافق إطار عمل اللجنة الاستشارية الحكومية GAC على أن هناك حالات نوعية يجب فيها اتخاذ إجراءات وهي التي تكون في حالات مواد الاعتداء الجنسي على الأطفال، والتوزيع غير القانوني على الإنترنت لأشباه الأفيونيات، والإتجار بالبشر، والتحريض النوعي والموثوق على العنف. الشريحة التالية، من فضلك.

وبما أننا الآن قمنا بتعريف انتهاك المحتوى على نظام أسماء النطاقات، فإننا أريد أن أستعرض مشكلة شبكات بوت نت التي تعمل على وسائل التواصل الاجتماعي. وأنا متأكد من أن بإمكاننا أن نلاحظ اليوم أن خوارزميات معالجة البيانات تصبح من الأدوات المؤثرة بشكل متزايد في فهمنا واستيعابنا لواقعنا. والأشهر حول شبكات البوت التي تعمل لصالح الجهات الفاعلة السياسية والتي تتمكن بعد ذلك من التلاعب بالرأي العام عبر أهم تطبيقات وسائل التواصل الاجتماعي التي نستخدمها كل يوم.

إن قدرة شبكة بوت نت على توجيه بناء وتركيب المشكلات العامة له تأثير مباشر على فهم وترتيب واقعنا الاجتماعي والسياسي. ونحن نرى ذلك كثيرًا جدًا في الدعاية الكمبيوترية، وقد أظهرت الدراسات - كتلك التي سأعرضها عليكم في الشريحة التالية - أنها يمكن أن تظهر على الأرجح خلال أزمة أو بعدها، مشوهة إياها ومحدثة الكثير من الضرر حول تلك الأزمة الخاصة.

ونظرًا لأن لحظات الكارثة ينجم عنها عدم يقين جماعي بالنسبة للجماهير، وهو ما يؤدي بالجماهير على هذه الشبكات إلى التعرض الشديد للتأثير. الشريحة التالية، من فضلك.

إذن فقد أجرت المجلة البريطانية لعلم الاجتماع دراسة حول الاتصالات من خلال موقعي تويتر وفيسبوك بعد تفجيرات مانشستر، والتي كانت عبارة عن هجوم إرهابي. وفي حالة واحدة، نشر حساب لسيدة على فيسبوك أنها كانت تؤوي أكثر من 60 طفلاً تائهًا. كما كان رقم هاتفها مرفقًا

أيضًا في هذا المنشور وسريعًا ما تم تعميمه عبر موقع تويتر. وقد انتشر المحتوى بشكل كبير لدرجة أنه تم وسهما في النهاية بعبارة ملاك مانشستر في جريدة ديلي ميل.

لكن تكمن المشكلة في أن هذه الفعالية لم تحدث أبدًا. وهذا ما يمكن أن نطلق عليه اسم الاستضافة الوهمية للفعاليات. وقد أوضحت السيدة للشرطة بعد ذلك أنها لم تنشر أبدًا أي منشورات أو أنها أعلنت حتى عن رقم هاتفها، وادعت بأن الحدث قد صعقها وأنها تلقت العديد من المكالمات طوال الليل. وقد حدثت 28 فعالية وهمية منفصلة مثل هذه في نفس الليلة، الأمر الذي أضفى مزيدًا من التخبط في أعقاب عملية التفجير. الشريحة التالية، من فضلك.

وهناك حادثة أخر منفصلة وقعت عبر الإنترنت في تلك الليلة، تم وضع منشور على فيسبوك يزعم أن هناك مسلح في مستشفى أولدام ويحتجز بها رهائن. وقد تم وضع هذا المنشور بعد التفجير مباشرة وشاركه 368 حساب على تويتر بعد الحصول على لقطات شاشة من فيسبوك. وقد أنكرت المستشفى هذه الشائعة، وبرغم ذلك لم تتوقف هذه المعلومات المغلوطة عن الانتشار في الساعات الحاسمة للغاية التي أعقبت الهجوم الإرهابي.

وبسبب هذه الحادثة الوهمية بالأخص، اضطرت بعض أطقم الطوارئ في مواقعها بعد أكاذيب وادعاءات من هذا النوع. وما يجعل مواقف مثل هذه خطيرة للغاية هو مدى ما يمكن أن تتأثر به سلامة المجتمعات على نطاق واسع عندما يكون بمقدور شبكات التواصل الاجتماعي فعليًا من قطع الاتصال بين خدمات الطوارئ ثم الجماهير التي تقدم لها تلك الخدمات. الشريحة التالية، من فضلك.

إذن وبشكل واضح فإن انتهاك محتوى مواقع الويب يمثل تهديدًا لحياة البشر وللسلامة المدنية، ومن ثم يجب مناقشتها للتوصل إلى سياسة في المستقبل. كما يجب وضع إجراءات من أجل تحفيز اعتماد تدابير وقائية لمكافحة الانتهاك في شروط وأحكام اتفاقيات السجل الجديدة أو المتطورة وذلك لضمان أمن الإنترنت ومجتمع مستخدميه في المستقبل. شكرًا.

ديبورا إسكاليرا: شكرًا لكِ سارة. أحسنت. حسنًا، هل هناك أية أسئلة موجهة إلى سارا؟ أنا لا أرى أي أسئلة. يمكنكم دائمًا طرح الأسئلة في النهاية إذا ما تبادر إليكم أي شيء. وبهذا، سوف ننتقل إلى المتحدث التالي، ميري بغداساريان. شكرًا.

ميري بغداساريان: شكرًا لكما، ديبورا وسيرانوش. طابت أوقاتكم أينما كنتم. أنا اسمي ميري بغداساريان وأنا خريج جديد في مجال القانون من كلية الحقوق بجامعة بنسلفانيا. وقد جاء بي اهتمامي بمجال الخصوصية ووضع السياسات في ICANN إلى موضوع كلمة اليوم، وهي على وجه الخصوص اعتماد خدمات الخصوصية والبروكسي. الشريحة التالية، من فضلك.

فقد اعتمد مجلس إدارة ICANN في 2013 اتفاقية اعتماد أمناء السجلات الجديدة، أو RAA وهي عبارة عن عقد يغطي العلاقة بين ICANN وأمناء السجلات المعتمدين لديها. وكما نرى، فقد كان لبنود هذه الاتفاقية تأثير على المسجلين والأطراف الأخرى المشمولين في نظام أسماء النطاقات.

وبالبدء في المفاوضات الخاصة بهذه الاتفاقية بين ICANN ومجموعة أصحاب المصلحة في أمناء السجلات في أكتوبر/تشرين الأول 2011، طلب مجلس إدارة ICANN أيضًا تقرير مشكلات من منظمة دعم الأسماء العامة بحيث إنه عند الانتهاء من المفاوضات بدأت منظمة دعم الأسماء العامة عملية لوضع السياسات من أجل التعامل مع أية مشكلات لم يتم التعامل معها أثناء هذه المفاوضات. وقد تم تحديد المشكلات ذات الصلة بخدمات الخصوصية والبروكسي بأنها واحدة من تلك المشكلات المتبقية.

وتحتوي اتفاقية اعتماد أمناء السجلات لعام 2013 فعليًا على مواصفة مؤقتة تغطي التزامات أمناء السجلات فيما يخص خدمة الخصوصية/البروكسي. وقد تم تمديد الموعد النهائي لهذه المواصفات المؤقتة عدة مرات بالفعل وحاليًا من المقرر ان تنتهي في 31 يوليو/تموز 2022 أو عندما تقوم ICANN بتنفيذ برنامج الاعتماد الجديد، أيهما يحدث أولاً.

ولكن قبل أن نكمل، دعونا نفهم ما هو المقصود بخدمات الخصوصية/البروكسي. ففي الوقت الحالي، فقد تم تعريفها بموجب المواصفة المذكورة. ومن ثم فإن أي خدمة خصوصية تتيح تسجيل اسم نطاق باسم المسجل ولكن جميع تفاصيل الاتصال الأخرى المعروضة في خدمات دليل بيانات التسجيل المتاحة للجمهور لا تقدم فعليًا من خلال موفر خدمة الخصوصية وليس أيضًا من خلال المسجل.

أما في حالة خدمة البروكسي، تتيح هذه الخدمة لصاحب الاسم المسجل ترخيص استخدام اسم النطاقات لأي عميل يستخدم النطاق فعليًا، ويتم تقديم معلومات الاتصال في هذا الدليل من خلال موفر خدمة البروكسي. الشريحة التالية، من فضلك.

بموجب هذه المواصفة، وهي المواصفة المعمول بها في الوقت الحالي، فإن لدينا الحد الأدنى من مجموعة المتطلبات التي تنطبق على خدمات الخصوصية/البروكسي. ويشمل الحد الأدنى من المتطلبات الرئيسية الأربعة الإفصاح عن شروط الخدمة الأساسية؛ ونشر نقطة الاتصال الخاصة بالانتهاك/إساءة الاستخدام؛ ونشر معلومات اتصال الأعمال؛ وأيضًا مستودع بيانات العملاء. وكما نرى، تحاول المواصفة تناول مسألة التعامل مع بيانات التسجيل غير العامة هذه. الشريحة التالية، من فضلك.

لكن ما الذي يحملنا على مناقشة هذا الموضوع؟ لماذا يعتبر هذا الأمر مهمًا؟ فإذا ما عدنا إلى عام 2011، عندما طلب مجلس إدارة ICANN تقرير المشكلات من منظمة دعم الأسماء العامة، سلط مجلس إدارة ICANN الضوء أيضًا على ضرورة معالجة هذه المشكلة في خدمات الخصوصية/البروكسي، لأن هذا الأمر سوف يوفر حماية أكبر للمسجلين وسوف يؤدي إلى تقليل عمليات انتهاك نظام أسماء النطاقات DNS.

ومنذ ذلك الحين، باتت المشكلة أكثر صعوبة فعليًا كما أنها تفاقمت أكثر خلال الجائحة. على سبيل المثال، خلال جلسة اللجنة الاستشارية الحكومية GAC في اجتماع ICANN68 حول انتهاك نظام أسماء النطاقات DNS، لوحظ أن نسبة 65% من النطاقات المستخدمة في الاحتيال عن الناس خلال الجائحة كانت مخفية عبر خدمات الخصوصية/البروكسي. وعلاوة على ذلك، أطلق بعد المحامين المتمرسين إنذارًا بأنه وبعد دخول قانون حماية البيانات العامة GDPR حيز التنفيذ، فإن عدد شكاوى السياسة الموحدة لفض نزاعات أسماء النطاقات في المنظمة العالمية للملكية الفكرية ضد منتهكي نظام أسماء النطاقات قد زاد بشكل كبير، كما أن غالبية هذه الشكاوى ينطوي على افتقار دائم للالتزام بالإفصاح عن معلومات الاتصال من موفري خدمة الخصوصية والبروكسي. ونتيجة لذلك، يطالب أمناء السجلات أو موفري البروكسي المرتبطين بهم من أصحاب IP رفع قضية بالإجراءات الموحّدة لتسوية نزاعات أسماء النطاقات من أجل الحصول على معلومات الاتصال الخاص بمنتهك نظام أسماء النطاقات.

ومن الواضح أن هذا الأمر يثير الكثير من المخاوف غير الضرورية فيما يخص قضاء المزيد من الوقت أو استعراض الإجراءات البسيطة بالإضافة إلى إنفاق المزيد من الوارد من أجل الحصول على معلومات الاتصال من أجل المضي قدمًا في شكاويهم. وبمعنى آخر، سوف يساعد الاعتماد فعليًا على تطوير حماية المسجلين من أجل الحد من انتهاك نظام أسماء النطاقات DNS إضافة إلى الحد من عدد شكاوى الإجراءات الموحّدة لتسوية نزاعات أسماء النطاقات. لنعد الآن مرة أخرى إلى طلب مجلس إدارة ICANN بإضافة تقرير من منظمة دعم الأسماء العامة ومناقشة ما حدث بعد [ذلك]. الشريحة التالية، من فضلك.

في الشريحة التالية، نشاهد نظرة عامة على عملية وضع السياسات في منظمة دعم الأسماء العامة أو عملية PDP. وبموافقة من مجلس الإدارة على اتفاقية اعتماد أمناء السجلات لعام 2013، فقد أطلقت منظمة دعم الأسماء العامة عملية وضع السياسات الخاصة بها وأسست مجموعة عمل فيما بعد في نفس العام.

وقد تم اعتماد توصيات السياسة من خلال مجلس منظمة دعم الأسماء العامة في يناير/كانون الثاني 2016 واعتمدها مجلس إدارة ICANN بعد ذلك في أغسطس/آب 2016. وبعد ذلك، فقد أوعز مجلس الإدارة إلى منظمة ICANN بتنفيذ التوصيات. الشريحة التالية، من فضلك.

وبالنسبة لبرنامج الاعتماد الجديد، كما نرى في الشريحة، فإنه يحتوي على متطلبات أكثر دقة من المواصفات التي ناقشناها للتو. واستنادًا إلى ما نراه على الشاشة، يتضح لنا أن البرنامج الجديد يحاول حل المشكلات التي ناقشناها للتو والتي تتصل بخدمات الخصوصية/البروكسي.

فعلى سبيل المثال، يوفر إطار عمل تفصيلي لردود موفر الخدمة على الطلبات المقدمة من جهات إنفاذ القانون وأصحاب الملكية الفكرية، أو يضع المعايير للمتطلبات الخاصة بترحيل الموفرين للاتصالات من الأطراف الأخرى إلى عملاء خدمة الخصوصية والبروكسي كما يوفر برنامجًا تعليميًا إلزاميًا لموفري الخدمة.

وكما نرى، يحاول البرنامج التعامل مع المشكلات الكائنة في المواصفة الحالية من أجل توفير إطار عمل أكثر شفافية ومعقولية من أجل الاعتماد. الشريحة التالية، من فضلك.

وكما ذكرت لكم، وبعد أن اعتمد مجلس منظمة دعم الأسماء العامة توصيات مجموعة العمل، فقد وافق مجلس إدارة ICANN عليه وأرسله إلى منظمة ICANN من أجل التنفيذ. وكان من

المتوقع أن يحل برنامج اعتماد جديد مخل المواصفات المطروحة بموجب اتفاقية اعتماد أمناء السجلات. وعلى الرغم من ذلك، لإن تنفيذ هذا البرنامج موقوف حاليًا، والسبب في ذلك ينبع من جهود ICANN المبذولة من أجل جعل ممارسات حماية البيانات الحالية متوافقة مع قانون حماية البيانات العامة.

وللعودة بالزمن قليلاً، في يوليو/تموز 2018، وبعد قرار مجلس إدارة ICANN باعتماد المواصفة المؤقتة لبيانات تسجيل gTLD، أطلق مجلس منظمة دعم الأسماء العامة وأسس عملية وضع السياسات المعجّلة أو EPDP وهي أول عملية EPDP في تاريخ ICANN.

وبعد ذلك في شهر مارس/آذار 2019، اعتمد مجلس منظمة دعم الأسماء العامة تقريرًا، وهو التقرير الأول لمجموعة العمل للمرحلة الأولى من عملية وضع السياسات المعجَّلة، بموافقة مجلس إدارة ICANN على 27 توصية من واقع 29 من هذا التقرير. وعلى الرغم من ذلك، وبموجب التوصيات الـ 27 من تقرير المرحلة الأولى، بات واضحًا أنه في ضوء هذه التطورات الجديدة وفي ضوء الممارسات الأكثر امتثالاً لقانون حماية البيانات العامة GDPR في ICANN، كانت هناك حاجة إلى مراجعة الممارسات ذات الصلة والتي تعود أيضًا—المرتبطة أيضًا بأي من بيانات التسجيل غير المتاحة أمام الجماهير.

وهذا هو السبب في أن هذا البرنامج ما يزال موقوفًا على تعقيبات ومراجعة المجتمع، وبشكل أساسي إذا ما فكرنا فيه، فإن توصيات برنامج الاعتماد تسير في اتجاه نفس الهدف، ألا وهو تقرير آلية قانونية للوصول إلى بيانات التسجيل غير العامة ومعالجتها. الشريحة التالية، من فضلك. وبعد استئناف عملية التنفيذ، فإننا نتوقع أن تتم المطالبة بتعقيبات وآراء المجتمع على المستندات التالية. الشريحة التالية، من فضلك.

سوف تتم المطالبة بتعقيبات وآراء المجتمع على سياسة اعتماد الخصوصية/البروكسي والاتفاقية والبرنامج ودليل مقدمي الطلبات إضافة إلى إجراءات التعليق وإلغاء الاعتماد ونقل الملكية. باختصار، نرى أن اعتماد خدمات الخصوصية/البروكسي مسألة هامة شقت طريقها في عملية وضع السياسات الخاصة بـ ICANN. لكن ولأن تنفيذ برنامج الاعتماد يعد جزءًا من الأحجية الأكبر في جهود ICANN للحصول على ممارسات ممتثلة لقانون حماية البيانات العامة GDPR، فإنه موقوف، وفي ضوء توصيات عملية وضع السياسات المعجَّلة [من الضروري] موافقة المشروعات لجميع أجزاء الأحجية لكي تتلاءم معًا.

وعلى أية حال، يحتوي برنامج الاعتماد على أسلوب أكثر دقة من متطلبات المواصفة الحالية. وعلى الرغم من ذلك، وفي نفس الوقت، فإن المشكلات الأساسية في خدمات الخصوصية/البروكسي لا يبدو أنها تتلاشى، لكن وكما ذكرت لكم، فقد تفاقمت خلال الجائحة. ولذلك، ومع الأخذ بالاعتبار أهمية البرنامج، فإنني أتمنى أن ينطلق التنفيذ في أقرب فرصة من أجل التعامل مع المشكلات الأساسية. شكرًا جزيلاً لكم، وأنا أتطلع لمعرفة المزيد حول هذا الموضوع والموضوعات الأخرى خلال اجتماع ICANN72. شكرًا.

ديبورا إسكاليرا: شكرًا لك، ميري. يبدو أن هناك سؤال في مربع الدردشة. السؤال يقول، "هلا تفضلتم بشرح مستودع البيانات قليلاً في سياق الموضوع قيد المناقشة؟"

ميري بغداساريان: نعم. هذا موضوع طويل فعلاً ولذلك ربما قمت فقط بكتابة إجابتي إذا ما أردتم مواصلة النقاش. لكن في عجالة، فإنه يتعلق بالكيفية التي سوف تتعامل بها خدمات الخصوصية/البروكسي مع أي طلب من جهات إنفاذ القانون أو من أصحاب الملكية الفكرية وكيف يمكنهم حفظ ومعالجة البيانات التي تتناولها هذه الخدمات. هذه إذن إجابة قصيرة، لكن يمكنني كتابة إصدار أطول من ذلك في مربع الدردشة إذا وافقتم.

ديبورا إسكاليرا: بالتأكيد. شكرًا جزيلاً. هل ثمة أسئلة أخرى موجهة إلى ميري؟ حسنًا، سوف نلقي نظرة على مربع الدردشة. شكرًا جزيلاً. أحسنت. حسنًا، سننتقل إلى المتحدث التالي، ساي شاندراسيكاران. ساي، الكلمة لكم.

ساي شاندراسيكاران: شكرًا لكما، ديبورا وسيرانوش. أنا ساي شاندراسيكاران وسوف أتحدث اليوم عن موضوع أهتم به كثيرًا خلال أبحاثي، والموضوع الذي سأتحدث عنه اليوم حول تعديل المحتوى.

والموضوعات التي سوف نغطيها اليوم هي التحديات التي يفرضها تعديل المحتوى، ومخاطر الخصوصية التي يمثلها تعديل المحتوى، وكيف لنا أن نحل هذه المشكلة المعقدة. الشريحة التالية، من فضلك.

وأود أن أقدم لكم لمحة سريعة لتعريفكم بي. أنا طالب في مرحلة التخرج في مجال أمن الفضاء الإلكتروني من جامعة إنديانا، وعلى مدار الشهور القليلة الماضية، كنت أعمل وأقوم بأبحاث حول بضعة موضوعات ذات صلة بحوكمة الإنترنت، والتي تشمل تعديل المحتوى. لذلك يسرني أن أطلعكم على ما لدي من رؤى فيما يخص الموضوع في هذا المنتدى. الشريحة التالية، من فضلك.

بالنسبة للغالبية منكم ممن اعتادوا على الأفكار أو تم توصيلهم بوسائل التواصل الاجتماعي، فقد صادفتم بالتأكيد كلامًا متناثرًا حول تعديل المحتوى. فربما تكونوا قد رأيتم حكومات تحاول كبح المعلومات المضللة، وعلى وجه الخصوص في أوقات الجائحة، وشركات تواصل اجتماعي تحاول كبح تهديدات الانتهاك وباحثون قانونيون يحاولون التوصل إلى سابقة قانونية في التعامل مع تعديل المحتوى، ومجموعات مؤيدة لحقوق الإنسان تثير مخاوف جدية يفرضها تعديل المحتوى على حرية التعبير وأيضًا على الخصوصية. الشريحة التالية، من فضلك.

لقد قمت بعمل إطار زمني مختصر فيما يخص الأحداث ذات الصلة بتعديل المحتوى. واختصارًا للوقت، لن أقوم باستعراض كل واحدة من هذه الأحداث، ولكنني أود ذكر القليل منها لإعطائكم سياق وقرينة حول سبب ارتباط هذا الموضوع وكيف أن هذه مشكلة معقدة للغاية.

على سبيل المثال، في 2021، أي منذ بضعة شهور، حضر معنا جراح الولايات المتحدة العام الذي دافع بانفتاح في محاولة منه لكبح جماح المعلومات المغلوطة في مجال الصحة وأخبرنا أنها تمثل تهديدًا خطيرًا على الصحة العامة، وأن تقييد انتشارها هو بالفعل مسئولية مدنية وأخلاقية. وفي حقيقة الأمر فإن [يتعذر تمييز الصوت] حث شركات التواصل الاجتماعي على [يتعذر تمييز الصوت] من أجل اكتشاف ومنع انتشار المعلومات المغلوطة.

وهناك شيء واحد نريد فهمه هنا وهو أن تعديل المحتوى ليس مشكلة محلية تخص الولايات المتحدة وحدها. بل هي مشكلة عالمية في حقيقة الأمر. ففي الهند في الآونة الأخيرة، مررت الهند سلسلة من قوانين الوسائط الرقمية التي اشترطت على موفري محتوى وسائل التواصل

الاجتماعي بتعديل المحتوى وأيضًا [يتعذر تمييز الصوت] التعقب. وقد قوبل ذلك في حقيقة الأمر بمقاومة عنيفة من شركة WhatsApp التي رفعت شكوى قانونية ردًا على هذا القانون الجديد.

وبالعودة بضعة أسابيع فقط، رأينا موظفًا سابقًا في شركة فيسبوك يقدم شهادة أمام مجلس الشيوخ فيما يخص ممارسات تحسين وتعديل محتوى فيسبوك وتأثيرها على المجتمع. الشريحة التالية، من فضلك.

لذلك إذا ما سألنا أي شخص يعمي في مجال الأمن والخصوصية، فسوف يخبرنا بأن أفضل طريقة ربما تكون موجودة لحل وفهم المشكلة تتمثل في إجراء تقييم للمخاطر. ومن ثم فقد أجريت تقييمًا لمخاطر الخصوصية فيما يخص تعديل المحتوى، وقد استند ذلك إلى معايير الصناعة، أي تصنيف الصناعة الذي وضعه دانيال سولوف الشهير.

على سبيل المثال، لنفترض أننا نشارك معلومات أو نتبادل رسائل من خلال إحدى خدمات الرسائل المشفرة من طرف لطرف مثل برنامج WhatsApp أو Apple Messages. وفي تلك الحالة، وبصفتنا مستخدم يكون لدينا توقع أساسي بالحصول على الخصوصية والسرية فيما يخص ما يجري تبدله من رسائل.

لكن لنفترض أنني -وبصفتي موفر خدمة- أستخدم خوارزمية للكشف عما إن كانت هذه الرسائل ضارة أم لا، وإن كان هذا هو الحال، [يتعذر تمييز الصوت] تعريض هذه المعلومات لأداة وفي تلك الحالة فإنني بشكل من الأشكال أنتهك خصوصية وسرية المستخدمين.

إذن هناك شيء ينبغي علينا فهمه هنا وهو السير حسب التاريخ، فكلما كانت هناك قدرة جديدة يجري تطويرها، فيجب عينا فعليًا ألا نفكر في الكيفية التي يمكننا استخدامهم بها ولكن يجب أن نفكر في الكيفية التي يمكن أن يساء استخدامها بها أيضًا. إذن ومع الأخذ في الاعتبار أن هذه التقنيات الخاصة بالفحص والتدقيق، وعلى وجه الخصوص في نظام مشفر، يمكن استخدامها من خلال الحكومات وأيضًا من خلال [جهات التهديد] الضارة ربما في تعزيز المراقبة واستراق السمع الأمر الذي له تأثيرات بالغة بالنسبة لحرية التعبير عن الرأي في مجتمعنا وهو ما يخلق أيضًا تأثيرًا مخيفًا للغاية.

وثمة أمر إضافية آخر أود أن أطلعكم عليه أيها السادة وهو أن الإفصاح عن المعلومات يمكن عكسه في بعض الأحيان. ولنفترض أنني بصفتي مستخدم فإن تفاصيلي الخاصة مثل توجهاتي

الجنسية وتعاطيً للمواد المخدرة أو الكحول يجري عرضه على النطاق العام. وفي تلك الحالة، لن تكون لدي تلك التدابير اللازمة للحماية من الأزمات الانفعالية الحادة والتأثير العقلي الذي يحدث لي بسبب الإفصاح.

لنفترض أننا نقارن ذلك بحدوث إفصاح عن معلوماتك المالية، فهذه مسالة مختلفة كليًا. ففي تلك الحالي، يمكنك فعليًا حجب بطاقة ائتمانك كإجراء لمنع أي تأثيرات ضارة. لكن هنا في هذه الحالة، وبما أن معلوماتك الصحية يجري كشفها، فلن تكون لديك [يتعذر تمييز الصوت] تلك التدابير. الشريحة التالية، من فضلك.

إذن في الشريحة السابقة، لقد كنت أتحدث حول تهديدات الخصوصية التي يمكن أن تحدث بسبب تعديل المحتوى. لكن على الجانب الآخر، ثمة بعض الافتراضات الجديدة الوجيهة يجري عرضها على الجانب الآخر أيضًا. على سبيل المثال، لنفترض أن بعض الأشخاص يقولون أن تعديل المحتوى يمكن استخدامه من أجل وقف العنف وحتى الوقاية من الموت في النهاية، وعلى وجه الخصوص من حيث العنف الذي حدث في ميانمار.

لذلك فإنني أعتقد بالتأكيد أنه يمكننا اعتماد أسلوب يحافظ على الخصوصية تجاه تعديل المحتوى وهو يقوم على ثلاثة أعمدة أساسية. الأول وهو الجانب الفني والذي ينطوي على التعاون بين المؤسسات الفنية والمؤسسات التعليمية من أجل التعاون للتوصل إلى أساليب تشفيرية آمنة تكتشف أي معلومات مغلوطة أو معلومات مزيفة وفي الوقت ذاته، تضمن خصوصية وسرية مستخدميها.

على سبيل المثال، في هذه الحالة، ربما يمكننا استخدام أسلوب تشفير متعدد الأطراف وآمن يقوم بالبحث عن الصورة ويقارن تلك الصور بمستودع من الصور والتي يتكون منها جميع المدرج في قائمة الانتهاك. فإذا لم تتطابق المعلومات، فلن يتم الإبلاغ عن الصورة إلى موفر الخدمة.

أما العماد الهام الآخر الذي أريد الحديث عنه فهو العملية، وهذا ما أطلق عليه اسم نموذج مراقبة المعلومات. ومن ثم فإنني أود من المستخدمين الإفصاح فعليًا وبمسئولية عن أي نوع من المعلومات المزيفة التي يحصلون عليها إلى موفري الخدمات بحيث يمكننا استحداث نوع ما من نماذج الثقة والمكافحة الاستباقية ضد المعلومات المغلوطة.

أما العماد الأخير الذي سأحدثكم عنه فهو المبدأ، والذي يتمثل في أنه بمجرد إحداث قدر من الثقة بين أصحاب المصلحة—لنأخذ مثالاً على ذلك هناك. إذا كنت أنا أحد موفري الخدمات ولا أتوانى

في تعديل المحتوى، فأعتقد أنه ينبغي عليّ ضمان قدر ما من الشفافية فيما يخص خوارزمياتي لضامن أنني أفوز بثقة جميع أصحاب المصلحة في العملية. الشريحة التالية، من فضلك.

وهذا يحيلني إلى آخر شريحة معي، وأنا أنظر إلى تعديل المحتوى باعتباره مشكلة تشبه إلى حد ما مشكلة التغير المناخي. وتريد العديد من الدول معالجة المشكلة. وكل الدول تقريبًا تريد التعامل مع المشكلة. لكن لديهم طرق مختلفة في التعامل مع المشكلة. وفي معظم الأوقات، لا تسير هذه الأشياء جنبًا إلى جنب في نفس الاتجاه.

ومن ثم فإنني أود إجراء أسلوب متعدد من حيث أصحاب المصلحة من أجل السعي لحل مشكلة تعديل المحتوى مع الأفراد الذين يفصحون بمسئولية عن أي نوع من المعلومات المزيفة إلى موفري الخدمات وبمساعدة المعرفة والأدوات المقدمة من جانب المعلمين والمؤسسات التعليمية. ويجب على المنصات الفنية التعامل مع القصور في تقديم المعلومات وتحديد أولوية الاكتشاف المبكر [لكبار موزعي الأضرار] ومعتادي الانتهاكات بطريقة تحافظ على الخصوصية.

ومن بين أهم أصحاب المصلحة في هذه العملية جميع حكومات العالم معًا والتي ينبغي عليها جمع كل نوع من المنظمات الخاصة غير الربحية والتوصل إلى أرضية مشتركة أو تدابير مشتركة من أجل التوصل إلى التدابير القانونية والتنظيمية المناسبة من أجل التعامل مع مسألة تعديل المحتوى. شكرًا لكم وقتكم وعلى ما أبديتموه من رحابة صدر. وأتطلع إلى الإجابة عن أي أسئلة قد تكون لديكم.

ديبورا إسكاليرا: شكرًا لك، ساي. هل هناك أية أسئلة موجهة إلى ساي؟ حسنًا، لقد واجه المترجمون الفوريون القليل من الصعوبات في هذا الجانب، لكنني أود تذكير الجميع بأن هذه الجلسة يجري تسجيلها ومن ثم سوف تكون لكم القدرة على الاطلاع عليها في غضون أسبوع أو نحو منه. فإذا أراد أي شخص الاطلاع على هذا التسجيل، فإمكانه ذلك.

حسنًا، إينوخ، هل لديك سؤال؟ تفضل رجاءً.

إينوخ نيكنغبونغ ديوت: نعم. شكرًا جزيلاً. لدي سؤال سريع للغاية حول تعديل المحتوى. تعديل المحتوى عبارة عن مشكلة ذات وجهين. فمن جهة، لا نريد إعاقة حرية التعبير وكل تلك الأشياء. ومن جهة أخرى، نريد أيضًا منع المحتوى الذي يجب ألا يكون في النطاق [العام].

ومن ثم هل لدينا حل وسط من شأنه الحد من مخاطر السماح للناس بأن يقولوا أي شيء وفي أي مكان، وفي نفس الوقت مع عدم إعاقة أو تعطيل حرية تعبير الناس عن رأيهم؟ على سبيل المثال، إذا ما نظرنا في الوسائط التقليدية، فإن لدينا منظمين. لكن فيما يخص وسائل التواصل الاجتماعي، هل يمكننا الحصول على منظمين مستقلين يساعدوننا في هذا الشأن؟ شكرًا جزيلاً.

ساي شاندراسيكاران: إينوخ، شكرًا لك على هذا السؤال. للأسف ليس لدينا في الوقت الحالي حل جاهز يوفر بالفعل توازنًا بين التعامل مع المعلومات المغلوطة وحرية التعبير عن الرأي. لكنني أعتقد أن هناك أمر واحد، إذا كنت تشاهد الأخبار مؤخرًا، فربما تكون قد سمعت بالتأكيد عن حادثة الفحص لجانب عملاء أجهزة Apple. أي فيما يخص رغبتهم في إدراء عملية فحص لجانب العميل في جانب المستخدمين من أجل اكتشاف أي نوع من الصور فيما يخص الاعتداء الجنسي على الأطفال وكل ما يخص ذلك، لكن هذا الأمر قوبل بانتقاد مدني من منتقدي الخصوصية وخبراء الأمن أيضًا.

فللأسف ليس لدينا أي شيء في الوقت الحالي، لكنني اقترحت في عرضي التقديمي، لدينا شيء يطلق عليه اسم أسلوب التشفير الآمن متعدد الأطراف وهو الذي يقارن فعليًا تلك الصور بمستودع من صور الاعتداء، وفي حالة تطابق المعلومات فقط، فسوف يقوم بإبلاغ موفر الخدمة. وإلا فلن يتم إرسال معلوماتك إلى موفر الخدمة. لذا أرجو أنني أجبت على سؤالك.

إينوخ نيكنغبونغ ديوت: شكرًا. هلا قمتم بوضع ذلك في مربع الدردشة من أجل المزيد من [يتعذر تمييز الصوت]، رجاء. شكرًا.

ساي شاندراسيكاران: بالتأكيد، إينوخ. شكرًا.

ديبورا إسكاليرا: حسنا. شكرًا على السؤال. هل هناك أي أسئلة أخرى موجهة إلى ساي؟ حسنًا، لننتقل إلى المتحدث التالي، كادي هامر. كادي، الكلمة لك.

كادي هامر: مرحبًا. أنا اسمي كادي هامر وأنا طالب في كلية الحقوق بالجامعة الأمريكية في العاصمة، وسوف أتحدث حول أحد مصطلحات جيل الألفية، ألا وهو حراسة البوابات الإعلامية وذلك بالإشارة إلى بروتوكولات البوابة الحدودية أو غير ذلك المعروفة بأنها آليات أمنية من أجل بروتوكولات البوابة، وعلى وجه الخصوص بروتوكولات البوابة الحدودية. الشريحة التالية، من فضلك.

في البداية أود أن أقدم لكم نظرة عامة مختصرة عن كيفية وصولنا إلى هنا وسبب مناقشتنا لبروتوكولات البوابة الحدودية. ولكي تعلموا جميعًا، فإنني لست متخصصًا في التكنولوجيا، بل أنا طالب حقوق. لذلك فقد استغرقت الكثير من الوقت لفهم الطريقة التي تعمل بها البينة التحتية للإنترنت. ولكن لأنني على يقين من أنكم جميعًا على دراية بذلك، فقد تم إنشاء الإنترنت بالأساس لأغراض الاتصال. ولم يكن الأمن بالضرورة من الشواغل الأولى أو يمثل قلقًا أوليًا عندما قمنا بتطوير البنية التحية للإنترنت. لكن هذا أصبح من المخاوف المتزايدة في عالم اليوم، وعلى وجه الخصوص ونحن ندرس الوجود المتزايد بلا توقف لتهديدات النطاق الإلكتروني والجهات المؤثرة في ذلك المجال.

ففي عام 1989، تم تطوير بروتوكول البوابة الحدودية من بين العديد من البروتوكولات الأخرى. BGP بروتوكول البوابة الحدودية—وهو ما سأشير إليه بلفظ بروتوكول البوابة الحدودية من أجل التبسيط—يعتمد على شبكات الأفراد التي تشارك المعلومات بلا انقطاع بين بعضها الآخر حول روابط البيانات المتاحة، وعناوين IP المتاحة، وهذا هو السبب في قدرة الإنترنت على مواصلة نموه إلى هذه الشبكة العالمية الواسعة حاليًا.

وتجدر الإشارة إلى أمر وهو أن بروتوكول البوابة الحدودية لا يتطلب توثيقًا لعناوين IP أو حتى النظم المستقلة التي تتفاعل معها. بل إن بروتوكول البوابة الحدودية يعمل بموجب ما يطلق عليه اسم إطار عمل الثقة، وربما تعرفون ذلك أيضًا باسم نظام الشرف حيث تثق الشبكات بأن الشبكات الأخرى هي جهات غير ضارة.

وعلى الإجمال رغم ذلك، فقد كان بروتوكول البوابة الحدودية بسيطًا، حيث وفر حلاً لضرورة التوصل إلى بروتوكولات توجيه، وقد وفر هيكلاً متعدد الجوانب بما يكفي لأن يدوم نعنا إلى يومنا الحالي. الشريحة التالية، من فضلك.

وإليكم نظرة عامة عليه، إليكم مخطط توضيحي وأيضًا قائمة ببروتوكولات التوجيه. وكما ذكرت لكم، فإن بروتوكول البوابة الحدودية واحد من بين العديد من بروتوكولات التوجيه. والهدف الأساسي من أي بروتوكول توجيه هو توجيه مرور بيانات الإنترنت بين أنظمة الشبكات الأخرى، أي الأجهزة. وتجدر الإشارة إلى أنه لا يضمن الأمن والسلامة في إيصال وإرسال المعلومات. ومرة أخرى، هذا يعود بنا إلى إطار عمل الثقة أو نظام الشرف.

وكما ترون، فهناك قائمة طويلة بأنواع بروتوكولات التوجيه. ولن أقرأها على مسامعكم. كما أن الرسم البياني الموجود جهة اليمين من الشاشة عبارة عن نظرة عامة على الكيفية التي يعمل بها بروتوكول البوابة الحدودية أو بروتوكول التوجيه الآخر، EGP بروتوكول البوابة الخارجية. ولكم أن تروا كيفية تواصل الشبكات مع بعضها الآخر، ومع النظم المستقلة—وهو ما سأوضحه بعد قليل—ومجرد نظرة عامة بصرية في حال كنتم مهتمين. الشريحة التالية، من فضلك.

وللدخول أكثر في التفاصيل الخاصة ببروتوكول البوابة الحدودية فإنه عبارة عن بروتوكول توجيه لمتجهات المسارات يعمل فيما بين النظم المستقلة على الإنترنت. وبدلاً من الاحتفاظ بالمخطط الكامل للإنترنت، تقوم أجهزة توجيه بروتوكول البوابة الحدودية بترحيل المعلومات من أجهزة التوجيه أو الأنظمة المجاورة والتي تختار بعد ذلك المسار الأقصر طريقًا للتضمين في قائمة التوجيه. يعلن كل جهاز توجيه بعد ذلك عن المسار إلى الجيران الآخرين الذين يطلبون تلك المعلومات. ويقومون بتغيير تلك المعلومات إذا سمحت السياسة بذلك.

ثمة شيء واحد يجب مراعاته هو أنه عندما نتحدث حول النظم المستقلة أو الشبكات التي يستخدمها بروتوكول البوابة الحدودية في التواصل، فقد تسمع أنه قد يشار إليها بلفظ النظام المستقل، وهو ما يشير ضمنًا إلى نظام واحد. وعلى الرغم من ذلك، تشتمل الأنظمة المستقلة في بعض الأحيان على منظمة كاملة، والتي تشمل العديد من أجهزة التوجيه أو الأجهزة. ومن ثم فإن هذا المصطلح يستخدم للحديث باستفاضة أكثر عن بما يوحي بأكثر من المعنى المجرد.

كما أن أرقام النظام المستقل للإنترنت مصممة من خلال موفر خدمة الإنترنت وهي الطريقة التي يستخدم بها المستخدمون كحالنا الإنترنت من أجل التواصل، أو في بعض الأحيان تقوم على تعيينها السجلات.

وفي النهاية، يساعد بروتوكول البوابة الحدودية أجهزة التوجيه على اختيار مسار، وعلى وجه الخصوص المسار الأقصر للحصول على تلك المعلومات، والسبب في الأهمية الكبيرة التي يحظى بها هذا البروتوكول مرة أخرى هو أن الحفاظ على مسار نظام الإنترنت الكامل هو عمل بطولي بحد ذاته. وهو يعتمد على الشبكات المجاورة في تبادل تلك المعلومات بحيث يمكنه إيصالك إلى المعلومات أو الموقع بسرعة أكبر بكثير.

والسبب في أهمية ذلك يرجع إلى الطريقة التي يعمل بها بروتوكول البوابة الحدودية، حيث يمكن استهداف الأنظمة معًا. فبدلاً من الهجوم على جهاز فردي، فإن مرتكب الفعل الضار يمكنه الهجوم على نظام مستقل بالكامل والذي يمكن أن يشمل منظمات وشركات إلخ. الشريحة التالية، من فضلك.

أما الشيء الذي أريد الحديث حوله اليوم والذي يحظى بالأهمية الأكبر هو مشكلات الأمان التي تظهر في البروتوكولات—وشكرًا إلى برايان الذي يقوم بالشرح في مربع الدردشة—ولكن على وجه الخصوص فيما يخص المشكلات الأمنية التي تنشأ في بروتوكول البوابة الحدودية. وعلى الرغم من أن هذه المشكلات الأمنية ليست مقتصرة على بروتوكول البوابة الحدودية، فإنها موجودة بالفعل في بروتوكولات التوجيه الأخرى.

ويعد الخطأ البشري من بين هذه المشكلات الأساسية. ويمكننا إلقاء نظرة على الحادثة المؤسفة في شركة فيسبوك والتي يمكنكم النظر إليها كمثال على ما يمكن أن يحدث، على الرغم من أن مشكلات شركة فيسبوك لم تكن مشكلة تتعلق تمامًا ببروتوكول البوابة الحدودية. إذن قد يؤدي الخطأ البشري إلى سوء تكوين عرضي يمكن فيه تعطيل مؤسسة كاملة أو نظام إنترنت مستقبل أو أن يضيع الاتصال به عبر الإنترنت والتسبب في أعمال تخريبية.

لكن الأمر الأهم الذي أريد الحديث حوله هو التدخل الضار. فقد تكون جميع بروتوكولات التوجيه أهدافًا للهجمات، سواء كان ذلك باستخدام انتحال IP أو اختراق الجلسات أو هجمات رفض الخدمات والعديد من الطرق الأخرى المختلفة التي يمكن للمهاجمين فيها تقديم معلومات غير صحيحة في قوائم بروتوكول البوابة الحدودية.

وأحد الأمثلة على ذلك يمكن أن يحدث بسبب اعتماد بروتوكول البوابة الحدودية على الشبكات المجاورة، فالشبكة المجاورة لك يمكن أن تكون جهة مرتكبة للأعمال الضارة وتقدم لك معلومات غير صحيحة في طلبك بتوجيهك إلى موقع ويب ضار أو أي شيء آخر.

ونظرًا لأن أجهزة التوجيه التي تعمل ببروتوكول البوابة الحدودية تثق في بعضها الآخر، كما أشرتُ لذلك، فليست هناك آليات توثيق حقيقية موجودة في بروتوكول البوابة الحدودية. وليس هناك طريقة يمكن بها توثيقة هوية الغير أو ما تقوله أنظمة الشبكات الأخرى في الوقت الحالي. هل تم توثيقة المعلومات، وإذا ما كانت معتمدة، وإذا ما كانت جديرة بالثقة. ثمة شيء آخر ألا وهو عدم تفويض التوثيق التشفيري. فهذه مسألة أخرى سوف أتطرق إيها في الشريحة التالية.

ولتقريب هذه المسألة، فقد أردت تقديم دراسة حالة حول ما يبدو عليه اختراق بروتوكول البوابة الحدودية وكيف حدث عبر نظام أسماء النطاقات الخاص بشركة Amazon. وفي 2018، استخدم مرتكبو الجرائم هجوم بروتوكول البوابة الحدودية (هجوم "الوسيط") وذلك من أجل إعادة توجيه مرور البيانات إلى خدمة المسار 53 لشركة Amazon من خلال استخدام خادم في مركز بيانات Chicago IBX، بما يتيح للمرتكبين اعتراض مرور البيانات عالميًا.

فعلى وجه الخصوص، استهدف المهاجمون موقع MyEtherWallet.com، وهو عبارة عن منصة لسلسلة كتل Ethereum، وذلك من خلال إعادة توجيه مرور بيانات العملاء إلى صفحة مزيفة أو سطحية قامت بسرقة معلومات عملائهم.

أما عن كيفية قيامهم بذلك فكان من خلال إعادة توجيه مرور بيانات الإنترنت إلى خادم مستضاف في روسيا، والذي تظاهر بأنه صفة ويب MyEtherWallet من خلال استخدام شهادة مزيفة وقام بسرقة العملات الرقمية للعملاء. وقد استلزم الهجوم الوصول إلى أجهزة توجيه بروتوكول البوابة الحدودية الخاصة بموفري خدمة الإنترنت واستلزم موارد محاسبية كبيرة. هذا من الأشياء التي أردت التنويه عنها. ولأنهم قاموا بإعادة توجيه جميع مرور البيانات ذلك، فكان عليهم التعامل مع مرور كبير لبيانات الإنترنت الداخل إلى الخوادم الخاصة بهم.

إذن السبب في أهمية ذلك يرجع إلى أن هذا الهجوم يسلط الضوء على المخاوف الأمنية الحالية في كل من بروتوكول البوابة الحدودية ونظام أسماء النطاقات، والأعم من ذلك في مختلف بروتوكولات التوجيه. وإلى يومنا الحالي، يعد هذا أكبر هجوم معروف من نوعه دمج بين كل من هشاشة بروتوكول البوابة الحدودية ونظام أسماء النطاقات، وهو الموضوع التي تحدث عنه

متحدثون آخرون من برنامج NextGen. ومخطط المعلومات البياني في الأسفل عبارة عن نظرة عامة مبسطة للكيفية التي يمكن أن يحدث بها ذلك. الشريحة التالية، من فضلك.

إذن كيف يمكن حراسة البوابات الإعلامية. على الإجمال، ثمة بضعة أشياء نحتاجها عندما نريد النظر في كيفية جعل بروتوكولات التوجيه أكثر أمانًا، وعلى وجه الخصوص كيفية جعل بروتوكولات البوابة الحدودية أكثر أمانًا.

على الإجمال، نحتاج إلى برامج لأجهزة التوجيه تقوم بتنفيذ IPSEC أي أمن بروتوكولات الإنترنت. ويمكنكم تنفيذ ذلك من خلال البنية التحتية للمفتاح الرئيسي أو التوقيعات الرقمية.

ويجب علينا تحديد الدور الذي تؤديه السجلات الإقليمية في توثيق مسئوليات السلطة—إذن من المسئول—عن سوابق العناوين ورقم النظام المستقبل، لكل من تعيينها وموقعها.

وهناك مكون كبير سوف يكون بمثابة استثمار مالي كبير ألا وهو ترقية البنية التحتية للعتاد والتي تشمل أجهزة التوجيه (موفري خدمة الإنترنت والمشتركين)، من أجل تحديد دور موفري خدمة الإنترنت في توثيق ومعالجة واعتماد هذه المعلومات. وبالطبع، فإن ترقية العتاد المادي يمثل استثمارًا كبيرًا من حيث التكلفة.

وينبغي علينا التفكير على المستوى الاستراتيجي أكثر وبشكل أكثر شمولاً في كيفية تحسين بروتوكول البوابة الحدودية في المستقبل، وعلى وجه الخصوص، ينبغي علينا الإبقاء على أسلوب مرتكز على الأمن في المستقبل، وأتمنى أن يكون ذلك من خلال الإقلال من الاستجابة والإكثار من الاستباقية. كما يجب علينا أيضًا تحديد معايير التقييم، أي كيف نقوم بتقرير وتحديد ما إن كانت شبكة أو جهاز توجيه أو أي شخص أو كيان يعتبر مصدرًا آمنًا أو معتمدًا أو موثوقًا أم لا، وما هي المعايير التي سنستخدمها في السماح بشكل أساسي أو عدم السماح لتلك الشبكات بالتفاعل والعمل في منظومة الإنترنت.

إذن فإن الحلول الثلاثة التي وضعتها على الشاشة، فليس أي منها جديدًا. فالبض منها يعود فعليًا إلى فترة إنشاء بروتوكول البوابة الحدودية، في فترة الثمانينيات أو بداية التسعينيات من القرن الماضي. ومن ثم هناك حلول موجودة فيما يخص الطريقة التي يمكننا بها حماية وتأمين بروتوكولات البوابة الحدودية خصيصًا.

أحد الخيارات يتمثل في تأمين بروتوكول البوابة الحدودية وهو ما يوفر ثلاث آليات نوعية للأمن. الأولى وهي البنية التحتية للمفاتيح العامة. ويمكن استخدام هذه الآلية من أجل توثيق ملكية أي عنوان IP أو حجب عناوين IP.

وهناك خيار آخر في ذلك الحل الأول وهو خاصية المسار الانتقالي. ويمكن استخدامها من أجل حمل التوقيعات الرقمية التي تعمل على توثيق معلومات جهاز التوجيه. فأثناء انتقال هذه المعلومات، يكون هناك رمز أمني موجود بتلك المعلومات. أو كما ذكرت لكم آنفًا، يمكنكم استخدام أمن بروتوكولات الإنترنت IPsec، وهو ما يستخدم بشكل أساسي في توفير البيانات التي تعمل على توثيق المعلومات قبل أن يتم تبادل أية معلومات من خلال بروتوكول البوابة الحدودية.

وهناك آلية أو حل آخر وهو بروتوكول البوابة الحدودية للمنشأ الآمن. وهذا يعود بنا إلى النقطة الثالثة من الحل الأول. فقبل أن يتم تبادل المعلومات، يجب على كل كيان أن يقوم بالتوثيق أو يخضع للتوثيق، ومن ثم يجب توثيق بيانات إثبات الهوية الخاصة به. ويجب توثيق كل شهادة اعتماد. مرة أخرى، فإن هذا الأمر يعود بنا إلى طبيعة الدور الذي تؤديه السجلات، والدور الذي يؤديه موفرو خدمة الإنترنت. فالمعلومات الواردة في هذه الشهادات يجب أن تترابط أيضًا بقاعدة البيانات الأكبر التي من شأنه استضافة هذه الشهادات. مرة أخرى، ما الدور الذي يمكن أن يؤديه السجل أو صحاب المصلحة في الإنترنت في الاحتفاظ بقاعدة البيانات تلك. ومرة أخرى، يجب عليكم التفكير في أمن قاعدة البيانات تلك.

وثمة حل آخر يطلق عليه النقل المرن لبروتوكول البوابة الحدودية وهو يحل محل بروتوكول التحكم بنقل البيانات TCP، وهو بروتوكول توجيه آخر أو بروتوكول نقل ذا ملكية خاصة. وقد لا يكون هذا الحل الخاص هو الأجدى بالنظر إلى أنه يؤدي إلى خصخصة ذلك، لكن من شأنه استخدام أسلوب يطلق عليه الغمر وهو ما يعمل على نقل البيانات من خلال إرسال رسائل اتصال فقط إلى جيرانه بدلاً من الاتصال بجميع الشبكات أو جميع أجهزة التوجيه الموجودة على الشبكة. الشريحة التالية، من فضلك.

من الواضح أن هناك تحديات في بروتوكول البوابة الحدودية الآمن وهذا هو السبب في عدم نجاح الحلول المقترحة والحالية إلى الآن أو السبب في أننا ما زلنا نجري هذه المناقشة. إذن فالتخوف الأولي دائمًا حيال ذلك هو التكلفة الفعلية التي قد تتطلبها هذه الحلول من حيث البنية التحتية وأفراد العمل والتنسيق وتعيين المسئولية. إذن هذه هي المكونات الأساسية لأول حلين.

وقد أتيت بالفعل على ذكر الحل الأخير، لكنه يتطلب التزامًا واسعًا. فإذا كنا ننوي تغيير بروتوكول بأكمله، فهذا يتطلب الكثير من العمل، والجانب الآخر في هذا الأمر أنه سوف يكون ذا ملكية خاصة، أي لن يكون مجانيًا، وقد لا يكون من الممكن الوصول إليه، وفي نهاية المطاف، قد تتحول السلطة أو آلية التحكم إلى المالك.

بالإضافة إلى ذلك وعلى الإجمال، فإن أحد أهم التحديات وجود قناعة على ما يبدو أو عدم اهتمام إلى أن تندلع الأزمة. وقد تحدثت بالفعل حول أسلوب رد الفعل الذي اتخذه غالبية أصحاب المصلحة—وأنا من بينهم أيضًا—تجاه أمننا الخاص، كما أننا نميل إلى وضع الضمادات على الجروح أكثر من تطبيق الحلول الاستباقية.

وبالطبع، إذا ما نظرنا إلى طول مدة وعمر الإنترنت وكم الوقت الذي مضى على وجود الإنترنت، فإن التحلي بالاستباقية أمر شاق فعليًا. وأما الأمر الآخر فهو أن هذه المشكلة ينظر إليها على أنها طفيفة، بالنظر إلى حجم الهجمات الصغير الذي وقع. وقد أشرت إلى أن MyEtherWallet كانت الأكبر من حيث الحجم، على الرغم من أنها استهدفت شركة واحدة، لكن لكم أن تتخيلوا مدى اتساع وقوع هذه الهجمات وما هو مقدار الضرر والإفساد الذي يمكن أن تتسبب فيها إذا كان بروتوكول البوابة الحدودية واحدًا من الأهداف الجديدة لمرتكبي الأعمال الضارة. الشريحة التالية، من فضلك.

إذن فقد تناولت بالفعل غالبية النقاط الموجودة هنا، لكن من بين الأشياء التي أريد تسليط الضوء عليها على الرغم من خطورة هذا الموقف، يمكننا النظر إلى النماذج الحالية حول الطريقة التي يمكننا بها استحداث التزام من جانب أصحاب المصلحة وتغيير الأسلوب الكلي المستخدم في تأمين بروتوكول البوابة الحدودية. وإذا ما نظرنا إلى HTTP وكيف أننا تحولنا من HTTP إلى HTTPS، فسوف نتمكن على الأرجح من حل هذه المشكلة. الشريحة التالية، من فضلك.

وهذا كل ما في الأمر. شكرًا جزيلًا لكم على وقتكم.

ديبورا إسكاليرا: عرض رائع. وشيق للغاية. رائع. حسنًا، إذن فقد كان هناك الكثير من الحوار الجيد الدائر في مربع الدردشة. وبشكل واضح، فهذا موضوع جيد، وموضوع شيق يهتم به الكثير من الناس، هل هناك أية أسئلة موجهة إلى كادي؟ عمل رائع، كادي، عرض جيد وكلام رائع للغاية.

حسنًا، إذا لم تكن هناك أية أسئلة أخرى—يجب أن نضع في اعتبارنا أنه يمكنكم إرسال الأسئلة بعد هذه الجلسة—سوف ننتقل إلى المتحدث التالي، سكوت كيم. سكوت، أنت التالي. شكرًا.

سكوت كيم: شكرًا. مرحبًا بكم جميعًا. أنا اسمي سكوت كيم، وأنا في الوقت الحالي طالب في مرحلة التخرج وأعمل ممارسًا لأمن المعلومات. والدور الذي أقوم به هو جمع المعلومات، وتحليل المعلومات، وتوزيعها إلى أصحاب المصلحة المناسبين. واليوم، سوف أتحدث حول استخدام أداة بحث ICANN من أجل الوصول إلى مؤشرات اختراق. الشريحة التالية، من فضلك.

إذن فإن الأشياء التي سوف أتحدث حولها سوف تكون عبارة عن ملخص لجهات ارتكاب تهديدات APT41، وبعض دراسات حالات الاستخدام، وبعد ذلك في النهاية سوف أختم بتوصية.

إذن فإن APT41 غير معروفة جيدًا بالنسبة للمجتمع، لكنها ذائعة الصيت بالنسبة لممارسي أمن المعلومات. كما أن APT41 معروفة أيضًا باسم آخر لشركة مختلفة، ومن ثم يمكن تسميتها باسم Blackfly وEarth Baku وWicked Panda. علمًا بأن APT41 بالأساس عبارة عن مجموعة تعمل في التهديدات الدائمة والمتطورة برعاية من الحكومة الصينية والتي أجرت حملات لنشر البرمجيات الضارة ذات الصلة بالتجسس ويعود تاريخ ذلك إلى عام 2012. وقد تم ربط هذه المجموعة في الغالب بأهداف الحزب الشيوعي الصيني المبينة في المبادرة الخمسية الثالثة عشرة في الصين لعام 2025. وكان معروفًا أنه يستهدفون شركات ألعاب الفيديو والجهات الفاعلة في مجال الاتصالات السلكية واللاسلكية والقطاعات الأكاديمية مؤخرًا. وقد أعلنت في سبتمبر/أيلول أن وزارة العدل الأمريكية اتهمت عدة أفراد لهم صلة بانتهاكات وأعمال مجموعة APT41. الشريحة التالية، من فضلك.

اكتشف فريق الأبحاث والمعلومات في شركة Blackberry حملة برمجيات ضارة شنتها مجموعة APT41 هذه باستخدام ملفها التعريفي المخصص من أجل إخفاء مرور شبكتها. كما تستخدم APT41 أيضًا برمجيات ضارة مختلفة مثل PlugX وCobalt Strike و[يتعذر تمييز الصوت] وShadowPad وكشفوا البنية التحتية لمجموعة APT41 من خلال أخذ بعض مؤشرات الانتهاك المتداخلة ذات الصلة بحملتين وثقتهما شركات أمن أخرى، وهي Positive Technologies وأيضًا [يتعذر تمييز الصوت]. وكما ترون في النطاقات، فقد

حاولوا التنكر في شكل نطاقات شرعية من مايكروسوفت. بالنسبة لأول ثلاثة، الثلاثة الأخيرة، النطاقات الخمسة أو الستة. الشريحة التالية، من فضلك.

تمنحك أداة البحث عن بيانات التسجيل لدى ICANN القدرة على البحث عن بيانات التسجيل الحالية لأسماء النطاق ومصادر أرقام الإنترنت. ولإجراء هذا البحث، سوف يتعين على المستخدمين الانتقال إلى الموقع WHOIS.icann.org وإدخال أي نطاق. وعلى الأخص بالنسبة لهذا النطاق، فقد اخترت الموقع isbigfish.xyz، وعندما قمت بكتابة النطاق، كانت هذه هي المعلومات التي تلقيتها.

إذن بالبحث عن هذه النطاقات وأرقام IP في مجموعة متنوعة من مستودعات الاستعلام مفتوحة المصدر فقد اكتشفنا بعض الروابط التي تحمل المزيد من التفسير. والنطاق المذكور هناك يخص عنوان IP وهو 107.182.24.93، وهو ما يظهر على مدونة لحملات البرمجيات الضارة من شركة Positive Technologies. لذا فقد كانت لديهم القدرة على ربط النقاط معًا من خلال استخدام هذه المصادر المفتوحة والبحث في عناوين IP هذه، والنطاقات، وما الذي يستخدمونه من حيث الحصول على وصول إلى مختلف البنى التحية والشبكات.

وكما تشاهدون في تواريخ الشهادات، فإنها تدوم فقط لمدة سنة، وهو ما يعد علامة تحذيرية من منظور الممارسين، لأن الجهات التهديدية في الغالب تستخدم هذا النوع من النطاقات المزيفة أو المتروكة في بعض من هذه الأنشطة الضارة. إذن سوف يوفر لنا هذا الكثير من المعلومات. الشريحة التالية، من فضلك.

وختامًا لهذا الكلام، كانت لدى شركة Blackberry القدرة على العثور على هذه المعلومات من خلال ربط مختلف المدونات من مختلف الممارسين والشركات الأمنية التي كانت متاحة بالفعل أمام الجمهور. إذن ففي هذا النوع من السيناريوهات، فإننا نشجع الجمهور فعليًا على مشاركة المعلومات من أجل استحداث صورة أكبر وصورة مكتملة حول التهديدات أو الجهات التهديدية. إذن ومن خلال الجهود الجماعية، يمكننا أيضًا كشف بعض الأنشطة الإجرامية التي تجري في الوقت الحالي. إذا كانت لديكم أية أسئلة، فلا تترددوا في طرحها عليّ. شكرًا.

ديبورا إسكاليرا: شكرًا لك يا سكوت. هل يوجد لدينا أية أسئلة أخرى؟ حسنًا، شكرًا جزيلاً. أحسنت. ومعنا المتحدث الأخير، جيمس بيك. جميس، الكلمة لك. شكرًا.

جيمس بيك: شكرًا جزيلاً لك، ديبورا. أنا اسمي جيمس بيك، والموضوع الذي سنتحدث حوله هو الاستبداد الرقمي، وكيفية مجابهته. الشريحة التالية، من فضلك.

سوف يسأل الكثير منكم نفسه، ما المقصود بالاستبداد الرقمي؟ استنادًا إلى تعريف تم تقديمه لنا، فهو بالأساس استخدام الإنترنت والتقنيات الرقمية ذات الصلة من جانب القادة أصحاب التوجهات الاستبدادية لخفض مستوى الثقة في المؤسسات العامة، وزيادة تأثير الرقابة الاجتماعية والسياسات وتقويض الحريات المدنية. إذن فأي شيء يمكن أن يكون بمثابة انتهاك للخصوصية، وعدوانًا على الحرية العامة وجميع تلك الأشياء التي يمكننا التسليم بها وربما لا ندرك أن الحكومة بإمكانها التحكم فيك في كل جانب [الأساسي في] المجتمع قد تخطر على بالك.

والآن أعتقد أن الكثير من ذلك يتعلق بماهية الأسباب الكامنة وراء الاستبداد الرقمي. حسنًا، قد يكون هو نفس الأمر كما في الحكومات الاستبدادية، سواء كان ذلك على المستوى السياسي أو الاجتماعي أو عدم الاستقرار الاقتصادي، أو تهالك الثقة الجماهيرية في المؤسسات، وزيادة الشرعية والاستقلالية والتحكم أو العبث بالرأي العام. وأعتقد أن هذا العنصر هو الأعم، وهو الخوف. وبالتأكيد، أعتقد أنه في النواحي التي نرى فيها الكثير من الزعر الجماهيري المتزايد حول ما يخفيه المستقبل لنا في مجتمعنا وليست لدينا أي فكرة عنه، فهناك الكثير من عدم اليقين. وبالطبع، فإن الجائحة وكل هذه الأشياء التي تجري في الوقت الحالي هي واحدة من الأسباب الشائعة وراء اعتقادي بوجود الكثير من عدم الثقة المتزايدة والمتنامية لعدم الثقة التي نراها الآن.

وبالطبع، فهذا يشمل عدم الرضا وبالطبع، أنا أعتقد أن لدينا الكثير من الحقوق وأننا لا ندرك من أين تأتي هذه الأشياء. وبالطبع، أعتقد أن هذا الأمر شائع للغاية، ألا وهو القومية والشعبوية، والكثير من الكيانات السياسية بدأت في الوصول إلى التأثير، وهذا هو السبب في أن الاستبداد الرقمي يتحول الآن إلى معيار للواقع في جميع الدول. الشريحة التالية، من فضلك.

ومن ثم أعتقد أننا بدأ في رؤية الكثير من الاتجاهات في هذا الشأن. لنأخذ مثالاً على ذلك وهي الصين والتي دأبت على الكثير من الزيادات المؤكدة في أعمال المراقبة، فالكاميرات في كل

أركان المدينة داخل الصين. لكم أن تحددوا في ذلك أي شيء وأي قطاع وأي زاوية من الشارع الذي تسيرون فيه. وبالتأكيد فقد بدأنا نرى الكثير من كاميرات المراقبة بالدوائر التليفزيونية المغلقة المركبة في كل ناحية وربما تكون [يمكنهم مراقبتك] في كل سلوك قد يخطر على بالكم، سواء كان ذلك القيادة المتهورة أو السلوك الاجتماع غير الدقيق أو أيًا يكن مما قد يخطر على بالكم وربما يمكن اعتباره سلوكاً جامحًا. وتلك هي الأشياء التي بدأنا في ملاحظتها كثيرًا، وهذا هو الحال بالتأكيد. وقد رأينا في هونغ كونغ حيث بدأت الحكومة الصينية في قمع [مواطني هونغ كونغ]. وقد رأينا في مشروع قانون هونغ كونغ لتسليم المطلوبين 2019 بالطبع فيما يخص تمرير قانون الأمن الوطني في الصين. ولا أنوي الخوض في تفاصيل هذا الأمر، لكنني أود إخباركم بأن ثورة التحكم الأخيرة داخل الصين يعود تاريخها إلى ما رأيناه في الثورة الثقافية من فترة خمسينيات القرن الماضي أو في عصر الحرب الباردة. لقد بدأنا نشاهد ظهور الكثير من هذه الأمور في الصين. وبالتأكيد، هل من الممكن أن يحدث ذلك في بلدان أخرى؟ يمكن بالتأكيد. ونحن لا ندري ما يجري—وقد بدأنا بالفعل نشاهد الكثر من نظام الرصيد الاجتماعي.

اسمحوا لي أن أسرد تفاصيل هذا الأمر. ما المقصود بنظام الرصيد الاجتماعي؟ إنه نظام للرصيد الوطني يقوم على تقييمات حول سلوكك الاجتماعي. وكما ذكرت لكم، قد يكون القيادة المتهورة للسيارة أو سوء السلوك أو أيًا يكن مما قد يحدث لك والذي يعتبره الحزب الشيوعي الصيني ليس سلوكاً اجتماعيًا جيدًا. ومن ثم يمكنهم معاقبتك مهما كان السبب وذلك استنادًا إلى تلك التقييمات، وربما سوف تفقد الكثير من الامتيازات مثل الانتقال إلى دول مختلفة. وربما تواجه أيضًا بعض العقوبات الأخرى.

وبالطبع، لقد رأينا حدوث ذلك سابقًا في كوريا الجنوبية أيضًا حيث بدأت هيئة الاستخبارات الوطنية وضع قائمة سوداء بالمشاهير الكوريين بسبب ما لديهم من آراء سياسية. بالإضافة إلى البدء في المشاركة في حرب نفسية من الحكومة السابقة التي شوهدت في السنوات الأخيرة وبدأت في ترهيب مستخدمي الإنترنت. وبالتأكيد، فإننا نشهد الكثير من التزايد في مراقبة ورصد من يزاولون أنشطة مناهضة للدولة، مهما كان ما يعتقدون أنه معارضة لسياسات الحكومة. الشريحة التالية، من فضلك.

وهناك دول أخرى أيضًا، وما نراه في الوقت الحالي في روسيا وبيلاروسيا وفرنسا، فقد بدأنا نشهد الكثير من أعمال المراقبة والرصد. من خلال التلاعب بالانتخابات، أليكسندر لوكاشينكو في روسيا البيضاء وإغلاق الإنترنت الذي حدث مؤخرًا. وفي روسيا، بدأنا نرى التدخل والتأثير

في الانتخابات والتدخل السافر في انتخابات دول أخرى. وتكرر هذا الأمر مرارًا في دول أخرى، وهو ما نراه كثيرًا في التلاعب بالانتخابات، وأعتقد أن هذا من الأشياء التي تسبب قلقًا كبيرًا في مصداقية الانتخابات والانتخاب نفسه ومنظومة التصويت. وربما يكون لذلك أيضًا تأثير على الكثير من أنماط السلوك الاجتماعي وذلك من خلال نشر الدعاية. ونرى أن الأمر يحدث بالمثل في فرنسا، حيث إننا نرى وبشكل أساسي أن قانون الأمن الوطني يمكن أن يعطي صلاحيات مراقبة مطلقة للحكومة الفرنسية في مراقبة أي شخص استنادًا إلى مقدار المضايقات ضد جهات إنفاذ القانون ومحاكمة المواطنين المخالفين للقانون. الشريحة التالية، من فضلك.

كما أن هناك الكثير من الطرق المختلفة لما يمكن اعتباره استبدادًا رقميًا. وبالتأكيد فقد ذكرت لكم المراقبة والرصد. ويشمل ذلك أيضًا التلاعب بالانتخابات والتعامل الوحشي من الشركة، والمعلومات المضللة والمعلومات المغلوطة إضافة إلى الرصد. والشريحة التالية تأتي إضافة إلى ذلك. الشريحة التالية، من فضلك.

وبالطبع، فأن هناك الكثير من ذلك. التعرف على الوجوه والهجوم الإلكتروني والقرصنة. والكثير من هذه الأشياء يعتبر استبدادًا رقميًا لم نفكر فيه بالمرة، لكن تم طرحها في هذا الموضوع الخاص بالاستبداد الرقمي، بما في ذلك التجسس والأخبار المزيفة والتزييف العميق، والتي تقوم بشكل أساسي بالعبث استنادًا إلى الصورة أو مقطع الفيديو الأصلي نفسه ومحاولة التلاعب بنسق مختلف. وقد بدأ ذلك في الشيوع الآن حتى وصل إلى عدم قدرة العديد من المواطنين ومستخدمي الإنترنت العاديين على تحديد ما إن كان ذلك مصدر أصلي أم لا وربما أيضًا يكون لذلك الكثير من الأثر على المجتمع اليومي وعلى كيفية تفسيرنا له. الشريحة التالية، من فضلك.

ما هي التهديدات الناجمة عن ارتفاع مستوى الاستبداد الرقمي؟ من المفهوم على نطاق واسع وبشكل أساسي أن هذا الأمر يقوض الديمقراطية، بما في ذلك المؤسسات أيضًا كما يحتمل أن تعيق أيضًا [الكثير إضافة إلى الجانب الاقتصادي الاجتماعي والسياسي] والثقافة في حد ذاتها في نفس الوقت ويعد انتهاكاً لحقوق الإنسان والحريات المدنية. وهناك أمر آخر—وهو أن هذه مسألة غير شائعة، لكن ربما يمكن أن تؤثر على حقوق المرأة، والتي تشمل زيادة التحرش الجنسي أو غير ذلك من الأضرار التي تلحق البشرية. الشريحة التالية، من فضلك.

إن ضم كل شيء آخر هنا يمكن أن يكون مرتبطًا إضافة إلى طبيعة التهديدات الأخرى. وقد ذكرت لكم بالفعل أن كل هذا يمكن أن يكون نماذج لما يمكن أن تكون عليه تهديدات الاستبداد

الرقمي والتي قد تكون بمثابة عواقب لم تكن في الحسبان في المستقبل القريب. الشريحة التالية، من فضلك.

إذا رأيتم هناك في البيانات الحديثة استنادًا إلى وحدة جمع المعلومات الاقتصادية فيما يخص مؤشر الديموقراطية، فيما يخص الديمقراطية، أعتقد أن هناك الكثير في الوقت الحالي وصول إلى مرحلة أننا في الجائحة وهناك الكثير من الدول والحكومات حول العالم بدأت في استخدام الكثير من الأدوات والكثير من الأعذار حول الكيفية التي يمكن أن نتعامل بها فعليًا وبشكل أساسي من أجل الدخول إلى أعتاب المستقبل حول الكثير التي يمكن أن نجابه بها الجائحة، بما في ذلك الطريقة التي يمكن بها استعادة المؤسسات الديمقراطية والنظام العام.

ونرى أن بلادي، الولايات المتحدة، بدأت في الدخول في أنظمة هجينة، أو بشكل واضح في هذه الحالة، فإننا في نظام ديمقراطي متصدع. وفي الأساس، لقد اعتدنا وضع درجات دائمًا حول الديمقراطيات الكاملة، ولكن بدأنا للأسف في التدهور استنادًا إلى الأحداث الأخيرة التي تتعلق بالأساس بالانتخابات وكل هذه الأشياء التي تجري حاليًا. لكن إذا ما نظرنا إلى الجانب الآخر من العالم، نجد أن الأمر لا يختلف كثيرًا. فالكثير من الدول تدهورت من حيث الديموقراطيات، وهذا الأمر مقلق ويمثل تحذيرًا بأننا إذا لم نقم بأي شيء من أجل مجابهة هذا الاستبداد الرقمي والسماح للحكومات بمضافرة كل الجهود حيث إننا سوف نواصل بشكل أساسي استخدام الكثير من هذه الأدوات في التعامل مع شؤون الحياة اليومية، وربما يكون ذلك من مسببات الأضرار لمجتمعنا ولا نريد أن نرى أي من الشمولية—كما في كوريا الشمالية أو الصين التي بدأنا رؤية ذلك فيها، فربما يقومون بتصدير الكثير من هذه الأشياء، أي كاميرات المراقبة أو أيًا ما يمكن أن يكون، ويتعين علينا التأكد من أننا نضع نهاية لهذا الأمر. الشريحة التالية، من فضلك.

وربما تسألون أنفسكم كيف يمكننا التغلب على هذا، أو التوصل إلى حل. وهناك الكثير من الطرق والوسائل المختلفة. ولكنني أود القول بأن أحد أكبر الأشياء التي سوف يتوجب علينا القيام بها هي تعزيز الديموقراطية وحقوق الإنسان في ديارنا. هذه هي الأولوية الأولى.

وما أود أن تقوم به الولايات المتحدة هو أن تكون نموذجًا يحتذى به في ذلك وبشكل أساسي. وإذا لم نعالج المشكلات الداخلية في بلادنا، فربما لا نتمكن من وضع نموذج في جميع أنحاء العالم الأخرى وربما نحمل الدول الأخرى على أن تقول، "مرحى، ينبغي عليكم اتباع الحقوق المعمول

بها لدينا"، والتأكد بشكل أساسي أنهك بحاجة لدعم وتعزيز حقوق الإنسان وكل شيء للتأكد من أن الجميع لديه الحق في الحرية، ولدعم وتعزيز جميع هذه الحريات.

لكن لسوء الحظ، إذا لم تتمكن الولايات المتحدة من القيام بذلك في الداخل ولم تكن راغبة بشكل أساسي في تحدي هذه المشكلات [يتعذر تمييز الصوت]، فلن يكون هناك سبب للأسف في إمكانية جعلها نموذجًا يحتذى بالنسبة للدول الأخرى حول العالم. ويمكنني قول ذلك بقياس تمثيلي مشابه حيث إننا إذا كنا في مهمة دبلوماسية وكنتم تمثلون الولايات المتحدة أو دول أخرى تمثلونها، فإن الناس على وشك إجراء تقييم أو تكوين مفهوم منكم استنادًا إلى شخصيتكم أو طبيعة ما أنتم عليه. وقد تكون هذه هي نفس الأشياء هنا. ومن ثم، يجب أن يكون لدينا زيادة في مستوى الثقة تجاه المؤسسات العامة، والتي تشمل الحكومات.

وهناك طريقة للقيام بذلك وهي التأكد من تقوية [الكياسة] من أجل منع [عدم الثقة] السياسية والاجتماعية. ويشمل ذلك ما هو معروف بأنه يخفف من التوترات العرقية الموجودة لدينا في الولايات المتحدة ومنع الانقسام داخل البلاد. وهذا من بين أكبر الأشياء التي لا أفضلها على الإطلاق، وبالتأكيد، يجب علينا تعديل ذلك من أجل التأكد من أننا بحاجة إلى توفير مجموعات متكاملة. وأنا أعلم أن هذا من الأشياء الأكثر صعوبة في التنفيذ، لكن يجب ع لينا تقوية الكياسة من أجل التأكد من أن لدينا صفة وشخصية اجتماعية جيدة بالإضافة إلى السلوك اللائق للتمثيل، بما في ذلك الولايات المتحدة من أجل تقوية الحرية على الإنترنت والشمول الرقمي وإمكانية الوصول. الشريحة التالية، من فضلك.

وهذا يشمل نطاقًا كبيرًا من الأشياء. وبشكل أساسي، فإن زيادة البناء على التحالفات متعددة الأطراف التي نراها في الآونة الأخيرة في الولايات المتحدة [يتعذر تمييز الصوت] الحوار الأمني الرباعي، وتحالف العيون الخمسة، مع تقوية ذلك أيضًا. وقد تكون هناك احتمالية بأنه ربما نواجه حلف ناتو آسيوي في المستقبل. لا أدري إلى الآن، لكن [هذا الأمر قيد الحدوث، أي تلك الاحتمالية] فنحن نراها في الوقت الحالي.

بالإضافة إلى الكثير من الاستثمار العام. وبالتأكيد، يتعين علينا الاستثمار في رأس المال البشري. وأنا أعلم بالتأكيد أن الصين ربما تقوم وبشكل واضح بزيادة الاستثمار في رأس المال البشري في الوقت الحالي، وتزيد من المتخصصين في مجال أمن الفضاء الإلكتروني للتأكد من أنهم مستمرون في زيادة ما لديهم من مهارات. لكن في الولايات المتحدة، فإننا نعاني من الكثير من

العجز والقصور في مجال أمن الفضاء الإلكتروني. وإذا لم نحصل على ذلك أو إذا بدأنا في التعرض لحالات العجز والقصور الكبيرة في المهارات في مجال العلوم والتقنية والهندسة والحساب، فسوف نتخلف كثيرًا وربما أيضًا نواجه عواقب غير محمودة. ويشمل هذا الاستثمار في الأبحاث والتطوير. وإذا لم يتم الاستثمار في هذه الأشياء، فسوف نتخلف بالتأكيد عن هذا الركب. وهذا يشكل الكثير من التقنيات الرقمية المختلفة، وتقوية أعمال التشفير.

وفي مجال العامل، فإننا بالتأكيد بحاجة إلى تقوية التنوع والشمول داخل مساحة العمل. وبالتأكيد، فإن المنظمة [يجب علينا المضي قدمًا] والدخول إلى عتبة المستقبل، والتخطيط من أجل ضمان أننا نستعين بأفضل المواهب، بما في ذلك ضمان أننا نتغلب على المرونة في أي أزمة وطنية، كتلك التي رأيناها في الجائحة التي نخوضها في الوقت الحالي، والكثير من الأشياء التي يجب علينا القيام بها من أجل ضمان أننا نواصل الصدارة والريادة في مجال التقنيات. الشريحة التالية، من فضلك.

تلك هي المراجعة والاقتباسات. الشريحة التالية، من فضلك. وهذه نهاية عرضي التقديمي. وأتوجه إليكم بالشكر على الاستماع إلى عرضي التقديمي حول هذه الموضوعات العالمية الشائعة، وأشكر لكم ما بذلتموه من وقت من أجل الاستماع إلى كلمتي. شكرًا جزيلاً. إذا كان لديكم أية استفسارات، فالرجاء عدم التردد في طرحها الآن.

ديبورا إسكاليرا: شكرًا يا جيمس. هناك سؤال من برايان في مربع الدردشة. لقد كان بشكل أساسي، أعتقد، أنه استهدف الجميع، لكن بما أننا نلقي كلمات فاسمح لنا بطرح الأسئلة عليك. ما رأيك في حرية الناس في التعبير عن رأي على الإنترنت خلال جائحة فيروس كورونا المستجد؟

جيمس بيك: برايان، أشكرك على هذا السؤال. لست متأكدًا من نوع السؤال الذي تحاول طرحه. هل يمكنني الحصول على عبارة واضحة حول ذلك.

ديبورا إسكاليرا: برايان، هل لديك أي توضيح حول ذلك؟

جيمس بيك: هل يجب أن أنتظر لكي أسرد لك تفسيري حول ذلك؟

ديبورا إسكاليرا: يمكنك المضي قدمًا وتقديم تفسيرك حول ما يسعى إليه.

جيمس بيك: برايان، أعتقد أن هذا قد يعني الكثير من الأشياء المختلفة استنادًا إلى التفسير [يمكنني الإشارة إلى ذلك]. لكن إن كنت تفكر في ماهية حرية الناس في التعبير عن الرأي على الإنترنت خلال جائحة فيروس كورونا المستجد، كما قلت لك فبالتأكيد فيما يخص العرض التقديمي نفسه، فإن الاستبداد الرقمي في تزايد. والكثير من الحالات التي تحدثت عنها، كالصين وروسيا وبيلاروسيا والكثير من هذه الأشياء—الآن، لا تسئ فهمي، ولا تتوقع أن الولايات المتحدة لديها كل الحريات على الإنترنت وكل تلك الأشياء. وبالتأكيد، هذا الأمر غير صحيح، لأن لدينا بالتأكيد الكثير من الأشياء التي ينبغي القيام بها. وبشكل أساسي، فقد رأينا في إحدى الحالات الحديثة التي وقعت في 2014 مع إدوارد سنودن، بالتأكيد، كان هذا مثال على قيام الحكومة -وبشكل أساسي- بجمع كمية هائلة من البيانات بسبب الأمن العام والتأكد من أننا نحافظ على الأمن الوطني بعد ما رأينها في أعقاب حادثة 9/11.

وفي الوقت الحالي وكما ذكرت لكم، فقد بدأنا في مشاهدة الكثير من الزيادة في السلوك الاستبدادي بالتحكم في مجتمعنا وفي الحريات على الإنترنت والبدء في التعرض للتدهور استنادًا إلى كل الأنواع المختلفة من الأدوات والتقنيات التي رأيناها—كما هو الحال عندما رأينا ذلك في منطقة أفريقيا وفي نيجيريا التي تعرضت لإغلاق عام مؤخرًا، بما في ذلك مناطق أخرى—لست متأكدًا حول ماهية المناطق الإفريقية الأخرى التي تأثرت بذلك. وبالتأكيد فإن هذا الكلام وبشكل أساسي لضمان أن الحكومة يجب ألا تكون لها القدرة على السيطرة على أي نوع من حرية المعلومات على الإنترنت، لأن ما سيحدث هو أننا ربما نشاهد عواقب وخيمة. وإذا كانت الحكومة تحاول السيطرة عليك استنادًا إلى طبيعة سلوكك، مهما كانت بيانات الخوارزميات التي لديهم والتي قد تفهم بأنك صاحب سلوك غير سوي، فربما يكون هذا من الأشياء المقلقة حقًا ويجب ألا تكون للحكومات الحق في التنصت عليك ومراقبتك استندا إلى طبيعة السلوك الذي تقوم به أنت. فهذه

بالأساس حريتك، وحقوقك، وحريتك في التعبير ولك الحق والقدرة على التأكد من الحفاظ على ذلك والتأكد من أن الحكومة لا تتخطى الحدود. فليس من شأنه التأكد من أن—بشكل واضح يجب عليهم عدم التدخل في حياتك الشخصية اليومية.

وكما ذكرت لكم، لا نريد أن نشهد سنوات أخرى من الطغيان والهيمنة، مثلما رأينا من السنوات الماضية، بما في ذلك ما نراه في كوريا الشمالية والصين تسير على هديها. هل نريد رؤية ذلك في بقية العالم؟ أنا لا أريد بالتأكيد رؤية ذلك. فهذا بشكل أساسي عدوان على الخصوصية. وحرية التعبير والحريات المدنية سوف تتعرض للتدهور استنادًا إلى ذلك المفهوم وصولاً إلى وضع غير مقبول.

وبشكل واضح فإنني لا أحبذ ما نراه، فالكثير من الدول تحاول اتخاذ سلوك استبدادي، لكنني أعتقد أن هذا من الأشياء التي يجب الاهتمام بها وجيب علينا الحفاظ على حرية التعبير وجميع الحريات المدنية، لأنه إذا لم نقم بذلك، فسوف نسلم بكل الأشياء ولا يمكننا السماح بحدوث ذلك للتأكد من أن—بشكل واضح أن المستبدين سوف يستحوذون على العالم. ولا نريد حدوث ذلك. ويجب علينا القيام بذلك من خلال التأكد من أننا نستثمر في أنفسنا ويجب علينا زيادة مستوى التعلم وزياد ثقة الجماهير في المؤسسات.

وهذا الأمر صعب المنال في الوقت الحالي في الولايات المتحدة، وفي بقية العالم، لكن يتوجب علينا التأكد من أننا نستمع جيدًا، وأيضًا التأكد من أننا نحترم جميع أنماط السلوك وفق مفهوم الآخرين. وهذا هو السبب في أنني تحدثت حول زيادة الكياسة، والتأكد من أننا بحاجة إلى احترام بعضنا بعضًا. وهذا الأمر يتجاوز الاستبداد الرقمي في حد ذاته، لكنني أعتقد أن الجوانب النفسية وراء سبب وجوب التأكد من أننا نظل محترمين ومنفتحين وأن نتحلى بالصبر والأناة تجاه الآخرين في حين أن لدينا آراء مختلفة. شكرًا جزيلاً.

ديبورا إسكاليرا: حسنا. شكرًا يا جيمس. أعتقد أن برايان قد أوضح السؤال في مربع الدردشة. لم يتبق لدينا إلى دقائق معدودة، ومن ثم سوف أقرأ ذلك عليكم وبعد ذلك سوف أطلب منكم الإيجاز الشديد في توضيحكم لهذا السؤال. يقول، "لقد ذكرت أن الحكومات تتحكم في حرية الشعوب في التعبير عن الرأي على الإنترنت بشكل أكثر خطورة عن ذي قبل. فهل تعتقد أن هذا تطور جيد في عالم ديمقراطي؟"

سوف أتيح لك دقيقتين فقط من أجل الرد على هذا الاستيضاح. شكرًا يا جيمس.

جيمس بيك: كما ذكرت لكم، يحب علينا الاستثمار في رأس المال البشري. وهذا يعني وبشكل أساسي أنه يجب علينا الاستثمار في شعوبنا، والتأكد من أننا نزيد من مستوى المعرفة الفنية. وإذا لم نقم بذلك، فسوف نشهد الكثير من العواقب غير المرغوبة. ويشمل ذلك التطورات الديمقراطية، ويجب أن يكون ذلك بالتأكد من أننا نعزز من ديمقراطيتنا في بلادنا أولاً، والتأكد من أن الدول الأخرى سوف تحذوا حذونا والتأكد من أن لديهم وبشكل واضح الديموقراطيات الخاصة بهم أيضًا.

[ولا أعتقد وبشكل واضح أن الديمقراطية في حد ذاتها] هي أفضل ما هو موجود في العالم. ولا أقول بأنها سيئة، لكنني أقول بذلك إلى النقطة التي يجب فيها أن تتحسن. وهذا بالتأكيد يجب أن يكون من خلال زيادة ثقة الجماهير في التأكد من أننا نثق بالمؤسسات، وعن كيفية القيام بذلك فإنه يجب علينا التأكد من أننا نثق في أنفسنا ونضمن بأننا نقوي من كياستنا في بلادنا. هل هو المجال الذي يجب علينا فيه احترام بعضنا بعضًا.

ديبورا إسكاليرا: حسنا. شكرًا. يبدو أن إينوخ لديه سؤال، وسوف أعطيك دقيقة واحدة للراد على ذلك لأنه يجب علينا ختام الجلسة. إينوخ، ما هو سؤالك؟

إينوخ نيكنغبونغ ديوت: شكرًا جزيلاً. ليس سؤالاً، فقط إضافة إلى السؤال الذي طرح. أعتقد أن من الضروري للغاية الإشارة إلى حقيقة أن عدد من الحكومات قد استغل في حقيقة الأمر حالة جائحة فيروس كورونا المستجد في تمرير قوانين تعطيهم الحق في الاطلاع والحصول على الرسائل والمراسلات الرقمية للشعوب وأن تكون لهم القدرة على استخدام ذلك كذريعة للقمع أو اتخاذ إجراءات، وهو ما يعد أعلى درجات تعديل المحتوى.

والبعض من هذه القوانين لم يقدم جديدًا لأن الجميع كان معارض للتضليل والمعلومات المغلوطة خلال موسم فيروس كورونا المستجد، ولكن هذه القوانين لم يكن مقررًا لها أن تنتهي بنهاية

فيروس كورونا المستجد، لذلك قد نرى حكومات تتناول هذه القوانين التي تم تمريرها خلال جائحة فيروس كورونا المستجد وتستغلها من أجل تقييد حرية الشعوب في التعبير عن الرأي عند انتهاء جائحة فيروس كورونا المستجد. لذلك أعتقد أن هذا من الموضوعات الهامة للغاية ويجب علين دراستها بشكل أعمق. شكرًا جزيلاً.

ديبورا إسكاليرا: شكرًا لك على تعليقك. وبهذا، نختم جلستنا لهذا اليوم. وأريد أن أتوجه للجميع بالشكر على دعمهم لنا وعلى انضمامهم إلينا. وشكرًا إلى سيرانوش على إدارة وتشغيل عرض الشرائح اليوم. وشكرًا لكل المتحدثين على كل العمل الذي قمتم به. لقد قمتم بعمل رائع اليوم، عمل رائع وموضوعات ممتازة وأحسنتم جميعًا في العرض والحديث. أتقدم بالشكر إلى فريق الاجتماعات على دعمه لنا اليوم، وللمترجمين الفوريين. فلم يكن لنا أن نقوم بذلك من دونكم. وشكرًا جزيلاً لكل من حضر اليوم وقدم الدعم للحاضرين من برنامج NextGen للجيل التالي في ICANN72. ونحن سعداء للغاية بأنكم هنا معنًا. وإلى المشاركين في برنامج NextGen، استمتعوا باجتماع ICANN72. فلدينا الكثير من العمل المخطط له هذا الأسبوع. أعلم أنه قد يكون مليئًا بالمصطلحات والمختصرات وكل شيء، لكن على رسلكم واستمتعوا بوقتكم. وأشكركم جميعًا على وجودكم بيننا اليوم. وهذا كل شيء. أتمنى لكم يومًا رائعًا.

**[نهاية التدوين النصي]**