حوكمة الإنترنت (2): الحوكمة باستخدام البنية التحتية

يوليو 25, 2022

الموارد الحرجة للإنترنت

الموارد الحرجة للإنترنت (Internet Critical Resources ICRs) قد تكون الساحة الأكثر أهمية في الصراع حول حوكمة الإنترنت. لتقدير أهمية الموارد الحرجة للإنترنت،

ومن ثم لفهم أسباب الصراعات الشرسة حول حوكمتها دعنا أولًا نقدم فكرة واضحة عما نعنيه بهذا المصطلح. (See chapter two in DeNardis 2014; chapter ten in Mueller 2010)

يشير مصطلح الموارد عادة إلى مخزون ملموس من المواد الخام أو المصنوعات الضرورية لواحد أو أكثر من احتياجات البشر أو العمليات والوظائف الضرورية للمجتمعات البشرية. المياه، البترول، الغاز الطبيعي، الذهب والمعادن النادرة الأخرى، السلع الوسيطة التي تدخل في تصنيع سلع أخرى، مثل الدقيق المنتّج من القمح والذي يدخل في صناعة الخبز، وغير ذلك. تلك هي الأشياء التي ترد إلى أذهاننا عندما نلتقي بمصطلح الموارد. في المقابل، الموارد الحرجة للإنترنت والضرورية لعملها هي في الحقيقة افتراضية وغير ملموسة. لنأخذ عناوين الإنترنت كمثال. هذه العناوين ليست إلا أرقام لا معنى لها في حد ذاتها، مثل أرقام الهاتف. ما يمنح عناوين الإنترنت معناها هو مجموعة من الافتراضات المتفق عليها، ولذلك هي موارد افتراضية. وهي بالطبع غير ملموسة، فلا يمكنك أن تلمس رقما أو تمسك به أو تضعه في صندوق.

لا ينبغي أن يكون ذلك مفاجئا بالطبع إذا ما تذكرنا أن الإنترنت نفسها، ليس لها وجود مادي ملموس، بل إن وجودها نفسه افتراضي. لا يوجد كيان مادي يمكننا أن نلمسه بأيدينا أو أن نذهب إليه يسمى بالإنترنت. نحن نتوافق على مجموعة من القواعد والتقنيات التي تخلق هذا الشيء الذي نسميه بالإنترنت. ولكن كون موارد الإنترنت افتراضية لا يجعلها أقل أهمية من أي مورد مادي، والأهم من ذلك لا يعني أن القبول بها هو أمر طوعي. ما يعنينا بخصوص أن الموارد الحرجة للإنترنت افتراضية وغير مادية هو أن ذلك يجعل بالإمكان الصراع حول إدارتها بطرق تختلف عن الصراع حول إدارة الموارد المادية. على وجه التحديد، يدور الصراع حول موارد الإنترنت حول الطريقة الفنية لتطبيقها، كمثال كيف يتم تعريف عناوين الإنترنت؟ ما هي احتياطات الأمن المتضمنة في بروتوكولات الإنترنت، ومن يحق له تصميم هذه البروتوكولات؟ من الذي يمكنه توزيع عناوين الإنترنت على من يحتاجونها؟ وبأي شروط؟

الملمح الأساسي الثاني للموارد الحرجة للإنترنت هو أنها مختصة بالإنترنت وحدها، أي ان لها قيمة فقط في سياق عمل واستخدام الشبكة. بعض الموارد الافتراضية أيضا مثل الطيف

الترددي لموجات الراديو، وهي ضرورية للاتصالات العالمية، وفي حين أنها تؤثر في الشبكات التي تستخدم في نقل حزم بيانات الإنترنت، إلا أنه لا يمكننا أن نعدها من الموارد الحرجة للإنترنت، حيث إن عمل الإنترنت لا يعتمد عليها. ذلك يعني أن الأدوات التقليدية التي تستخدمها الدول وغيرها من الأطراف للتحكم في الموارد المختلفة لا تتيح تأثيرا حاسما على موارد الإنترنت الخاصة بها وحدها. بعض الدول والفاعلين الآخرين يملكون نفوذا كبيرا نتيجة لقدرتهم على التحكم في بعض الموارد الهامة عالميا، الأقرب للتأثير على الإنترنت على سبيل المثال الكابلات البحرية التي تنقل الاتصالات بعيدة المدى بين الدول والتي تمر بنقاط تجمع تفرضها طبيعة البحار، وبعض أهم هذه النقاط تقع تحت سيطرة دول بعينها لوجودها في مياهها الإقليمية. ولكن الكابلات البحرية مع أهميتها البالغة، إلا أن استمرار الإنترنت عالميا لا يعتمد عليها بشكل كامل، فثمة دائما بدائل لنقل بيانات الإنترنت، وحتى إذا أدى عطب أحد الكابلات الرئيسية إلى توقف خدمة الإنترنت عن غالبية المستخدمين في قارات بأكملها، فهذا لن يعني توقف الإنترنت عن العمل. في المحصلة وحدها الموارد الحرجة للإنترنت هي تلك التي يمكن من خلالها التحكم فيها، وبالتالي فلا مجال للتحكم في الإنترنت إلا بالسيطرة على هذه الموارد دون غيرها.

أخيرا، الموارد الحرجة للإنترنت عالمية بطبيعتها، وبالتالي لا يمكن إدارتها محليا داخل أي دولة بشكل مستقل عن بقية الدول. هذا أيضا يعني أن من الضروري أن تكون هذه الموارد فريدة عالميا؛ لا يمكن أن يشير عنوان على الإنترنت إلا إلى جهاز واحد وواحد فقط من بين كل الأجهزة المتصلة بها في نفس اللحظة. ومن ثم فتوزيع موارد الإنترنت ينبغي إدارته بشكل مركزي، وهو ما يعني أن جهة واحدة فقط في العالم كله يمكن أن تقوم بتوزيع هذه الموارد بين من يحتاجونها لضمان عدم التعارض فيما بينها. أخيرا يعني ذلك أيضا يعني أن هذه الموارد متناهية، ثمة دائما حد أقصى لما هو متاح منها في أي وقت، ولرفع هذه الحد الأقصى لابد من أن تكون الحلول واحدة ويلتزم بها الجميع، وبالتالي مرة أخرى ستكون هناك جهة واحدة يؤول إليها وحدها القرار النهائي حول أي الحلول يمكن تنفيذه. هذا يفسر كثيرا من التجاذب حول حوكمة هذه الموارد، نتيجة لأن تاريخ الحوكمة المركزية لها لا يزال يلقي بظلاله على الحاضر، مما يجعل كثيرا من الفاعلين غير مرتاحين بأي حال للوضع القائم.

أسماء وأرقام الإنترنت

الموارد الأكثر أهمية للإنترنت والتي تشكل بنيتها التحتية ومن ثم لا يمكن في الواقع لأحد أن يصل إلى الإنترنت دونها، هي أسمائها وأرقامها الأساسية. تحديدا ثلاثة أنواع من هذه الموارد، عناوين بروتوكول الإنترنت (IP addresses)، أسماء النطاقات (Domain Names)، وأرقام النظم المستقلة (Autonomous System Numbers). الأول والثاني كانا ضروريين للإنترنت منذ بداياتها المبكرة، عندما كانت لا تزال تعتبر ظاهرة أمريكية. والثالث أصبح ضروريا عندما حققت الإنترنت الغرض من تصميمها لتصبح شبكة عالمية للشبكات.

عناوين بروتوكول الإنترنت *IP Addresses*

حتى يمكن لأي جهاز أن يتصل بالإنترنت، ويتبادل البيانات مع بقية الأجهزة المتصلة بها، لابد أن يكون له عنوان فريد، إما دائم/ثابت أو مؤقت/متغير. عناوين الإنترنت هي أرقام، ولكن في حين أنه في الرياضيات يمكن للأرقام أن تستمر في الزيادة إلى مالا نهاية، فإن الأرقام التي يمكن للحواسيب التعامل معها محدودة بالطريقة التي يتم بها تخزينها. بالنسبة للحاسوب كل شيء هو عبارة عن سلسلة من الوحدات المتناهية الصغر. بلغة الأرقام تأخذ هذه الوحدات أحد قيمتين، إما 1 أو 0. ولذلك فنظام العد الأساسي للحاسوب هو النظام الثنائي وليس نظام العد العشري الذي نعتاد التعامل معه في حياتنا اليومية، والذي يمكن للوحدات فيها أن تأخذ واحدة من بين عشر قيم مختلفة هي 0، 1، 2، ... وحتى 9. تسمى الوحدة المتناهية الصغر التي يتعامل معها الحاسوب "بت" (Bit)، وحتى يمكن التعبير عن أي بيانات ذات معنى يتم تجميع هذه الوحدات الصغرى في وحدات أكبر تسمى كل منها "بايت" (Byte). ويتكون كل بايت من 8 بت. للتعبير عن أي رقم يجب استخدام عدد محدد ومعروف مسبقا من وحدات البايت، لأن الحاسوب لا يمكنه أن يخمن أين يبدأ رقم ما وأين ينتهي، ولكن يمكنه فقط أن يتعامل مع عدد محدد من الوحدات على أنها تمثل رقما ما.
وحتى يمكن للحواسيب تبادل البيانات فيجب أن يكون عدد الوحدات المستخدمة لتخزين أي نوع من البيانات قياسيا وواحدا بين الحواسيب كلها. ولذلك فعناوين الإنترنت لها عدد محدد من وحدات التخزين، والحد الأقصى لها محدود بأعلى رقم يمكن لوحدات التخزين هذه أن تعبر عنه.

لماذا لعناوين الإنترنت حد أقصى لا يمكن تخطيه؟

في البدايات المبكرة، استخدم عدد محدود من الوحدات الرقمية لتخزين عناوين الإنترنت، ولذا كان ثمة فقط عددا محدودا من الأجهزة التي بمكن أن تتصل بالإنترنت. ومنذ عام 1972 وحتى عام 1981، كانت عناوين الإنترنت تخزن في 8 وحدات رقمية صغرى، وهذا سمح فقط بوجود 256 رقم تعريفي فريد ومختلف عن غيره، مما يعني أن 256 جهازا فقط كان يمكنها الوصول إلى الإنترنت في أي لحظة بعينها. ومع تقديم الإصدار 4 من بروتوكول الإنترنت IPv4، تم إطالة العناوين إلى 32 وحدة رقمية، مما سمح بوجود حوالي 4.3 مليار رقم تعريفي فريد. وهذا يعني أن حوال 4.3 مليار جهاز يمكن أن تتصل بالإنترنت في نفس الوقت. وفي وقت هذه التوسعة كان يُظن أن هذا العدد من الأرقام التعريفية سيكون كافيا، ولكن الإنترنت توسعت بسرعة بالغة وتخطت الحدود التي فرضها طول عناوين الإنترنت. وأدى هذا إلى إنشاء الإصدار 6 من بروتوكول الإنترنت IPv6، الذي يتيح عددا هائلا من الأرقام التعريفية الفريدة بإطالة العنوان إلى 128 وحدة رقمية صغرى (2^128 أي حوالي 340 أنديكيليون رقم مختلف).

عناوين بروتوكول الإنترنت عالمية، أي أن أي حاسوبين متصلين بالإنترنت لا يمكن أن يكون لهما نفس العنوان في نفس الوقت، وإلا فلن يمكن لحاسوب ثالث أن يعرف إلى أي منهما سيرسل البيانات التي طلبها. بالتالي يجب إدارة عناوين الإنترنت بشكل مركزي، وأن تشرف عليها سلطة واحدة. وفي الوضع الحالي يتم توزيع عناوين الإنترنت من خلال نظام توجد على قمته توجد مؤسسة هي "سلطة الأرقام المخصصة للإنترنت" (Internet Assigned Numbers Authority – IANA)، وهذه المؤسسة تعمل الآن تحت إشراف "شركة الإنترنت للأسماء والأرقام المخصصة" (Internet Corporation for Assigned Names and Numbers – ICANN). توزع IANA مجموعات من عناوين الإنترنت على خمس "سجلات إقليمية للإنترنت" (Regional Internet Registries – RIRs)، وهذه بدورها تقوم بتوزيع مجموعات من عناوين الإنترنت من بين تلك التي يملكها كل منها على "سجلات الإنترنت المحلية" (Local Internet Registries – LIRs)، و"سجلات الإنترنت الوطنية" (National Internet Registries – NIRs)، أي لكل بلد. هؤلاء هم من يوزعون عناوين الإنترنت على "مقدمي خدمة الإنترنت" (Internet Service Providers – ISPs)، الذين يخصصون عناوين الإنترنت لعملائهم، إما بشكل ثابت دائم، أو بشكل متغير مؤقت، لكل عميل.

على الرغم من المزايا الكبيرة لعناوين بروتوكول الإنترنت الجديد IPv6، وحقيقة أن IANA قد أعلنت بالفعل في فبراير عام 2011 أنه لم يعد لديها مجموعات من عناوين IPv4 متاحة لتوزيعها على سجلات الإنترنت الإقليمية، فالانتقال من IPv4 إلى IPv6 قد أثبت كونه تحديا كبيرا. أسباب ذلك منها عدم وجود وعي كاف حول الحاجة إلى هذا الانتقال، ومحدودية توافر الموارد المالية الضرورية للاستثمار في التجهيزات التقنية خاصة في الدول النامية. مشكلة نفاد عناوين الإنترنت، هي واحدة من الاهتمامات الأساسية لحوكمة الإنترنت، حيث إنها تعوق مزيدا من تطور الإنترنت. وقد تواجه الدول النامية بصفة خاصة مشاكل في ملاحقة التطبيقات الجديدة للإنترنت، خاصة "إنترنت الأشياء" (Internet of Things – IoT)، التي تتطلب توسعا كبيرا لعناوين الإنترنت. هذا قد ينعكس على المستخدمين الذين قد يضطرون إلى دفع المزيد في مقابل الوصول إلى الإنترنت في الوقت الذي ستصبح فيه عناوين الإنترنت اللازمة لذلك أكثر ندرة.

نظام أسماء النطاقات *DNS*

في حين تستخدم عناوين الإنترنت لأي جهاز متصل بالإنترنت، حتى يميز كل منها الآخر على الشبكة، فيمكنها التواصل وتبادل البيانات، فبعض الحواسيب بشكل خاص، عادة الخوادم، التي تقدم المحتوى والخدمات التي يستهلكها المستخدمون، تحتاج أن يكون لها أسماء يمكن للبشر استخدامها. هذا يمكن تحقيقه بتخصيص أسماء مقروءة باللغات الطبيعية مثل الإنجليزية، لهذه الخوادم. هذا يتطلب قبل أي شيء طريقة لترجمة هذه الأسماء إلى عناوين الإنترنت (IP addresses) التي تميز كل جهاز أو خادم متصل بالشبكة. حيث إن عناوين الإنترنت فريدة، فكذلك يجب أن تكون الأسماء القابلة للترجمة إليها. ولكن في حين أن عناوين الإنترنت هي ارقام، والتي مهما كانت محدودة بطولها فبالإمكان أن يكون ثمة عدد ضخم منها، فالأسماء محدودة أكثر بكثير بسبب محدودية الكلمات ذات المعنى في أي لغة. لذا كان لابد لنظام أسماء النطاقات الذي اخترع لهذا الغرض أن يكون هرميا.

يتكون نظام أسماء النطاقات حاليا من "خوادم الأصل" (Root name servers)، وخوادم نطاقات المستوى الأعلى (top-level domains – TLDs)، وعدد ضخم من خوادم أسماء النطاقات (Name Servers) موزعة حول العالم. ثمة نوعان رئيسيان من نطاقات المستوى الأعلى، النطاقات العامة (generic TLDs – gTLDs)، مثل com،

وorg، وnet؛ و"نطاقات أكواد البلدان" (ccTLDS – country code TLDs)، مثل us، uk، وeg.

يحتفظ كل من خوادم الأصل بعناوين الإنترنت لخوادم أسماء نطاقات المستوى الأعلى، التي يدير كل منها سجل لأسماء الإنترنت (Registry) ويختص بأحد النطاقات العامة، أو نطاقات أكواد البلدان، ويقوم كل من هؤلاء بحفظ وإدارة قاعدة بيانات لكل الأسماء المسجلة تحت النطاق الخاص به. السجلات هي شركات أو منظمات أو ربما مؤسسات حكومية، ويمكن أيضا أن يقوم أحدها ببيع وتسجيل أسماء النطاقات، ولكن المعتاد أن يقوم بذلك جهات متخصصة هي "المسجلين" (Kurbalija 2016, p. 46). (registrars) على قمة هذا النظام بكامله توجد شركة الإنترنت للأسماء والأرقام المخصصة ICANN، التي تنشئ أي نطاق عام جديد وتضع القواعد للسجلات. أما القواعد المتعلقة بنطاقات أكواد البلدان فتضعها الحكومات ذات الصلة، أو أي جهة تعهد إليها هذه الحكومات بالمهمة.

منذ البدايات المبكرة للإنترنت التجاري، كانت أسماء النطاقات موضع خلافات متجددة. المشكلة الأولى كانت العلامات التجارية. في تلك الأيام كان تسجيل أسماء النطاقات مبني على الأسبقية، بمعنى أن أول من يتقدم لتسجيل اسم نطاق بعينه يتم تخصيص الاسم له. خلق ذلك مشكلة التعدي على النطاقات، حيث يتسابق البعض عمدا لتسجيل أسماء نطاقات تحت مسميات لعلامات تجارية مشهورة لشركات أو منظمات أو مؤسسات، بنية أعادة بيع حق استخدام هذه النطاقات إلى الملاك الأصليين للعلامة التجارية مقابل أثمان باهظة. أدى هذا إلى عديد من النزاعات في المحاكمة، والتي لم يكن من السهل تسويتها لعدم وجود تشريعات ذات علاقة. حل هذه المشكلة أخذ وقتا طويلا لتطويره من قبل ICANN، بالتعاون مع المنظمة العالمية لحقوق الملكية الفكرية (WIPO). معا طور الطرفان "السياسة الموحدة لتسوية النزاعات" (Uniform Domain-Name Dispute-Resolution Policy) والتي تضع قواعد تحديد لمن يتم تسجيل أسماء النطاقات المتنازع عليها.

مجال آخر للصراع المتكرر أيضا هي إنشاء أسماء نطاقات مستوى أعلى عامة جديدة. تقديم مثل هذه النطاقات يعني ان الملاك المعنيين لأي أسماء تجارية سيكون عليهم تسجيل نطاقات جديدة باسم علاماتهم التجارية تحت نطاقات المستوى الأعلى الجديدة. على الجانب

الآخر توسع الإنترنت وتنوع استخداماتها يتطلب توسيع نظام أسماء النطاقات بصفة عامة والذي لا يمكن تحقيقه إلا بإضافة نطاقات مستوى أعلى عامة حيث إن نطاقات أكواد البلدان محدودة بالعدد الموجود بالفعل منها وعادة تكون قواعد التسجيل تحتها أكثر بيروقراطية مما يجعل النطاقات العامة مفضلة أكثر.

إدارة نطاقات أكواد البلدان هو أحد المجالات حيث تتقاطع السياسة مع حوكمة الإنترنت بشكل واضح، على مستوى البنية التحتية. سؤال هو كيف يمكن التعامل مع الكيانات ذات الوضع المتنازع عليه في مناطق الصراع. أحد الأمثلة على قضية خلافية ذات صلة كان ما إذا يمكن تخصيص اسم نطاق خاص بالسلطة الفلسطينية، حيث إن فلسطين ليست دولة معترف بوجودها رسميا بعد. ولكن IANA خصصت النطاق "ps" للسلطة الفلسطينية بناء عل قاعدة تخصيص نطاقات أكواد الدول حسب القواعد القياسية العالمية ISO 3166 لأكواد الدول، وهو مبدأ أرساه أولا جون بوستل الذي أدار وظائف IANA طوال 30 عاما حتى 1998. (Kurbalija 2016, p. 48)

الحوكمة باستخدام البنية التحتية للإنترنت

في ورقة بحثية مهمة بعنوان "الروافع الخفية للسيطرة على الإنترنت: نظرية لحوكمة الإنترنت قائمة على البنية التحتية"، (DeNardis 2012) استخدمت لورا ديناردیس Laura DeNardis مصطلح "التوجه إلى البنية التحتية في حوكمة الإنترنت"، لتصف اتجاها سائدا يستغل فيه فاعلون مختلفون "نظم البنية التحتية للإنترنت –مثل نظام تسمية النطاقات– لأغراض [سياسية واقتصادية] مختلفة عن تلك التي صممت هذه النظم لتحقيقها." (DeNardis and Musiani 2016) بالتعاون مع باحثين آخرين، طورت ديناردیس هذه الفكرة أكثر في كتاب بعنوان "التوجه إلى البنية التحتية في حوكمة الإنترنت" (Musiani et al, 2016). واليوم، هذا المصطلح والقضايا المختلفة التي يشير إليها هي أكثر اتصالا بالواقع، حيث إن استخدام الحكومات وشركات التقنية الكبرى للبنية التحتية للإنترنت لأغراض سياسية واقتصادية قد ازداد من حيث تنوع صوره ومعدلات تطبيقه، بحيث اجتذب اهتمام الإعلام السائد والجمهور العام.

في حين ناقش الجزء السابق من هذه السلسلة الموارد الحرجة للإنترنت، وهي أحد فروع البنية التحتية للإنترنت، يوسع هذا الجزء نطاق تركيزه ليتعامل مع قضايا مختلفة على صلة بالموارد الحرجة للإنترنت وكذلك جوانب أخرى للبنية التحتية لها. فكرة "التوجه إلى البنية التحتية في حوكمة الإنترنت،" تقدم عدسة مناسبة لرؤية هذه القضايا من خلالها. وثمة مفهوم آخر قد يساعد كمدخل لهذه المناقشة هو "حيادية الشبكة"، وهو مبدأ أن كل حزم البيانات تنشأ متساوية، ومن ثم ينبغي معاملتها بشكل متساو. انتهاك مقدمي خدمات الإنترنت لهذا المبدأ بذرائع عملية مختلفة يفتح الباب أمام صور عديدة لاستغلال البنية التحتية للإنترنت لأغراض سياسية واقتصادية.

حوكمة البنية التحتية للإنترنت في مقابل الحوكمة باستخدامها

تعتمد الإنترنت على عدد كبير من الموارد المادية والافتراضية التي يمكن تقسيمها بين ثلاث طبقات هي: الطبقة المادية (Physical Layer)، طبقة النقل (Transport Layer)، وطبقة التطبيقات (Application Layer). (Kurbalija 2016, p. 35) الطبقة الأولى في الواقع تضم البنية التحتية للاتصالات السلكية واللاسلكية التي تعتمد الإنترنت عليها لنقل البيانات بين أنواع مختلفة من الأجهزة التي يمكن أن تتصل بها. تلك مع ذلك ليست مختصة بالإنترنت وحدها ومن ثم لا مكان لها في هذه المناقشة. الطبقة الثانية تضم بروتوكولات الإنترنت وقواعدها القياسية مثل بروتوكول التحكم في نقل البيانات وبروتوكول الإنترنت (TCP/IP)، نظام أسماء النطاقات (DNS)، الوب (WWW)، إلخ. وأخيرا تضم الطبقة الثالثة التطبيقات العاملة على الإنترنت لتقدم خدمات مختلفة لمستخدميها. هاتان الطبقتان مختصتان بالإنترنت، وينتميان إلى بنيتها التحتية لأن كلا منهما تخلق نقاط تحكم في تدفق البيانات خلال الشبكة. نقاط التحكم هذه هي التي يتم عندها تطبيق سياسات حوكمة البنية التحتية للإنترنت.

في الجزء السابق ركزنا على قضايا تتعلق بإدارة الموارد النادرة للإنترنت، وهي تحديدا عناوين الإنترنت، وأسماء النطاقات. بعض هذه القضايا كان لها طبيعة سياسية، مثل تحديد أي جهة هي المؤهلة لمكانة الدولة بحيث يمكن تخصيص اسم نطاق على المستوى الأعلى برمز هذه الدولة لها. ولكن هذا ينتمي إلى ما يمكننا تسميته بسياسة حوكمة البنية التحتية

للإنترنت، أي السياسة التي تتورط عرضا في الوظائف اليومية لحوكمة البنية التحتية للإنترنت.

ما سنركز عليه في هذا الجزء هو استغلال أدوات حوكمة البنية التحتية للإنترنت في سياق نزاع سياسي، ثقافي أو اقتصادي. ملاحظة الفرق بين الأمرين قد تكون أمرا مراوغا في حالات كثيرة. على سبيل المثال، عندما أعلنت شركة الإنترنت للأسماء والأرقام المخصصة (Internet Corporation for Assigned Names and Numbers – ICANN) توسعا كبيرا للنطاقات العامة على المستوى الأعلى (Global Top-Level Domains – gTLDs)، اعترضت بعض الدول على إنشاء أسماء نطاقات جديدة مثل (gay، sexy، porn، islam)، على أساس دعاوى تمثيل ثقافية، أخلاقية أو هوياتية. كيف تختلف هذه الحالة عن حالة تخصيص نطاق من المستوى الأعلى لجهة تمثل دولة؟ ببساطة، في حالة تخصيص نطاق لدولة لم تحتج ICANN لتسوية النزاع حول وضع الجهة بنفسها، ولكنها فقط استخدمت القواعد القياسية المتفق عليها دوليا لتخصيص أكواد الدول. بعبارة أخرى لم يستخدم أداء ICANN لإحدى وظائف حوكمة كأداة في نزاع سياسي. في الحالة الأخرى، ليس ثمة قواعد قياسية متفق عليها دوليا لتسوية هذه النزاعات الثقافية، الأخلاقية أو الهوياتية. أيا ما كان القرار الذي تتخذه ICANN في هذه الحالة سيعني استخدام وظيفة حوكمة الإنترنت المخول لها أداءها لترجيح كفة أحد أطراف النزاع على الآخر. وهذا ما ندعوه بالحوكمة باستخدام البنية التحتية للإنترنت.

الحوكمة باستخدام بروتوكولات الإنترنت

بروتوكول الإنترنت الأكثر أهمية، أي الـ TCP/IP صمم كوسيلة لنقل البيانات بين طرفين. وهو يعمل بأعلى كفاءة له عندما تعامل حزم البيانات على أنها كذلك فقط، بمعنى كحزم مصمتة من البيانات الرقمية. فنيا، ليس ثمة حاجة لفحص المحتوى الفعلي لهذه الحزم، ومن ثم فمبدأ حيادية الشبكة متضمن في بروتوكول الإنترنت لنقل البيانات. وأي حاجة إلى انتهاك هذا المبدأ بمكن فقط أن تنشأ لتحقيق أهداف بخلاف وظيفة هذا البروتوكول.

في عام 2003، اخترعت تقنية الفحص العميق لحزم البيانات (DPI)، الغرض من التقنية في البداية كان عزل المحتوى الخبيث (الفيروسات بأنواعها)، ولكن تقنية الفحص العميق استخدمت منذ ذلك الحين في أغراض سياسية واقتصادية عديدة. (Wagner 2009) يستخدم مقدمو خدمات الإنترنت التقنية للتفرقة بين الأنواع المختلفة من المحتوى لغرض معلن هو ضبط تدفق البيانات على الشبكة، وتحسين الأداء. المحتوى الذي يتطلب سرعة أكبر لأداء أفضل، على سبيل المثال بث الفيديو، يُعطى أولوية على أنواع أخرى من المحتوى، لا يكاد يمكن للمستخدم ملاحظة تأخيرها. ولكن استخدام تقنية الفحص العميق لا تتوقف عند تحقيق هذا الغرض. فمقدمي خدمات الإنترنت يستخدمونها أيضا لتفضيل محتوى على أساس عنوان الإنترنت لمصدره، فيعطون خدماتهم، أو محتوى طرف آخر، أفضلية لضمان أداء أفضل. وتستخدم تقنية الفحص العميق أيضا لتفضيل بعض المحتوى بمحاسبة المستخدم بتعريفة أقل عليه أو تقديمه مجانا.

باستخدام تقنية الفحص العميق وغيرها من التقنيات يمكن لمقدمي خدمات الإنترنت التمييز ضد المعلومات المنقولة على الإنترنت بناء على عنوان الإنترنت للمصدر (لحجب مواقع بعينها)، أو عنوان الإنترنت للمرسل إليه (قطع الاتصال بالإنترنت لمستخدمين بعينهم)، أو البروتوكول (خفض السرعة أو حجب البيانات التي تستخدم بروتوكول بعينه مثل الـ BitTorrent أو VoIP)، أو التطبيق (خفض السرعة أو حجب بعض التطبيقات مثل Skype).(Zhao 2012; Margoni and Perry 2000).

فحص المحتوى الفعلي لحزم البيانات (Internet Filtering) هو أيضا وسيلة لممارسة الرقابة بعزل وحجب المحتوى، والمراقبة برصد المحتوى الذي يرسله المستخدمون. ويمكن للحكومات أن تقوم بذلك فقط بالتعاون الطوعي أو القسري من قبل مقدمي خدمات الإنترنت.

بعض السياسات التي يستخدمها كثير من مقدمي الخدمات تستهدف مستخدمين بعينهم، مثل خفض السرعة للمستخدمين ذوي الخطط غير المحدودة عندما يتجاوز استهلاكهم حدا أقصى محدد خلال فترة زمنية. ومرة أخرى هذه سياسة تستخدم التعرف على المستخدم بواسطة عنوان الإنترنت لأغراض غير تلك التي صممت لها. والتقنيات التي تستخدمها هذه السياسات تمثل انتهاكا لخصوصية المستخدم، والتي يمكن استغلالها لأغراض المراقبة من قبل الأنظمة القمعية، حيث إن عناوين الإنترنت يخصصها مقدمو خدمة الإنترنت

لمستخدمين بعينهم، وهؤلاء يقدمون بياناتهم الشخصية عند التسجيل، ويحتفظ مقدمو الخدمة بها.

الحوكمة باستخدام نظام تسمية النطاقات

عندما نشرت ويكيليكس برقيات دبلوماسية سرية للولايات المتحدة، توقف أحد مقدمي خدمة ترجمة أسماء النطاقات إلى عناوين الإنترنت المقابلة لها عن الاستجابة للطلبات على النطاق Wikilieaks.org. هذا مثال واضح لاستخدام البنية التحتية للإنترنت لعرض سياسي، وهو في هذه الحالة معاقبة جهة لتعد سياسي ومحاولة المساعدة في تقليل الخسائر المتسبب فيها هذا التعدي بالحد من الوصول إلى المواد السرية. (Musiani 2016)

يمكن استغلال نظام تسمية النطاقات لأغراض مختلفة. التقنية المعتادة هي ترجمة الطلبات على اسم نطاق بعينه إلى عنوان إنترنت مختلف عن المقابل له (DNS Hijacking). هذه التقنية تستخدم لإعادة توجيه الوصول إلى المواقع التي تقدم موادا محمية بقوانين الملكية الفكرية، ولكنها تستخدم أيضا لأغراض الرقابة لإعادة توجيه الوصول عن مواقع المحتوى الجنسي، أو مدونات النشطاء السياسيين، أو المواقع الإعلامية المعارضة في بعض الدول، وغير ذلك. وفي حين أن مقدمي خدمات الإنترنت، والذين عادة ما يقدمون أيضا خدمات ترجمة أسماء النطاقات لعملائهم، قد يحولون الوصول إلى بعض المواقع عندما تطالبهم جهات إنفاذ القانون في إحدى الدول بذلك، ففي حالات أخرى قد يقومون بذلك عندما يطلبه منتجو المحتوى في حال باع أحد المواقع المواد ذات الملكية الفكرية أو قدمها مجانا بشكل غير قانوني.

إحدى التقنيات الأخرى المستخدمة لأغراض سياسية واقتصادية هي تقنيات "حقن" اسم النطاق (DNS Injection). بعض هذه التقنيات يسمى "الرجل في المنتصف" (Man in the middle)، وهو يرصد طلبات أسماء النطاقات ويحقن النتيجة المرسلة للمستخدم بمعلومات زائفة. ومن المعروف أن هذه التقنيات يستخدمها مجرمو الفضاء السيبري لإعادة تحويل المستخدمين إلى صفحات زائفة، حيث يمكنهم الحصول على بيانات شخصية حساسة/ مثل أرقام بطاقات الإئتمان البنكية. وتستخدم بعض الحكومات هذه التقنيات أيضا لأغراض الرقابة، على سبيل المثال يستخدم ما يدعى بالحائط الناري العظيم للصين

(China Great Firewall) تقنيات حقن أسماء النطاقات للرقابة على المحتوى وحجبه. يمكن أيضا للشركات الخاصة أن تستخدم هذه التقنية لحقن معلومات مضللة لأغراض سياسية. بعض مقدمي خدمات الإنترنت ومقدمو المحتوى المنخرطون في الإعلانات، أو في جمع البيانات على الشبكة، قد يقومون باختطاف طلبات أسماء النطاقات أحيانا لإعادة تحويلها إلى صفحات "تحميل" وسيطة تعرض إعلانات أو محتويات أخرى.

جانب آخر لاستخدام نظام أسماء النطاقات لأغراض غير وظيفته هو معاملة أسماء النطاقات على أنها ممتلكات أو أصول منتجة. على سبيل المثال حصل مجموعة من ضحايا تفجير انتحاري وقع في القدس ودبرته حركة حماس على أمر من محكمة أمريكية بصرف بلايين الدولارات كتعويضات من الحكومة الإيرانية بسبب دعمها لحركة حماس. وسعيا من المدعين لتحصيل بعض هذه التعويضات طالبوا (ICANN) بأن تصادر أسماء النطاقات من المستوى الأعلى لأكواد الدول لكل من إيران وكوريا الشمالية وسوريا، وتسليمها إليهم لاستغلالها تجاريا. لكن (ICANN) رفضت الطلب متحججة بأن أسماء النطاقات العليا لأكواد الدول ليست مملوكة لحكوماتها، ولا يمكن بالتالي التصرف فيها على هذا الأساس. (Musiani et al. 2016, p. 3)

كيف يؤثر استغلال البنية التحتية للإنترنت على المستخدمين؟

التقنيات المختلفة لاستغلال البنية التحتية للإنترنت لأغراض غير تلك التي صممت لأجلها تعدل خبرة المستخدمين بالإنترنت بطرق متعددة، تتراوح بين المزعج إلى الخطر بشدة. اختبار سرعات متدنية، تأخير، أو أزمنة أطول للتحميل وتنزيل المواد يتسبب في الانزعاج. عدم القدرة على الوصول إلى مواقع وصفحات قد يمنع المستخدمين من استخدام الإنترنت لأغراض التعلم والبحث والعمل، والحصول على الاستشارات الطبية، إلخ. انتهاكات الخصوصية والمراقبة يمكن أن تمثل تهديدات مختلفة للمستخدمين، بعضها قد يكون مهددا للحياة.

مقارنة بالتدخلات التي تمارس على مستويات أعلى من شبكة الإنترنت، فإن تلك التدخلات التي تستخدم بنيتها التحتية هي في الأغلب غير مرئية، وبعيدة عن متناول المستخدم النهائي، ولا يمكن تجنبها بسهول وأحيانا لا يمكن تجنبها على الإطلاق. وفي حين أن بعض

الدول تقوم بسن تشريعات تفرض حيادية الشبكة فتحد من بعض الممارسات، إلا أن هذا محدود بنطاق تطبيق هذه القوانين، كما أنه سيعاني من الصعوبات المتعلقة باستخدام القوانين في حوكمة الإنترنت في العموم، وهي ما سيناقشه جزء تال من هذه السلسلة.

في المحصلة، ذلك الذي يستغل مواضع الضعف في البنية التحتية للإنترنت يمكن فقط التعامل معه بتضمين الإجراءات المضادة في هذه البنية التحتية نفسها. ولكن في منظومة حوكمة يديرها أصحاب المصالح المتعددة، كثير من بين الأكثر نفوذا بينهم يستفيد بطريقة أو بأخرى من تطويع أدوات حوكمة البنية التحتية للإنترنت لأغراض خاصة بهم، من الصعب كثيرا تحقيق التغيير المطلوب. فقط بتمثيل فعال للمستخدمين النهائيين للإنترنت داحل المنظومة العالمية متعددة-أصحاب-المصلحة لحوكمة الإنترنت، يمكن التأثير على هذه المنظومة بطريقة تدعم مصالح هؤلاء المستخدمين.

المصادر

DeNardis, Laura. 2012. “Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance.” *Information, Communication & Society* 15 (5): 720–38. .https://doi.org/10.1080/1369118X.2012.659199

———. 2014 .*The Global War for Internet Governance*. New Haven: Yale University Press.

DeNardis, Laura, and Francesca Musiani. 2016. “Governance by Infrastructure.” In *The Turn to Infrastructure in Internet Governance*, edited by Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, 3–21. Information Technology and Global Governance. New York: Palgrave .Macmillan US. https://doi.org/10.1057/9781137483591_1

Kurbalija, Jovan. 2016. *An Introduction to Internet Governance*. 7th edition. Msida, Malta Geneva .Belgrade: DiploFoundation

Margoni, Thomas, and Mark Perry. 2000. “Deep Pockets, Packets; Harbours: Never the Three Shall Meet.” *SSRN Electronic Journal*. https://www.academia.edu/25908268/Deep_Pockets_Packets_and_Harbours_Never_the_Three_Shall_M .eet

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Information .Revolution and Global Politics. Cambridge, Mass: MIT Press

Musiani, Francesca. 2016. “Alternative Technologies as Alternative Institutions: The Case of the Domain Name System.” In *The Turn to Infrastructure in Internet Governance*, edited by Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, 73–86. Information Technology and Global .Governance. New York: Palgrave Macmillan US. https://doi.org/10.1057/9781137483591_4

Musiani, Francesca, Derrick Cogburn, Laura DeNardis, and Nanette Levinson. 2016. *Turn to Infrastructure in Internet Governance*. Place of publication not identified: Springer Nature. .http://link.springer.com/openurl?genre=book&isbn=978-1-349-57846-7

Wagner, Ben. 2009. “Deep Packet Inspection and Internet Censorship: International Convergence on an ‘Integrated Technology of Control.’” SSRN Scholarly Paper 2621410. Rochester, NY: Social Science .Research Network. https://doi.org/10.2139/ssrn.2621410

Zhao, Jinshuang. 2012. “Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society The Privacy Security Research Paper Series Issue #1 The Privacy & Security -Research Paper Series,” July. https://www.academia.edu/es/5102177/Implications_of_Deep_Packet_Inspection_DPI_Internet_Surveillance_for_Society_The_Privacy_and_Security_Research_Paper_Series_issue_1_The_Privacy_and_Security_Research_Paper_Series.