آراء مجتمع الإنترنت
حظر المحتوى على الإنترنت: نظرة عامة

مارس 2017

Internet Society

جدول المحتويات

تمهيد

يُعتبر استخدام حظر الإنترنت من قِبل الحكومات، لمنع الوصول إلى محتويات غير قانونية، من الأمور الشائعة عالميًا والآخذة في التنامي. وهناك العديد من الأسباب التي تدفع واضعي السياسات إلى خيار حظر الوصول إلى بعض المحتويات، كالمقامرة عبر الإنترنت والملكية الفكرية وحماية الأطفال والأمن القومي. ورغم ذلك، وبعيدًا عن المسائل المتعلقة باستغلال الأطفال في الأعمال الإباحية، يوجد توافق دولي محدود بخصوص مواصفات المحتوى المناسب من وجهة نظر السياسة العامة.

وتهدف هذه الورقة إلى توفير تقييم تقني للطرق المختلفة لحظر محتوى الإنترنت، بما في ذلك مدى جودة عمل كل طريقة والمشاكل والمخاطر المصاحبة لكل طريقة. ولم نحاول تقييم شرعية حظر محتويات الإنترنت أو دوافعه المتعلقة بالسياسة[1].

تتمثل النتائج التي توصلنا إليها، بناءً على التحليل التقني، في أن استخدام حظر الإنترنت لاستهداف المحتويات أو الأنشطة غير القانونية هو أمرٌ غير فعال عمومًا، وغالبًا ما يكون غير مؤثر ويتسبب في الإضرار بمستخدمي الإنترنت على نحوٍ غير مقصود.

ومن وجهة النظر التقنية، نوصي بأن يتروى صانعو السياسة عند التفكير في استخدام أدوات حظر الإنترنت لحل المشاكل المتعلقة بالسياسة العامة. فإذا قرروا انتهاج تقنيات مختلفة وقاموا بتنفيذها، فسيكون ذلك انتصارًا مهمًا من أجل إنترنت عالمي ومفتوح وموثوق وقابل للتشغيل المتبادل.

1 يمكن للقرّاء المهتمين بالتقييمات القانونية لحظر المحتوى زيارة المصادر التالية:
- المادة 19: https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf
- المجلس الأوروبي:
http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet

مقدمة

يعود كثير من الفضل في تحول الإنترنت إلى ظاهرة اجتماعية عالمية إلى للمحتوى والخدمات التي استفادت من الهيكل الفريد الذي تتميز به الشبكة. وهناك اقتصاديات بأكملها تعتمد على تدفق المحتويات عبر الحدود. ومن المحتمل أن تتسبب الابتكارات اليومية في تعطيل خدمات صناعية بأكملها. ويُعتبر الإنترنت الآن جزءًا أساسيًا من العملية الديمقراطية والنقاشات السياسية. والعلاقات الشخصية تنشأ وتنتهي عبر الإنترنت.

وما زال الاتجاه في تزايدٍ دون تباطؤ. فوفقًا للتقديرات[2]، ستساوي حركة الإنترنت العالمية عام 2020 ما يعادل 95 ضعف إجمالي حركة الإنترنت العالمية لعام 2005. وسيكون عدد الأجهزة المتصلة بشبكات IP ثلاثة أضعاف سكان العالم عام 2020.

إلا أن الإنترنت ما زال يضم بعض المحتويات التي يرغب صناع السياسة والمشرعون والمنظمون، حول العالم، في حظرها. وأصبح استخدام تقنيات حظر محتوى الإنترنت لمنع الوصول إلى محتويات تُعتبر غير مشروعة بموجب قوانين وطنية معينة، بدءًا من مواقع المقامرة الأجنبية في أوروبا وأمريكا الشمالية ووصولًا إلى الأحاديث السياسية في الصين، ظاهرة عالمية. وتتعدد الدوافع السياسية العامة لحظر محتوى الإنترنت، بدايةً من التنازع على انتهاك حقوق الملكية الفكرية، والمواد المسيئة للأطفال، والأنشطة غير القانونية عبر الإنترنت، ووصولًا إلى حماية الأمن القومي.

ولا يكمن الهدف من هذه الورقة في تقييم هذه الدوافع أو تحديد الجيد أو السيئ من تقنيات الحظر من وجهة نظر أخلاقية أو قانونية أو اقتصادية أو سياسية أو اجتماعية. ولكننا سنقدم تقييمًا تقنيًا لمزايا وأضرار تقنيات الحظر الرائجة المُستخدمة لمنع الوصول إلى المحتويات التي تُعتبر غير قانونية. حيث يكمن هدفنا في مساعدة القراء على إدراك ما تستطيع كل تقنية حظره وما لا تستطيع، بالإضافة إلى الآثار الجانبية والمخاطر والموازنات والتكاليف المصاحبة.

وقد توصلنا إلى أن استخدام حظر الإنترنت لاستهداف المحتوى غير القانوني هو أمرٌ غير فعال عمومًا وغالبًا ما يكون غير مؤثر، وقد يتسبب في حدوث أضرار جانبية غير مقصودة لمستخدمي الإنترنت، قمنا بتلخيصها في الجدول الموجود بصفحة 6.

ومن وجهة النظر التقنية، **ندعو صانعي السياسة إلى التروي** في استخدام هذه التدابير وندعوهم إلى تحديد أولوياتهم في التجاوب والتركيز بشكلٍ أساسي على استهداف المشكلة من مصدرها (يمكنك الاطلاع على توصيات أكثر تفصيلاً في نهاية هذه الورقة، بما في ذلك إرشادات حول كيفية تقليل الآثار السلبية لهذه التدابير).

ينبغي ملاحظة أن هذه الورقة لا تركز على تدابير الحظر التي تُطبق لأغراض الإدارة التنظيمية أو الأمنية (مثل استهداف الرسائل الإلكترونية غير المرغوبة أو البرامج الضارة). ففي هذه الحالات، غالبًا ما تكون بعض الأدوات التي أوردناها في هذه الورقة، فعالة في تحقيق الأهداف المرجوة.

هامش جانبي:
تصفية أم حظر أم مراقبة؟

عند وصف تصفية الإنترنت، تظهر مصطلحات مثل "التصفية" و"الحظر" و"الإيقاف" و"المراقبة" (إلى جانب العديد من المصطلحات الأخرى). ومن وجهة نظر المستخدم، يكون المصطلح المختار أقل أهمية من التأثير: فبالنسبة له، يكون جزءًا من الإنترنت غير ممكن الوصول إليه. وبالنسبة لواضعي السياسات والناشطين الرقميين، عادة ما يكون اختيار مصطلح معين مدفوعًا بالمعنى الدلالي أكثر من الصحة التقنية. فمصطلح "المراقبة" يحمل دلالة سلبية قوية، في حين يبدو مصطلح "التصفية" عملية لطيفة وغير ضارة، مثل إزالة البذور غير المرغوب فيها من كوب عصير البرتقال. ولقد اخترنا استخدام مصطلح "الحظر" كعبارة بسيطة ومباشرة طوال هذا البحث.

2 مؤشر شبكة سيسكو® المرئية: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html

يُلخص الجدول أدناه، الأضرار الأساسية المصاحبة لحظر محتوى الإنترنت بناءً على اعتبارات تخص السياسة العامة:

المشكلة	التفاصيل
يسهل التحايل عليها	قد يتمكن المستخدمون أصحاب الدوافع القوية من تجاوز جميع التقنيات الواردة في هذه الورقة. فكلما اكتشف المستخدمون طرقًا للالتفاف على حظر المحتوى، قلَّت فاعلية إجراء الحظر.
لا تحل المشكلة	إجراء الحظر لا يُزيل المحتوى المُصنف باعتباره غير قانوني. وفي بعض الحالات، قد يكون الحظر المحلي غير متوافق مع المعايير الدولية، ولكن في حالة وجود اتفاق واسع النطاق على عدم شرعية المحتوى، فإن الحل الأمثل للمشكلة يكون بحذف المحتوى من مصدره.
تُسبب أضرارًا جانبية	عندما يكون كلا المحتويين، القانوني وغير القانوني، يتشاركان نفس عنوان IP أو اسم النطاق أو مواصفاتٍ أخرى، فسيؤدي حظر المحتوى إلى حظر الوصول إلى كل شيء، سواء قانوني أو غير قانوني. على سبيل المثال، حظر الوصول إلى إحدى المقالات على Wikipedia باستخدام تصفية نظام اسم المجال (DNS) سوف يؤدي أيضًا إلى حظر ملايين المقالات الأخرى على Wikipedia.
يعرض المستخدمين للخطر	عندما تُعتبر خدمة الإنترنت المحلية غير موثوقة وغير مفتوحة، فقد يلجأ مستخدمو الإنترنت إلى طرق بديلة وغير قياسية، مثل تنزيل أحد البرامج التي تعيد توجيه حركتهم لتجنب عوامل التصفية. وهذه الحلول المؤقتة تعرض المستخدمين لمخاطر إضافية فيما يتعلق بالحماية.
يشجع على انعدام الشفافية	تُعد البيئة التي تتسم بالشفافية والثقة، من الأمور المهمة لتشغيل الإنترنت بطريقةٍ ناجحة. ويؤدي حظر المحتوى إلى انعدام تلك الشفافية، ويقوض الطبيعة المفتوحة التي تتميز بها الشبكة، ويتسبب في فقدان الثقة في المصادر العامة للمعلومات.
يؤدي إلى ظهور الخدمات السرية	عندما يُصبح حظر المحتوى أمرًا شائعًا، تظهر الخدمات "السرية" وطبقات متراكبة من الشبكات البديلة التي تعرض المحتوى بعيدًا عن أعين جهات إنفاذ القانون. فعلى سبيل المثال، قد ينتقل المحتوى إلى الإنترنت المظلم، أو قد يوجه المستخدمون البيانات عبر شبكات VPN.
يتدخل في الخصوصية	يحتاج العديد من أنواع حظر المحتوى إلى فحص حركة بيانات المستخدم، بما في ذلك حركة البيانات المشفرة. وتُنتهَك خصوصية مستخدمي الإنترنت، عندما يقوم طرف خارجي بمراقبة ما يفعله المستخدم أو يسجل تعاملاته أو يكسر شفرات الأمان الأساسية.
تُثير المخاوف بخصوص حقوق الإنسان والمعالجة الواجبة	إن تطبيق حظر المحتوى، دون النظر إلى بعض المبادئ مثل الضرورة والتناسب، قد يتسبب في أضرار جانبية كبيرة ويفرض قيودًا على الحريات والتواصل المفتوح وحقوق الأفراد.

دوافع حظر المحتوى

نركز في هذه الورقة على **الحظر القائم على اعتبارات السياسة العامة** وآثارها على الإنترنت ومستخدميه (أنظر الهامش الجانبي للاطلاع على دوافع حظر المحتوى الأخرى)

يُستخدم الحظر القائم على اعتبارات السياسة العامة من قِبل السلطات المحلية لوضع قيود على الوصول إلى المعلومات (أو الخدمات ذات الصلة) التي إما أنها غير قانونية في اختصاص قضائي معين، أو تُعتبر تهديدًا للنظام العام، أو مثيرة لاعتراض شريحة معينة من الجمهور.

فعلى سبيل المثال، توجد رغبة عامة لدى معظم البلدان في حظر وصول الأطفال إلى المواد الإباحية أو وصول أي شخص إلى المواد التي بها إساءة للأطفال. وقد يتم حظر المحتوى أيضًا، بناءً على البيئة التشريعية المحلية، إذا كان منتهكًا لقوانين الملكية الفكرية، أو يمثل تهديدًا للأمن القومي، أو محظورًا لأسبابٍ ثقافية أو سياسية.

ومن ضمن التحديات التي تدفع السلطات المحلية إلى استخدام تدابير حظر المحتوى، كون الجهات الفاعلة المختلفة التي تقدم المحتوى المصدر إلى المستهلكين تنتمي لبلدانٍ أخرى تعمل بقوانين مختلفة تحدد المحتوى القانوني "وغير القانوني". والأكثر من ذلك، أن بيئة الإنترنت العالمية تجعل من مسألة إيقاف مصدر المحتوى غير القانوني، أصعب من مجرد إغلاق الخادم المحلي ببساطة. فعلى سبيل المثال، قد يكون الشخص الذي يقدم المحتوى والخوادم التي تستضيفه واسم النطاق الذي يشير إليه، من ثلاثة بلدان مختلفة، وجميعها يقع ضمن الاختصاص القضائي لسلطة محلية واحدة. وهو ما يسلط الضوء على أهمية التعاون بين الاختصاصات القضائية والحاجة إلى التنسيق الوثيق بين أصحاب المصلحة غير الحكوميين.

أنواع أخرى من دوافع حظر المحتوى

في هذا البحث، كنا نركز على الحظر القائم على اعتبارات السياسة العامة، ولكن هناك سببان شائعان آخران لتنفيذ الحظر الشبكي. السبب الأول هو **منع التهديدات الأمنية للشبكة أو الاستجابة لها**. ويعد هذا النوع من الحظر شائعًا للغاية. فعلى سبيل المثال، تحاول معظم المؤسسات حظر البرامج الضارة من الدخول إلى شبكاتها. ويقوم العديد من مزودي خدمات الإنترنت (ISP) بوضع حظر لحركة البيانات الخبيثة التي تخرج من شبكاتهم، مثل أجهزة إنترنت الأشياء المقرصنة (مثل كاميرات الويب). وتعد تصفية البريد الإلكتروني عملية شائعة للغاية، وتتضمن حظر البريد الإلكتروني المجمع غير المرغوب فيه بالإضافة إلى البريد الإلكتروني الضار مثل رسائل التصيد الاحتيالي. ولم يتم مناقشة هذه الأنواع من الحظر في هذا البحث.

والسبب الثاني للحظر هو **إدارة استخدام الشبكة**. فالمجال المتزايد لحظر محتوى الإنترنت يستند إلى متطلبات الشبكة أو عرض النطاق الترددي أو إدارة الوقت، بدلاً من أنواع معينة من المحتوى. وعلى سبيل المثال، قد يرغب أصحاب العمل في تقييد وصول موظفيهم إلى مواقع التواصل الاجتماعي في حين استمرار وصولهم إلى الإنترنت على سطح المكتب. ويمكن لمزودي خدمات الإنترنت حظر محتوى معين أو السماح به أو خنقه أو تسريعه على أساس الخدمات المتعاقد عليها. ونادرًا ما تكون إدارة استخدام الشبكة مسألة تتعلق بالسياسة العامة، إلا عندما تدخل في مجال السلوك المناهض للمنافسة. سيجد القراء المهتمون بحياد الشبكة مراجع في لمزيد من الاطلاع، صفحة 26.

نظرة عامة على تقنيات حظر المحتوى

تشتمل كل تقنية على حدودٍ وتبعات تقنية وسياسية يجب الالتفات إليها عند اقتراح أي نوع من أنواع حظر المحتوى. وتهدف هذه الورقة إلى تقديم طريقة عامة لتقييم فعالية هذه التقنيات وآثارها الجانبية. وسيجد القراء المهتمون بمناقشات فنية أكثر بخصوص حظر المحتوى مراجعَ لمستندات التقنية لفرقة العمل المتخصصة بهندسة الإنترنت في لمزيدٍ من الاطلاع، صفحة 26.

تستهدف هذه الورقة تقييم الأنواع التالية من حظر المحتوى:

- الحظر القائم على عنوان IP والبروتوكول
- الحظر القائم على فحص حزم البيانات
- الحظر القائم على عنوان URL
- الحظر القائم على النظام الأساسي (وبالأخص محركات البحث)
- الحظر القائم على DNS

اخترنا هذه الأنواع الخمسة من الحظر، لأنها تستهدف عناصر الدائرة النموذجية للمستخدم النهائي في العثور على المعلومات واسترجاعها، بما في ذلك استخدام محرك البحث واستعراض المعلومات من خلال مستعرض ويب أو أداة مشابهة. وتُعتبر هذه الدائرة معروفة جدًا لدى صُناع السياسة، حيث أنهم مستخدمون للإنترنت أنفسهم، وهذه هي العمليات التي تحاول تعطيلها معظم وسائل الحظر القائم على اعتبارات خاصة بالسياسة العامة.

نوضح في الرسم التخطيطي إلى اليمين الخطوات التي قد يتبعها مستخدم الإنترنت العادي في لعثور على المعلومات، إلى جانب أنواع الحظر التي يتم استخدامها لتعطيل هذه الدائرة عندما يتم تطبيق الحظر القائم على اعتبارات السياسة العامة. وفي مخططنا، يبحث أحد مستخدمي الإنترنت عن محتويً ما باستخدام محرك بحث (الخطوة 1)، وهي نقطة بداية شائعة. ويعود محرك البحث بمجموعة من النتائج (الخطوة 2)، ويحدد المستخدم أحد النتائج ثم ينقر عليها (الخطوة 3). يُستخدم أحد أنواع الحظر، وهو الحظر القائم على النظام الأساسي، لتعطيل هذا الجزء من الدائرة من خلال حظر بعض النتائج من الظهور على محرك البحث.

يحاول كمبيوتر المستخدم العثور على الخادم الذي يستضيف البيانات في نظام DNS الخاص بشبكة الإنترنت (الخطوتان 4 و5). ويُستخدم نوع آخر من الحظر، وهو الحظر القائم على DNS، لتعطيل هذا الجزء من الدائرة.

ومن ثم، يحاول مستعرض الويب الخاص بالمستخدم الاتصال بالخادم (الخطوة 6). فيتم حظر هذا الجزء من الدائرة باستخدام ثلاثة أنواع أخرى من الحظر: الحظر القائم على عنوان IP والبروتوكول، والحظر القائم على عنوان URL، والحظر القائم على الفحص العميق لحزم البيانات.

نظرة عامة: خطوات استرجاع المعلومات وحظرها عبر الإنترنت

1
يبحث المستخدم عن "قنبلة" باستخدام محرك البحث.

2

3
ينقر المستخدم على نتيجة (http://مثال.com/قنبلة)

4
يبحث جهاز الكمبيوتر الخاص بالمستخدم عن "مثال.com" في شبكة DNS حتى يتمكن من الاتصال بخادم الويب.

DNS
مثال.com؟
محلل

5
192.0.222=مثال.com

6
يتصل متصفح الويب الخاص بالمستخدم بخادم الويب الخاص بـ "مثال.com" ويطلب صفحة الويب المحددة التي نقر عليها المستخدم.

إلى: 192.0.222
طلب من جهاز الكمبيوتر الخاص بالمستخدم إلى خادم مثال.com
الحصول على: (http://مثال.com/قنبلة)

7

من: 192.0.222
طلب من خادم مثال.com إلى المستخدم
الحصول على:

دون التصفية، يرى المستخدم نتيجة

إذا حدث حظر، فهذا ما قد يشاهده المستخدم بدلاً من ذلك:

مع **الحظر القائم على الفحص العميق لحزم البيانات**، قد تؤدي الكلمات الأساسية في صفحة الويب إلى انقطاع حركة البيانات. هناك خطر كبير لمنع المحتوى غير المقصود.

تم إعادة تعيين الاتصال

مع **الحظر القائم على عنوان URL**، يتم حظر حركة البيانات في حالة العثور على عنوان URL في قائمة الحظر.

تم حظر هذا الموقع من قبل مسؤول الشبكة

مع **الحظر القائم على IP والبروتوكول**، يتم حظر الاتصال بالخادم مع IP=192.0.222. جميع المحتويات الموجودة على الخادم غير متاحة سواء كانت مقصودة أو غير مقصودة.

انتهت مهلة الاتصال

مع **الحظر القائم على DNS**، لا يمكن لجهاز الكمبيوتر الخاص بالمستخدم العثور على الخادم، لذلك لا يمكنه الاتصال لرؤية صفحة الويب. سيشاهد المستخدم "لم يتم العثور على الخادم".

لم يتم العثور على الخادم

مع **تصفية البحث** وغير ذلك من أسباب الحظر القائم على النظام الأساسي، يتم حجب النتائج عن المستخدم، إذا كان يستخدم محركًا معينًا.

لم يتم العثور على نتائج لـ "قنبلة"

وبالطبع لا يقتصر الإنترنت على عمليات البحث ومستعرضات الويب، وهناك العديد من التقنيات التي تمت مناقشتها أدناه، والتي تعد فعالة في حظر ما هو أكثر من صفحات ويب. فعلى سبيل المثال، يُمكن حظر استخدام خدمات VPN لتشفير حركة البيانات وإخفاؤها، من خلال الجمع بين الحظر القائم على الفحص العميق لحزم البيانات والحظر القائم على عنوان IP والبروتوكول.

وتُستخدم هذه الأنواع من الحظر بشكلٍ محدد للغاية (مثل استخدامها مع مستند معين على موقع ويب معين) أو بشكلٍ عام للغاية (مثل "المواد المُثار حولها قضايا" أو "خدمات انقل الصوت عبر IP").

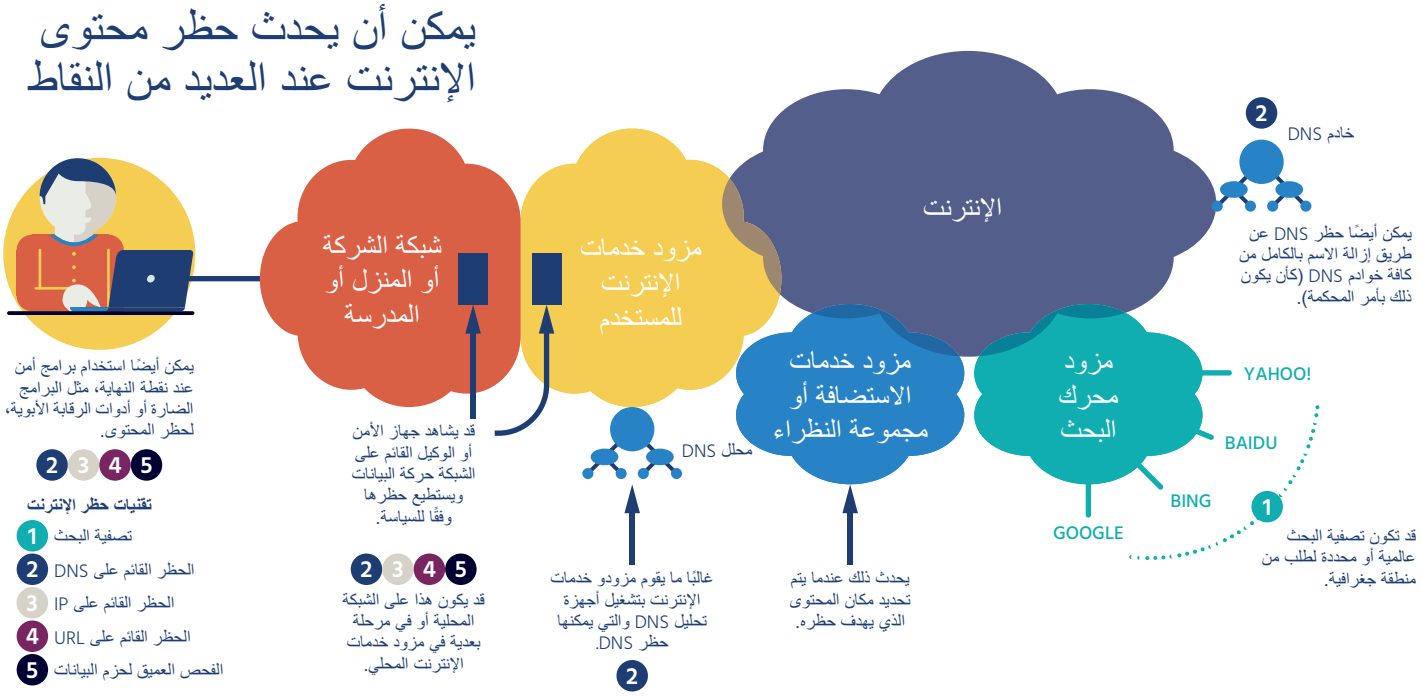
أين يحدث حظر المحتوى؟

يُمكن استخدام العديد من تقنيات حظر المحتوى، التي تمت مناقشتها هنا، عند نقاطٍ مختلفة؛ كما هو موضح في الجدول أدناه.

على المستوى المحلي	في حالة التكليف من قبل الحكومة، قد تخضع حركة البيانات التي تدخل البلد أو تخرج منها بالكامل لحظر المحتوى. ويتطلب هذا الأمر مراقبة صارمة لجميع الاتصالات العابرة للحدود، من خلال أدوات من قبيل البوابة الوطنية أو جدار الحماية الوطني، أو فرضها على جميع شركات الاتصال ومزودي خدمات الإنترنت في البلد المعني بالتوازي.
على مستوى شركات الاتصال ومزودي خدمات الإنترنت	قد تقوم شركات الاتصال الخاصة بتثبيت أدوات للحظر، بما في ذلك شركات الهواتف المحمولة وشركات الإنترنت التقليدية.
على مستوى الشبكة المحلية	يكون الاتصال النموذجي لأجهزة الكمبيوتر المحمول والكمبيوتر المكتبي الخاصة بالمستخدم النهائي عبر شبكات في المنزل أو الشركة أو المدرسة، ولا تكون مربوطة بشركة الاتصال مباشرةً. وقد تشتمل هذه الشبكات المحلية على برامج حظر مثبتة، وعادة ما يكون هذا الحظر قائمًا على إدارة الشبكة أو سياسة الأمان، وليس على أساس سياسة حكومية.
على مستوى نقطة النهاية	قد يتم تثبيت برامج تنفذ سياسة حظر مباشرةً على أجهزة الكمبيوتر الخاصة بالمستخدم النهائي.ويعد ذلك شائع الاستخدام في شبكات المنازل والشركات، وعادة لأسباب أمنية ولكن أيضًا لإدارة الشبكة أو لأسباب الرقابة الأبوية.

لاحظ أنه في حالة الحظر القائم على اعتبارات السياسة العامة، تطبق غالبية التدابير على المستويين الأولين (المستوى الوطني، ومستوى شركة الاتصالات، ومستوى مزود خدمات الإنترنت)

يلخص الرسم البياني أدناه بعض المواقع الرئيسية التي يمكن أن يحدث فيها الحظر، وأي أنواع الحظر يمكن أن يحدث عند كل نقطة.



هامش جانبي:
حظر محتوى عند نقطة النهاية

يركز هذا البحث على حظر محتوى الإنترنت القائم على اعتبارات السياسة العامة.

وبرغم ذلك، فمن المهم أن نلاحظ أن أحد أكثر الطرق فعالية لمنع المحتوى غير المرغوب فيه هو من خلال استخدام البرامج المثبتة على جهاز المستخدم، وتسمى عادة "نقطة النهاية" لأنها هي النقطة الأخيرة من الاتصال بين المستخدم والإنترنت. ويستخدم معظم مستخدمي الكمبيوتر برامج نقطة النهاية لحظر البرامج الضارة (الفيروسات وأحصنة طروادة والتصيد الاحتيالي)، سواء تم تثبيتها شخصيًا أو من قبل مجموعة تكنولوجيا المعلومات بالمؤسسة.

كما تستخدم المنظمات برامج حظر محتوى نقطة النهاية أيضًا لحظر المحتوى لأسباب أخرى. وعلى سبيل المثال، غالبًا ما تقوم المكتبات بتثبيت هذا النوع من البرامج على أجهزة الكمبيوتر العامة لحظر عرض المواد الإباحية من قبل العملاء، وقد يستخدمها الآباء لحظر المحتوى غير المرغوب فيه عن أطفالهم.

قد يستخدم حظر محتوى عند نقطة النهاية العديد من التقنيات الموضحة في هذا البحث، بما في ذلك مسح المحتوى وتصنيف عناوين URL وحظر عناوين IP واعتراض DNS. وبوجه عام، يحدث الحظر والتحليل في نقطة النهاية نفسها. ومع ذلك، يتزايد عدد الباعة لهذا البرنامج أيضًا باستخدام الأدوات السحابية بما في ذلك مسح المحتوى والحظر القائم على DNS، بالتعاون مع كمية صغيرة من برامج نقطة النهاية. وفي هذه الحلول الجديدة، قد يمر محتوى الإنترنت أو جزء منه من خلال خدمة سحابية. وتتمثل ميزة نقل عملية صنع القرار إلى السحابة في أنه لا يجب تحديث نقاط النهاية باستمرار، ويتم نقل تأثير أداء تقييم المحتوى من جهاز الكمبيوتر الخاص بالمستخدم أو هاتفه الذكي إلى سحابة من أجهزة الكمبيوتر محددة الحجم بسهولة. ورغم ذلك، عندما يتم توجيه حركة البيانات عبر طرف ثالث، يخلق هذا أيضًا مشكلات تتعلق بالخصوصية عن طريق جعل المحتوى متاحًا للطرف الثالث، وإذا تم تنفيذه بشكل سيء، ستنشأ مشكلات متعلقة بالأمن أيضًا.

أنواع حظر المحتوى المقيَّمة

إن أنواع حظر المحتوى المشترك الخمسة متفردة فيما تحظره وفي كيفية عملها.

وفيما يلي، نناقش تقنيات حظر المحتوى بمزيد من التفصيل، ونقيمها في ضوء أربعة معايير محددة[3]

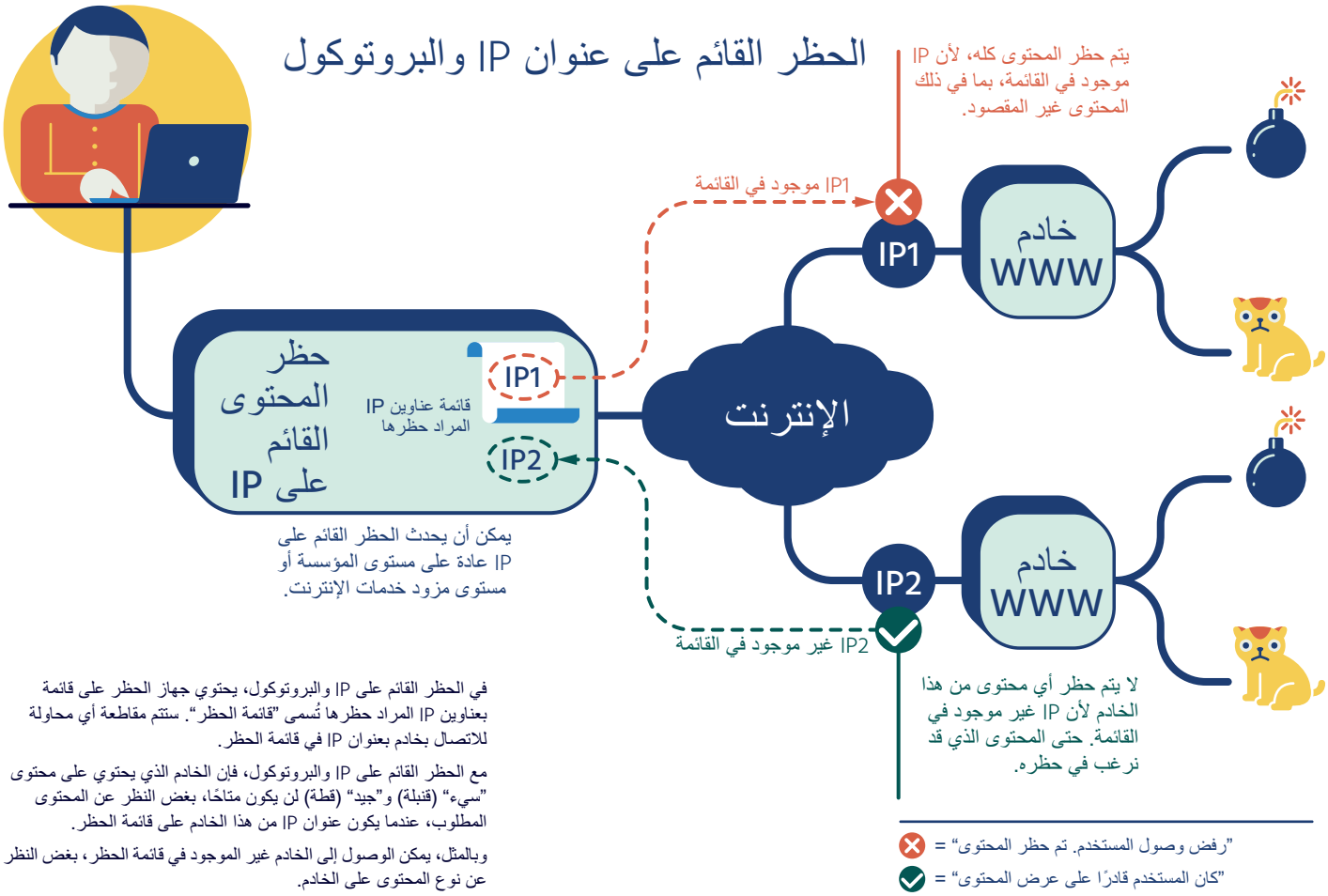
1. **أيّ من مجموعات المستخدمين وخدمات الإنترنت تتأثر** بهذه التقنية؟ ما المجموعات التي لا تتأثر؟
2. **ما مدى تخصص التقنية** في منع الوصول إلى محتوى معين؟ ما الأضرار الجانبية (الحظر غير المقصود) التي تنشأ عن تقنية الحظر هذه؟
3. **ما مدى فعالية** هذه التقنية في حظر المحتوى؟ ما أنواع المستخدمين ومزودي المحتوى القادرون على الالتفاف على هذه التقنية؟
4. **ما الآثار الجانبية الشائعة** لهذه التقنية؟ ما المشكلات الفنية التي تسببها هذه التقنية؟ ما المشكلات غير الفنية، مثل التأثير على الثقة والحقوق الأساسية، التي تنشأ عن استخدام هذه التقنية؟

3 تؤخذ هذه المعايير من معيار الإنترنت RFC 7754، "الاعتبارات التقنية لحظر خدمات الإنترنت وتصفيتها."

الحظر القائم على عنوان IP والبروتوكول

يضع الحظر القائم على IP حواجزَ في الشبكة، مثل جدران الحماية، التي تحظر كل حركات البيانات إلى مجموعة من عناوين IP. ويستخدم الحظر القائم على البروتوكول معرفات شبكة أخرى ذات مستوى منخفض، مثل رقم منفذ TCP/IP الذي يمكنه تحديد تطبيق معين على خادم أو نوع من بروتوكول التطبيق. ولا تعمل تقنيات حظر المحتوى البسيطة المذكورة على حظر المحتوى مباشرةً- فهي تحظر حركة البيانات لعناوين IP أو منافذ TCP/IP أو البروتوكولات المعروفة المرتبطة ببعض المحتويات أو التطبيقات. ويمكن أيضًا أن يتم الحظر القائم على عنوان IP والبروتوكول ببرامج تُثبت على أجهزة الكمبيوتر الخاصة بالمستخدم، وعادة ما يكون ذلك لأغراض أمن الشبكات.

على سبيل المثال، إذا كان الهدف هو حظر كل المحتوى المستضاف في البلد الخيالي إلبونيا، يمكن استخدام الحظر القائم على عنوان IP إذا كانت مجموعة عناوين IP التي تستضيف المحتوى في إلبونيا معروفة. وبالمثل، إذا كان الهدف هو حظر جميع خدمات VPN (التي تستخدم لتشفير حركة البيانات وإخفاء كل من الوجهة والمحتوى)، يمكن استخدام الحظر القائم على البروتوكول لوقف خدمات VPN عبر البروتوكولات أو أرقام منفذ TCP/IP المعروفة.



في الحظر القائم على IP والبروتوكول، يحتوي جهاز الحظر على قائمة بعناوين IP المراد حظرها تُسمى "قائمة الحظر". ستتم مقاطعة أي محاولة للاتصال بخادم بعنوان IP في قائمة الحظر.

مع الحظر القائم على IP والبروتوكول، فإن الخادم الذي يحتوي على محتوى "سيء" (قنبلة) و"جيد" (قطة) لن يكون متاحًا، بغض النظر عن المحتوى المطلوب، عندما يكون عنوان IP من هذا الخادم على قائمة الحظر.

وبالمثل، يمكن الوصول إلى الخادم غير الموجود في قائمة الحظر، بغض النظر عن نوع المحتوى على الخادم.

نقطة الاختلاف في هذه التقنية عن الحظر القائم على IP هو خنق حركة البيانات. ففي هذا السيناريو، لا يتم حظر حركة البيانات كلها، بل يتم حظر نسبة معينة منها. ويمكن للمستخدمين تلقي الخدمة ببطء شديد أو بصورة متقطعة. ويمكن استخدام هذا لتثبيط المستخدمين عن استخدام الخدمة من خلال جعلها تبدو وكأنها غير موثوقة، أو التشجيع على استخدام خدمات بديلة، دون الكشف عن حدوث الحظر. (يمكن أيضًا القيام بذلك لأسباب تتعلق بإدارة الشبكة وعرض النطاق الترددي على مستوى المؤسسة أو مستوى مقدم خدمات الإنترنت.)

يستخدم الحظر القائم على عنوان IP والبروتوكول الأجهزة الموجودة بين المستخدم النهائي والمحتوى، مما يتطلب من الطرف المطبق للحظر (مثل مقدم خدمات الإنترنت الخاص بالمستخدم) أن يكون له سيطرة كاملة على الاتصال بين المستخدم النهائي و شبكة الإنترنت. ولن يتأثر بهذا النوع من الحظر المستخدم غير الموجود "خلف" جهاز الحظر أو ذلك الذي يستخدم تقنية مثل شبكة VPN التي تخفي الوجهة الحقيقية لحركة البيانات.

عمومًا، إن الحظر القائم على عناوين IP عبارة عن تقنية تصفية ضعيفة والتي توصف بأنها غير فعالة، ومن الصعب الحفاظ على فعاليتها، ولديها مستوى عال من الحظر الاعتباطي غير المقصود، ويمكن الالتفاف عليها بسهولة من قبل الناشرين الذين ينقلون المحتوى إلى خوادم جديدة (مع عناوين IP جديدة).

كما أن الحظر القائم على عناوين IP لا يعمل عندما يستخدم مقدمو المعلومات شبكات تسليم المحتويات (CDNs)، لأن عناوين IP الخاصة بالمعلومات تتمتع بديناميكية عالية وتتغير باستمرار.[4] وتستخدم شبكات CDN أيضًا عنوان IP نفسه للعديد من العملاء وأنواع المحتويات، ما يؤدي إلى وجود مستوى عال من عمليات الانقطاع غير المقصودة في الخدمة.

يعمل الحظر القائم على عنوان IP والبروتوكول بشكل أفضل عندما يستخدم لحظر تطبيقات محددة، بدلاً من محتوى محدد. وعلى سبيل المثال، قد يتم حظر حركة VPN بواسطة آليات حظر منفذ TCP/IP والبروتوكول، إلى جانب آليات حظر عناوين IP لخدمات VPN العامة المعروفة. وتعد تلك التقنية شائعة وفعالة للغاية.

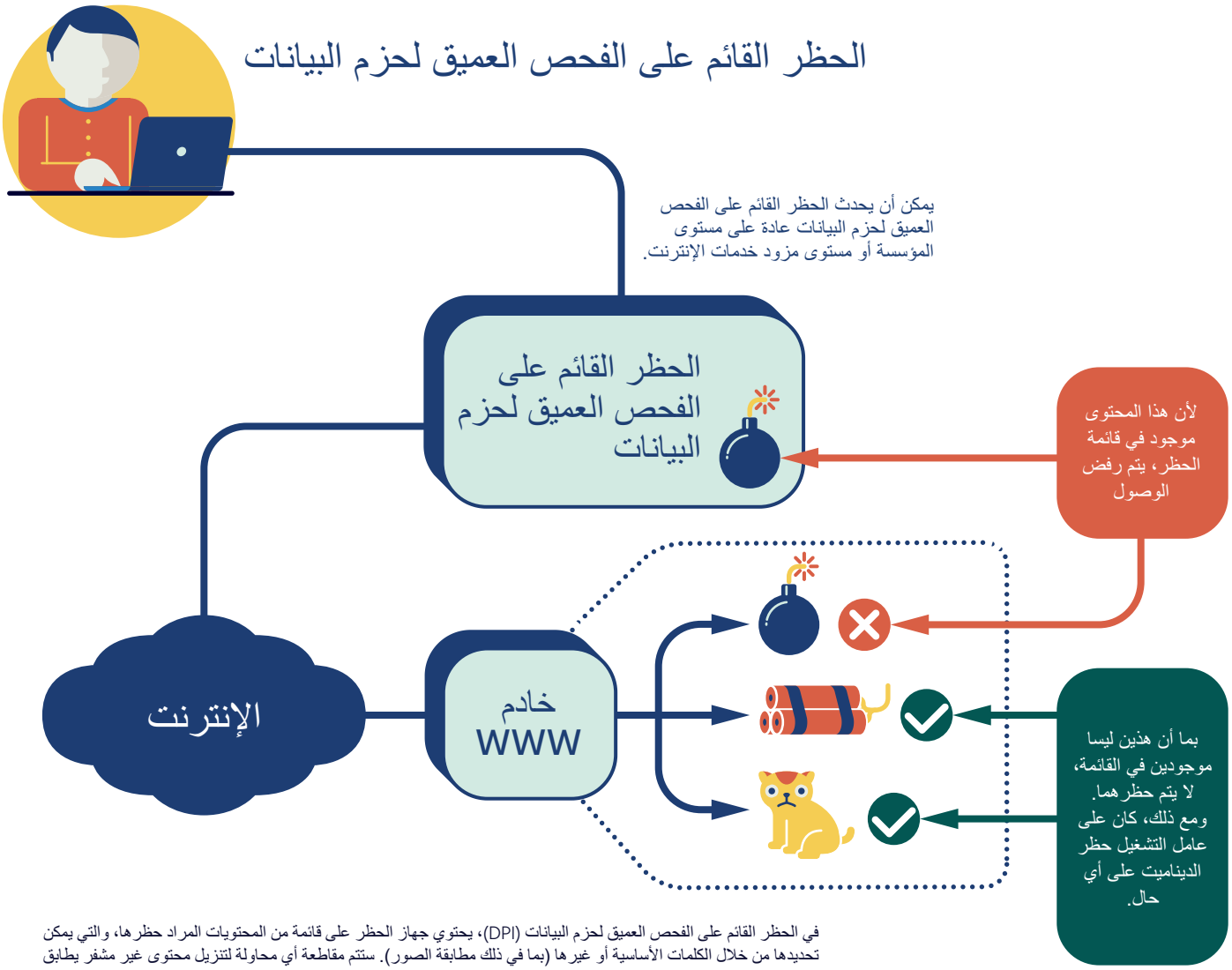
كما أن الحظر القائم على عناوين IP هو الأكثر فعالية عندما يتم استضافة المحتوى في خادم معين في مركز بيانات محدد، أو مجموعة محددة جدًا من الملفات المعنية. ولا يعد الحظر القائم على IP فعالاً لخدمات الاستضافة الأكبر الموزعة عبر العديد من مراكز البيانات أو التي تستخدم شبكات توزيع المحتويات (CDNs) لتسريع الوصول.

4 شبكة توزيع المحتوى هي شبكة كبيرة من الخوادم وموزعة جغرافيًا تُعنى بتسريع تسليم محتويات الويب لمستخدمي الإنترنت. وتمتلك شبكات CDN الكبيرة مئات الآلاف من الخوادم في العديد من البلدان لإتاحة وصول أسرع لمحتويات عملائها. وتقوم شبكات CDN بتخزين نسخ من محتويات نصوص العملاء والصور والصوت والفيديو في خوادمها الخاصة حول "حواف" الإنترنت، بحيث يمكن تلبية طلبات المستخدمين بواسطة خادم حافة CDN قريب بدلاً من خوادم العميل المركزية.

الحظر القائم على الفحص العميق لحزم البيانات

يستخدم الحظر القائم على الفحص العميق لحزم البيانات (DPI) الأجهزة بين المستخدم النهائي وبقية الإنترنت التي تقوم بالتصفية استنادًا إلى محتويات أو أنماط أو أنواع تطبيقات معينة. ويكون هذا النوع من الحظر الشبكي مكثف للغاية من الناحية الحسابية وبالتالي يكون مكلفًا، لأنه يجب تقييم المحتوى بكامله في ضوء قواعد الحظر. ويمكن أيضًا أن يتم الحظر القائم على الفحص العميق لحزم البيانات (DPI) من خلال برامج تُثبت على أجهزة الكمبيوتر الخاصة بالمستخدم، ويكون ذلك لأغراض أمن الشبكات عادة.

يتطلب الحظر القائم على الفحص العميق لحزم البيانات (DPI) بعض أنواع التوقيعات أو المعلومات حول المحتوى ليكون فعالاً. وقد تكون هذه التوقيعات في صورة كلمات أساسية أو خصائص حركة البيانات (مثل أحجام الحزم أو معدلات الإرسال)، أو أسماء ملفات، أو غيرها من المعلومات الخاصة بالمحتوى. ويستخدم الحظر القائم على الفحص العميق لحزم البيانات (DPI) بشكل فعال لحظر أو خنق تطبيقات معينة (مثل تبادل الملفات بين الأقران أو نقل الصوت عبر برتوكول الإنترنت [VoIP]) وأنواع ملفات البيانات (مثل ملفات الوسائط المتعددة).



في الحظر القائم على الفحص العميق لحزم البيانات (DPI)، يحتوي جهاز الحظر على قائمة من المحتويات المراد حظرها، والتي يمكن تحديدها من خلال الكلمات الأساسية أو غيرها (بما في ذلك مطابقة الصور). ستتم مقاطعة أي محاولة لتنزيل محتوى غير مشفر يطابق القائمة.

مع الفحص العميق لحزم البيانات (DPI)، تكون النتائج الإيجابية الخاطئة (حظر المحتوى بشكل غير صحيح) والنتائج السلبية الخاطئة (الفشل في حظر المحتوى كما هو مقصود) أمرًا شائعًا. يكون من الصعب أيضًا القيام بعملية الفحص العميق لحزم البيانات (DPI) بشكل صحيح عندما يتم تشفير حركة البيانات.

في الرسم البياني هنا، تم حظر القنبلة لأنها تطابق المحتوى. ومع ذلك، لم يتم حظر الديناميت، حتى وإن كان عامل تشغيل جهاز الفحص العميق لحزم البيانات (DPI) يريد حظره، لأن الديناميت لا يتطابق مع قائمة حظر المحتوى.

يشيع استخدام الحظر القائم على الفحص العميق لحزم البيانات (DPI) في المؤسسات الخاصة بنظم حماية تسرب البيانات، وبرامج مكافحة البريد الإلكتروني العشوائي والبرامج الضارة (مكافحة الفيروسات)، ولإدارة شبكة تحديد أولويات حركة البيانات (مثل تعزيز أولوية المؤتمرات عبر الفيديو بالمؤسسة). ومع ذلك، فإنه يمكن أيضًا أن يُستخدم لأغراض الحظر القائم على السياسات. وعلى سبيل المثال، كثيرًا ما يكون استخدام خدمات VoIP غير المتاحة من قبل شركة الاتصالات الوطنية محكومًا أو مقيدًا، كما أن الحظر القائم على الفحص العميق لحزم البيانات (DPI) يكون فعالاً في إنفاذ تلك القيود.

يستخدم الحظر القائم على الفحص العميق لحزم البيانات (DPI) الأجهزة التي يمكنها رؤية كافة حركات المرور بين المستخدم النهائي والمحتوى والتحكم فيها، مما يتطلب من الطرف المطبق للحظر (مثل مقدم خدمات الإنترنت الخاص بالمستخدم) أن يكون له سيطرة كاملة على الاتصال بين المستخدم النهائي والإنترنت. وعندما يتم تشفير حركة البيانات، كما هو الحال في كثير من الأحيان، فإن أنظمة الحظر القائم على الفحص العميق لحزم البيانات (DPI) قد لا تعد فعالة. ويتم مناقشة ذلك بمزيد من التفصيل في الهامش الجانبي "التشفير والوكيل وتحديات الحظر" في الجانب الأيسر.

يمثل الحظر القائم على الفحص العميق لحزم البيانات (DPI) عمومًا تقنية فعالة في حظر أنواع معينة من المحتويات التي يمكن تحديدها باستخدام التوقيعات أو قواعد أخرى (مثل "حظر كافة تنقلات الصوت عبر IP"). وكان الحظر القائم على الفحص العميق لحزم البيانات (DPI) أقل نجاحًا بكثير مع أنواع أخرى من المحتويات، مثل بعض ملفات الوسائط المتعددة أو الوثائق التي تضم كلمات أساسية معينة. ولأن الحظر القائم على الفحص العميق لحزم البيانات (DPI) يفحص كافة حركات البيانات للمستخدمين النهائيين، فإنه أيضًا يكون أكثر تدخلًا في خصوصية المستخدم النهائي.

تختلف الفعالية العامة للحظر القائم على الفحص العميق لحزم البيانات (DPI) اختلافًا كبيرًا تبعًا للأهداف وأدوات الفحص العميق لحزم البيانات (DPI) المستخدمة. وبوجه عام، فإن أدوات الفحص العميق لحزم البيانات (DPI) تحقق أقصى فعالية في إدارة الشبكات وإنفاذ الأمن، وهي ليست مناسبة تمامًا للحظر القائم على السياسات.

الحظر القائم على عنوان URL

تعد طريقة الحظر القائم على عنوان URL طريقة حظر شعبية للغاية، ويمكن أن تحدث على جهاز الكمبيوتر الفردي، أو في على جهاز شبكي بين جهاز الكمبيوتر وبقية الإنترنت. ويعمل الحظر القائم على عنوان URL مع تطبيقات الويب، ولا يتم استخدامه لحظر التطبيقات غير القائمة على الويب (مثل VoIP). وفي الحظر القائم على عنوان URL، يعترض عامل تصفية تدفق حركة (HTTP) على شبكة الإنترنت وفحص عنوان URL، الذي يظهر في طلب HTTP، في ضوء قاعدة بيانات محلية أو خدمة عبر الإنترنت. واستنادًا إلى الرد، يسمح عامل تصفية عناوين URL بالاتصال بخادم الويب المطلوب أو يحظره.

بوجه عام، تتم إدارة عناوين URL حسب الفئة (مثل "المواقع الرياضية") ويتم حظر فئة كاملة أو خنقها أو السماح بها[5]. وفي حالة وجود سياسة وطنية تتطلب حظر عناوين URL، يصبح من المحتمل إدارة الحكومة لخدمات الإنترنت وسياسات الحظر. ويمكن لعامل تصفية عناوين URL إيقاف حركة البيانات ببساطة، أو يمكنه إعادة توجيه المستخدم إلى صفحة ويب أخرى، أو عرض بيان السياسة أو ذكر أن حركة البيانات تم حظرها. ويمكن فرض الحظر القائم على عناوين URL في الشبكة عن طريق الوكلاء، فضلاً عن جدران الحماية والموجهات.

هامش جانبي:
التشفير، الوكلاء، وتحديات الحظر

للعديد من التقنيات التي تم مناقشتها في هذا البحث، بما في ذلك الحظر القائم على الفحص العميق لحزم البيانات (DPI) والحظر القائم على عنوان URL، لديها قيود حقيقية للغاية: إذ يجب أن تكون قادرة على رؤية حركة البيانات أثناء تقييمها. ولا يمكن تشفير خوادم الويب التي توفر التشفير أو المستخدمين الذين يضيفون التشفير إلى اتصالاتهم (عادة من خلال تقنية التشفير الخاصة بالتطبيقات، مثل TLS/SSL) بشكل موثوق من قبل الأجهزة داخل الشبكة. ويتم التحايل على العديد من التقنيات الأخرى أيضًا بسهولة عندما يكون لدى المستخدم إمكانية وصول إلى تكنولوجيا VPN التي تقوم بتشفير الاتصالات وتخفي الوجهة الحقيقية ونوع حركة البيانات. وعلى الرغم من أن الباحثين والبائعين قد طوروا بعض الطرق لتحديد بعض أنواع حركة البيانات من خلال الاستدلال والتحليل، إلا أن هذه التقنيات غالبًا ما تعتمد على مجرد التخمين لنوع حركة البيانات التي تشاهدها.

في الأبحاث الأخيرة، تم تشفير 49% من حركة البيانات على شبكة الإنترنت الأمريكية (حسب الحجم) في فبراير، 2016. (انظر: http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf) وستكون حركة البيانات هذه غير مرئية بشكل فعال إلى أدوات الحظر القائم على عنوان URL وأدوات الفحص العميق لحزم البيانات (DPI) التي تفحص المحتوى، لأن المعلومات المرئية ستكون اسم النطاق للخادم الذي يستضيف المعلومات فقط. وللتعويض عن هذا "الظلا"، تستخدم بعض تقنيات الحظر الشبكي أجهزة نشطة (تسمى الوكلاء) التي تعترض وتفك تشفير حركة البيانات بين المستخدم وخادم الويب، وتفك نموذج التشفير من النهاية إلى النهاية الخاص بـ TLS/SSL.

عند استخدام الوكلاء، فإنها تتسبب في مخاوف كبيرة تتعلق بالأمن والخصوصية. ومن خلال فك تشفير نموذج TLS/SSL، يحصل الطرف المطبق للحظر على إمكانية الوصول إلى جميع البيانات المشفرة ويمكنه عن غير قصد تمكين أطراف ثالثة من فعل الشيء نفسه. كما يمكن للوكيل تغيير المحتوى. وإذا كان لدى الطرف المطبق للحظر سيطرة على نظام المستخدم (على سبيل المثال، الجهاز الذي تتم إدارته من قبل الشركة سيكون خاضعًا للسيطرة بدرجة عالية)، فقد يكون الوكيل شفافًا للغاية. ومع ذلك، فإن وجود وكيل سيكون واضحًا للمستخدم النهائي بوجه عام، على الأقل لحركة بيانات (TLS/SSL) المشفرة (على سبيل المثال، قد يحصل المستخدم على تنبيه بأن الشهادة ليست من سلطة موثوق بها). وبالإضافة إلى ذلك، فإن معايير الصناعة وفرقة العمل المعنية بهندسة الإنترنت الجديدة (مثل أمن النقل الصارم لـ HTTP [RFC6797] وتثبيت المفتاح العام لـ HTTP [RFC 7469] وبروتوكول DANE [RFC 6698]) وميزات الأمان الجديدة في متصفحات الإنترنت الحديثة تجعل من الصعب توفير خدمة الوكيل (وفك التشفير) لحركة TLS/SSL دون معرفة المستخدم النهائي وتعاونه.

قد تؤدي تثبيت الوكلاء لأسباب حظر المحتوى إلى حدوث اختناقات في أداء تدفق حركة بيانات الشبكة، مما يجعل الخدمات بطيئة أو غير موثوقة.

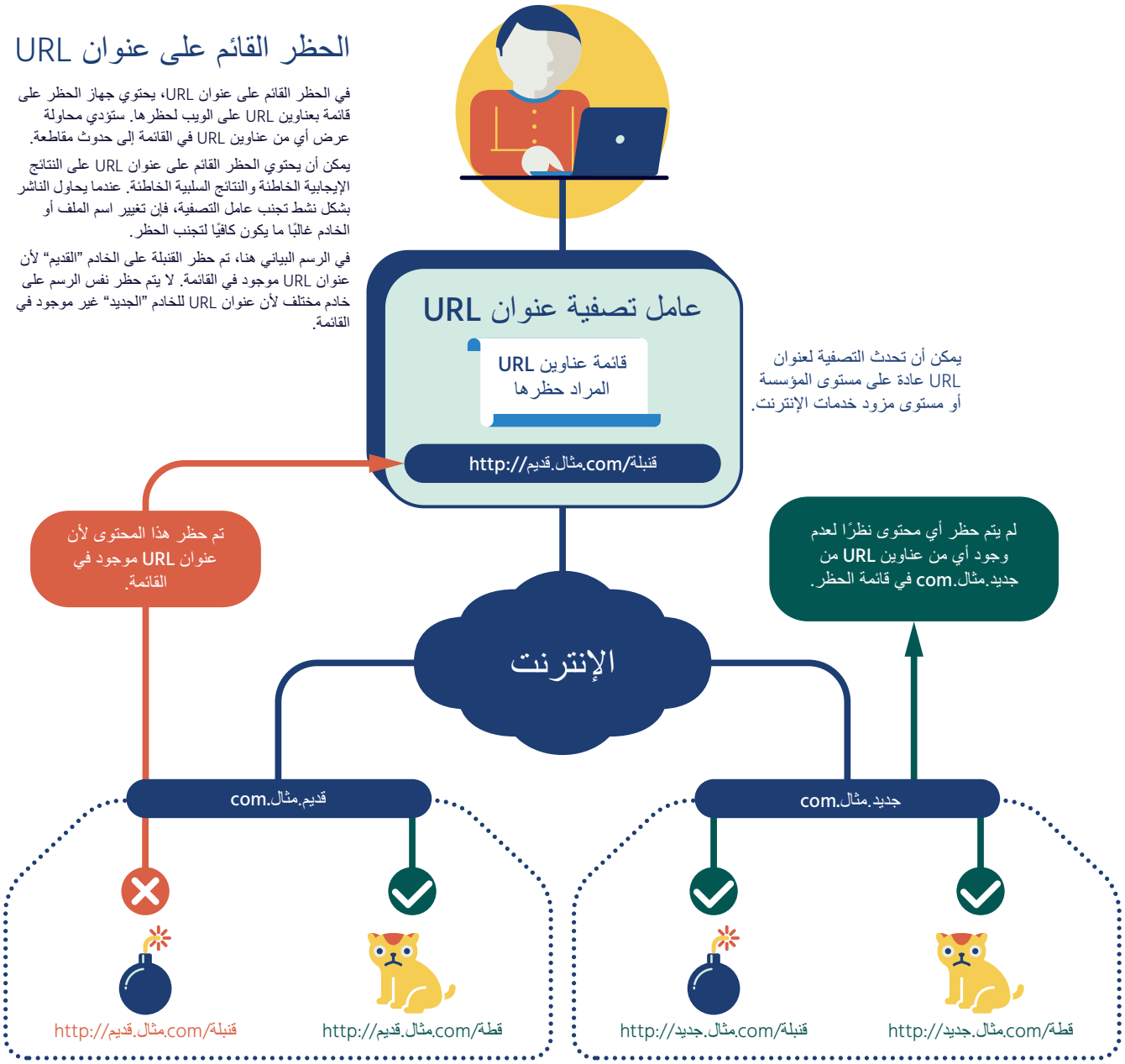
5 يتم إنشاء فئات تصفية لعناوين URL من قبل مقدمي خدمات الأمن، وغالبًا ما تستند إلى مجموعة من التحليلات البشرية لصفحات الويب إلى جانب بعض المسح الآلي لمحتوى صفحة الويب. ويقدم معظم مقدمي خدمات الأمن قواعد بيانات تصفية لعناوين URL لأغراض إدارة حركة بيانات الشبكات المؤسسية، ولكن يمكن استخدامها في سياقات أخرى، مثل تلك التي تمت مناقشتها في هذه الورقة.

الحظر القائم على عنوان URL

في الحظر القائم على عنوان URL، يحتوي جهاز الحظر على قائمة بعناوين URL على الويب لحظرها. ستؤدي محاولة عرض أي من عناوين URL في القائمة إلى حدوث مقاطعة.

يمكن أن يحتوي الحظر القائم على عنوان URL على النتائج الإيجابية الخاطئة والنتائج السلبية الخاطئة. عندما يحاول الناشر بشكل نشط تجنب عامل التصفية، فإن تغيير اسم الملف أو الخادم غالبًا ما يكون كافيًا لتجنب الحظر.

في الرسم البياني هنا، تم حظر القنبلة على الخادم "القديم" لأن عنوان URL موجود في القائمة. لا يتم حظر نفس الرسم على خادم مختلف لأن عنوان URL للخادم "الجديد" غير موجود في القائمة.



يتطلب الحظر القائم على عناوين URL من الطرف المطبق للحظر (مثل مقدم خدمات الإنترنت الخاص بالمستخدم) القدرة على اعتراض ومراقبة حركة البيانات بين المستخدم النهائي والإنترنت. وعادة ما يكون حظر عناوين URL مكلفًا، لأن جهاز التصفية يجب أن يكون بشكل عام بين المستخدم والإنترنت، وبالتالي يتطلب مستوى عال من الموارد لتقديم الأداء المقبول.

يعد الحظر القائم على عناوين URL بوجه عام فعالاً للغاية في تحديد المحتوى الذي قد يكون على خوادم أو خدمات مختلفة لأن عنوان URL لا يتغير حتى إن قام الخادم بتغيير عناوين IP. وفي حالات قليلة، قد يفشل الحظر القائم على عناوين URL في حظر حركة البيانات بشكل كامل عندما تكون عناوين URL معقدة للغاية أو تتغير بشكل متكرر. وقد يحدث ذلك لأن ناشر المعلومات قد قرر عمدًا التخلص من حظر عامل تصفية عناوين URL بشكل فعال، أو قد يكون له أثر جانبي لبعض أنظمة النشر المتقدمة مثل تلك المستخدمة في المطبوعات الكبيرة على الإنترنت.

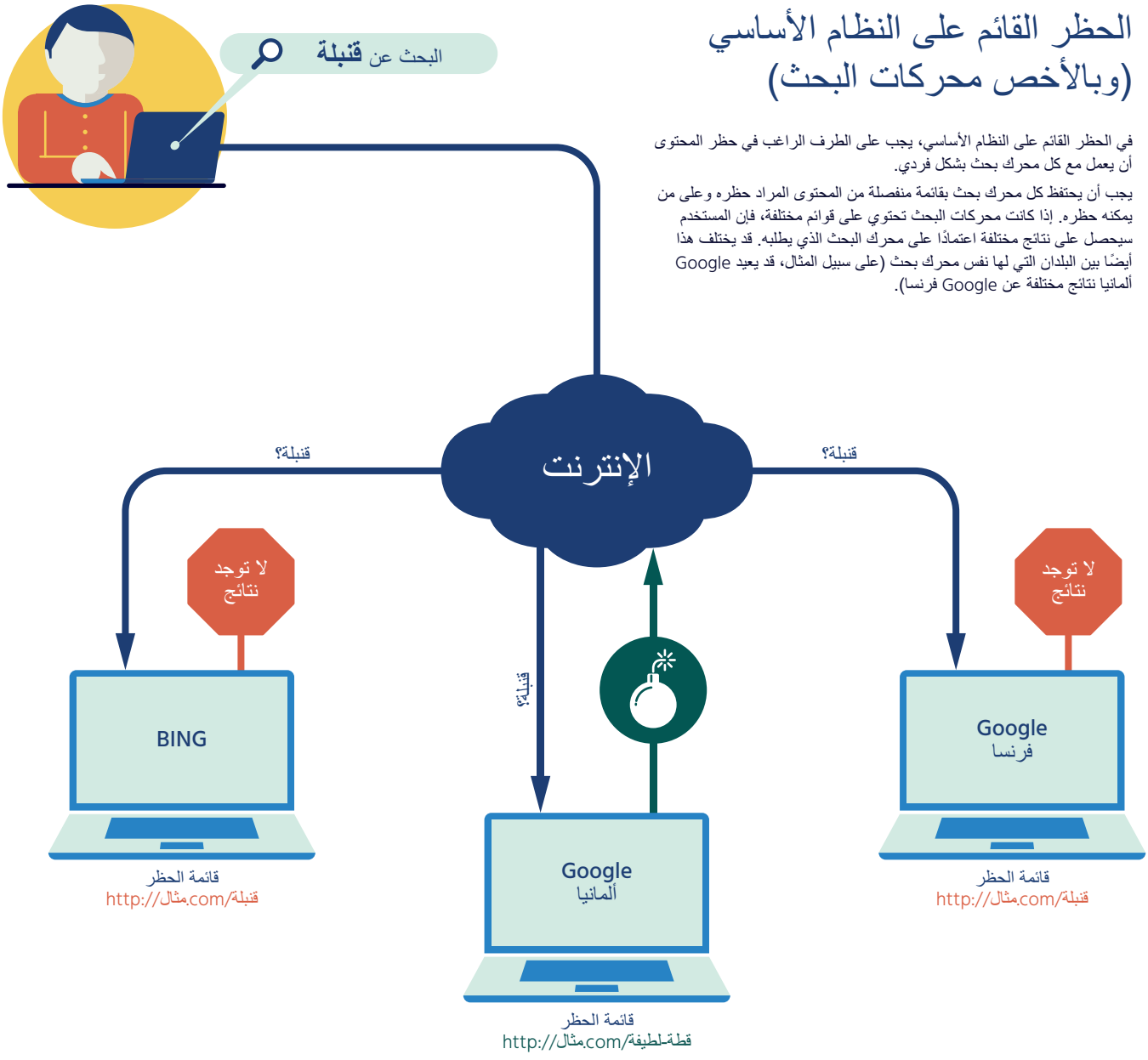
عادة ما يكون الحظر القائم على عناوين URL فعالاً في عناوين URL عالية المستوى، مثل صفحة ويب معينة، ولكنه لا يكون فعالاً عندما يتم النظر في الروابط العميقة (مثل وحدات البت الفردية من المحتوى ضمن صفحة ويب). واعتمادًا على كيفية انتقال المستخدم إلى المحتوى المحدد، قد يكون الحظر القائم على عناوين URL قادرًا أو غير قادر على حظر كل الوصول - إذا كان المستخدم لديه "رابط عميق" لا يغطيه عامل تصفية عنوان URL، يتم السماح بالمحتوى. فعلى سبيل المثال، يتضمن موقع الويب Playboy كل من عناوين playboy.com، ولكنه يضمِّن أيضًا المحتوى باستخدام اسم النطاق "playboy.tv". كما أن عامل تصفية عنوان URL الذي لم يتضمن عناوين "playboy.tv" لن يحظر محتوى الفيديو.

تعتمد جميع أنواع الحظر القائم على عناوين URL بشكل كبير على جودة عامل التصفية، وقد يؤدي عامل التصفية المصمم بشكل سيء أو ذو النطاق الموسع إلى حظر حركة بيانات بصورة غير مقصودة أو يكون له تأثيرات سلبية أخرى على تجربة المستخدم، مثل التأثير في تحميل صفحات الويب أو تنسيقها عند حظر بعض المكونات.

كما هو الحال في أنواع الحظر القائم على الفحص العميق لحزم البيانات، يتطلب حظر عناوين URL وكيلًا من نوع ما لرؤية عنوان URL الكامل عند تشفير حركة البيانات باستخدام HTTPS (TLS/SSL). وانظر الهامش الجانبي "التشفير والوكيل وتحديات الحظر"، في صفحة 15، للحصول على مزيد من المعلومات حول التأثيرات على خصوصية المستخدم النهائي. وبالنسبة إلى حركة البيانات المشفرة، يمكن للحظر القائم على عناوين URL مشاهدة عنوان IP للخادم فقط، وليس عنوان URL الكامل، مما يؤدي إلى حدوث مستوى أعلى بكثير من الحظر غير المقصود. ولأنالاستعانة بالوكلاء تكون مكلفة ومتداخلة لتجربة المستخدم، فإن حظر عناوين URL لا يعمل بشكل جيد كأداة للحظر القائم على السياسات.

الحظر القائم على النظام الأساسي (وبالأخص محركات البحث)

في بعض الحالات، تتعاون السلطات الوطنية مع مقدمي خدمات المعلومات الرئيسيين في حظر المعلومات داخل منطقتهم الجغرافية دون حظر النظام الأساسي بأكمله. ومن الأمثلة الأكثر شيوعًا لتصفية النظام الأساسي من خلال مقدمي محركات البحث الرئيسية والأنظمة الأساسية لوسائل التواصل الاجتماعي. وفي الآونة الأخيرة، قيل أيضًا أن متاجر تطبيقات الهواتف النقالة (مثل متجر Apple وGoogle Play) تعمل مع السلطات الوطنية لحظر التنزيلات من تطبيقات محددة في بلدها.



الحظر القائم على النظام الأساسي تقنية تتطلب مساعدة مالك النظام الأساسي، مثل مشغل محرك البحث مثل Google أو Microsoft. وفي هذه التقنية، ستتلقى الاستعلامات من مجموعة معينة من مستخدمي الإنترنت إلى محرك البحث مجموعة مختلفة من النتائج من بقية الإنترنت - ما يؤدي إلى تصفية المؤشرات إلى المحتوى الذي يكون غير مقبول في بعض الحالات. وفي بعض الحالات، يعتمد تعريف ما سيتم حظره على اللوائح المحلية والمتطلبات الحكومية، ولكنه قد يكون أيضًا بسبب مخاوف مشغل محرك البحث. على سبيل المثال، يمكن أن يحظر محرك البحث مؤشرات البرامج الضارة أو المحتوى الذي يعتبر غير مناسب وفقًا لشروط الخدمة الخاصة به.

نظرًا لأن الحظر القائم على محرك البحث يتطلب تعاون مزود محرك البحث، فإن ذلك سوف يحصر استخدامه لسيناريوهين محددين للغاية وهما: القواعد على المستوى القطري (حظر المحتوى القائم على قواعد محددة على المستوى القطري وقواعد محددة على المستوى الإقليمي) والقواعد القائمة على العمر (حظر المواد غير المناسبة
لصغار السن).

ولا يؤثر الحظر القائم على محرك البحث إلا على المستخدمين الذين يختارون محرك بحث بعينه، وفقط عندما يُحدَّد المستخدمون باعتبارهم ينتمون إلى مجموعة معينة بواسطة قواعد التصفية. وفي الحظر القائم على العمر، مثل ميزة البحث الآمن[6] (التي تقدمها محركات البحث وموفرو المحتوى)، تستدعي الحاجة وجود اشتراك صريح من المستخدم.

نظرًا لأن الحظر القائم على محرك البحث لا يصفّي إلا مؤشرات المحتوى وليس المحتوى نفسه، فإنه يعد تقنية غير فعالة إلى درجة كبيرة، ويمكن أن يكون له عواقب غير مقصودة تتمثل في استرعاء الانتباه بشكل متزايد للمحتوى المحظور. وما يُصعِّب تنفيذ هذا النوع من الحظر إلى درجة كبيرة، توفر العديد من محركات البحث، بالإضافة إلى وسائل أخرى بديلة للعثور على المحتوى.

بالرغم من أن الحظر القائم على محرك البحث يبدو وكأنه يؤدي القليل حيال حظر المحتوى، فإن التقنية لاقت شعبية كبيرة على الصعيد المحلي، ومن المعروف أن الحكومات حول العالم تطلب أن تنفذ محركات البحث الرئيسية عوامل تصفية وفقًا للوائحهم، مثل انتهاك حقوق التأليف والنشر أو أنواع خاصة من الخطابات التي يحظرها القانون المحلي. فعلى سبيل المثال، أصدرت شركة Google تقريرًا في 2015 أوضحت فيه أنها تلقت 8,398 طلبًا من 74 محكمة محلية لإزالة 36,834 نتيجة من نتائج البحث[7]. ولاقت طلبات انتهاك حقوق التأليف والنشر التي يتقدم بها الأفراد شعبية كبيرة أيضًا: ففي يونيو 2016، أصدرت شركة Google تقريرًا أوضحت فيه أن 6,937 من أصحاب حقوق التأليف والنشر طلبوا إزالة حوالي 86 مليون نتيجة بحث من نتائج Google خلال الشهر المذكور[8].

يستخدم الحظر القائم على محرك البحث أيضًا من قبل الأفراد كجزء مما يسمى "بحق النسيان"، مع طلب حظر مليون عنوان URL عالمي في العامين المنصرمين (من مايو 2014 إلى يونيو 2016).

هامش جانبي:
الحظر القائم على أنظمة أساسية أخرى

في حين أن الحظر القائم على محرك البحث هو النو ع الأكثر شيوعًا من أنواع الحظر القائم على النظام الأساسي، غالبًا ما يتم اعتبار أنظمة أساسية أخرى ذات مجتمعات هائلة من المستخدمين لهذه التقنية. وتتضمن الأمثلة الشائعة لهذه الأنواع من الأنظمة الأساسية موقع Facebook (الذي يضم أكثر من 1.5 مليار مستخدم نشط شهريًا) وYouTube (مع أكثر من مليار مستخدم متفرد). وتعد محاولات استخدام التقنيات القائمة على الشبكة أو عنوان URL لحظر عناصر المحتوى الفردية، مثل بعض المقالات الإخبارية، صعبة للغاية. ونظرًا لعدم رغبتهم في أن ينظر إليهم كأنهم يحظرون موقع Facebook بأكمله(على سبيل المثال)، اقترحت السلطات المحلية العمل مع مقدمي الأنظمة الأساسية لتصفية أنواع محددة من المحتوى الذي يعتبرونه غير قانوني.

لا يُعرف عن فعالية الأنواع الأخرى للحظر القائم على النظام الأساسي أو نطاقها أو آثارها الجانبية سوى القليل جدًا، نظرًا لأن هذه التقنية لم يتم ملاحظتها بشكل واسع وعلى نحو موثوق في الأنظمة الأساسية الأخرى بخلاف محركات البحث. وفي الوقت الذي تحظر فيه الأنظمة الأساسية الرئيسية، مثل Facebook و YouTube وTwitter، أنواع معينة من المحتوى بوجه عام (مثل البرامج الضارة والمواد الإباحية) وتقدم موجزات محتوى مخصصة لمستخدميها، لا تتوفر المعلومات بشأن الحظر على المستوى المحلي.

6 البحث الآمن ميزة في محركات البحث الرئيسية، بما فيها محرك بحث Google وMicrosoft Bing وYahoo!، التي تحظر النتائج التي تحتوي على "صور غير مناسبة أو إباحية" من نتائج البحث.

7 https://www.google.com/transparencyreport/removals/government/?hl=en

8 https://www.google.com/transparencyreport/removals/copyright/?hl=en

حظر المحتوى القائم على نظام أسماء النطاقات (DNS)

يتفادى حظر المحتوى القائم على DNS واحدة من المشكلات التي تواجهها التقنيات الأخرى وهي: تأثير التكلفة والأداء على تصفية جميع حركات البيانات على الشبكة. وبدلاً من ذلك، يركز حظر المحتوى القائم على DNS على فحص استعلامات DNS والتحكم فيها.

مع حظر المحتوى القائم على DNS، يكون لمحلل DNS المتخصص (انظر الهامش الجانبي: نظرة عامة على DNS) وظيفتين: بالإضافة إلى إجراء عمليات بحث DNS، يتحقق المحلل من الأسماء في ضوء قائمة حظر. وعندما يحاول جهاز الكمبيوتر الخاص بالمستخدم استخدام اسم محظور، يُرجع الخادم الخاص معلومات غير صحيحة، مثل عنوان IP الخاص بالخادم الذي يعرض إشعارًا بحظر المحتوى. أو، قد يزعم الخادم أن الاسم غير موجود. ويتمثل تأثير هذا النوع من الحظر في إعاقة المستخدم من الوصول السهل إلى المحتوى باستخدام أسماء نطاق معينة.

كما هو الحال مع جميع تقنيات الحظر القائم على الشبكة، يعتبر حظر المحتوى القائم على DNS فعالًا فقط عندما يكون لدى المؤسسة المنفذة للحظر تحكمًا كاملاً على اتصال المستخدم النهائي بالشبكة. إذا كان بمقدور المستخدم تحديد اتصال مختلف، أو استخدام مجموعة مختلفة من خوادم DNS، فإن التقنية لن تؤثر عليه. فعلى سبيل المثال، عندما حظرت تركيا استعلامات DNS في 2012، غيّر المستخدمون أنظمتهم بحيث تستخدم خوادم DNS العامة المعروفة وتجنبوا الحظر. واستجابت السلطات التركية عن طريق قطع حركات البيانات إلى خدمة DNS الخاصة بشركة Google، ما تسبب في أضرار جانبية بالغة. ويحتاج حظر المحتوى القائم على DNS إلى جدران حماية أو أجهزة أخرى تستطيع أن تعترض جميع استعلامات DNS لخوادم DNS المخصصة المتوافقة مع الحظر أو تعيد توجيهها وإلا لن تكون فعالة على نحو كبير.

تُعتبر فعالية حظر المحتوى القائم على DNS مماثلة لفاعلية الحظر القائم على عناوين IP. يعتبر حظر المحتوى القائم على DNS أكثر فعالية بقدر طفيف لأن قائمة أسماء النطاق تكون أسهل في إبقائها محدثة وتكون أكثر دقة من قائمة بعناوين IP لمعظم أنواع حظر المحتوى. وبالرغم من ذلك، يكون أقل فعالية بقدر طفيف لأن تغيير أسماء النطاق يكون أبسط من تغيير عناوين IP، ما يجعله أيسر لكل من المستخدمين النهائيين وناشري المعلومات من حيث تجنب هذا النوع من الحظر.

يوجد شكل بديل من حظر المحتوى القائم على DNS وهو عندما يتم تسجيل أسماء النطاق أو إزالتها من DNS تمامًا. وتعد هذه الطريقة أكثر صعوبة للتحايل عليها، وأضرارها الجانبية محدودة بعض الشيء. وفي العديد من الحالات، يعتمد هذا النوع من الحظر على فعالية التعاون عبر الحدود، عندما يصدر طلب أو قرار محكمة من اختصاص قضائي مغاير للمكان الذي يعمل فيه السجل أو المسجل.

يحتوي حظر المحتوى القائم على DNS على عوائق مماثلة للحظر القائم على عنوان IP: قد يوجد محتوى محظور وآخر غير محظور في نفس الخادم بنفس الاسم (مثل "facebook.com")، ومع ذلك سيعم الحظر الجميع. وبالإضافة إلى ذلك، قد يسبب تعديل استجابات DNS مشكلات تقنية أخرى تتسبب في انقطاع خدمات صالحة أخرى[9].

يعتمد حظر المحتوى القائم على DNS أيضًا على المستخدم الذي يعمل حسب القواعد العادية للإنترنت واستخدام خدمة DNS القياسية لتحويل الأسماء إلى عناوين IP. ويمكن للمستخدمين الذين يتحكمون تحكمًا كاملاً في أجهزة الكمبيوتر الخاصة بهم والخبراء الفنيين إعادة تكوين هذه الأجهزة بحيث تتجنب خدمة DNS القياسية واستخدام البدائل أو الحصول على قائمة بتحويلات الأسماء إلى عناوين محفوظة محليًا.

هامش جانبي:
نظرة عامة على DNS

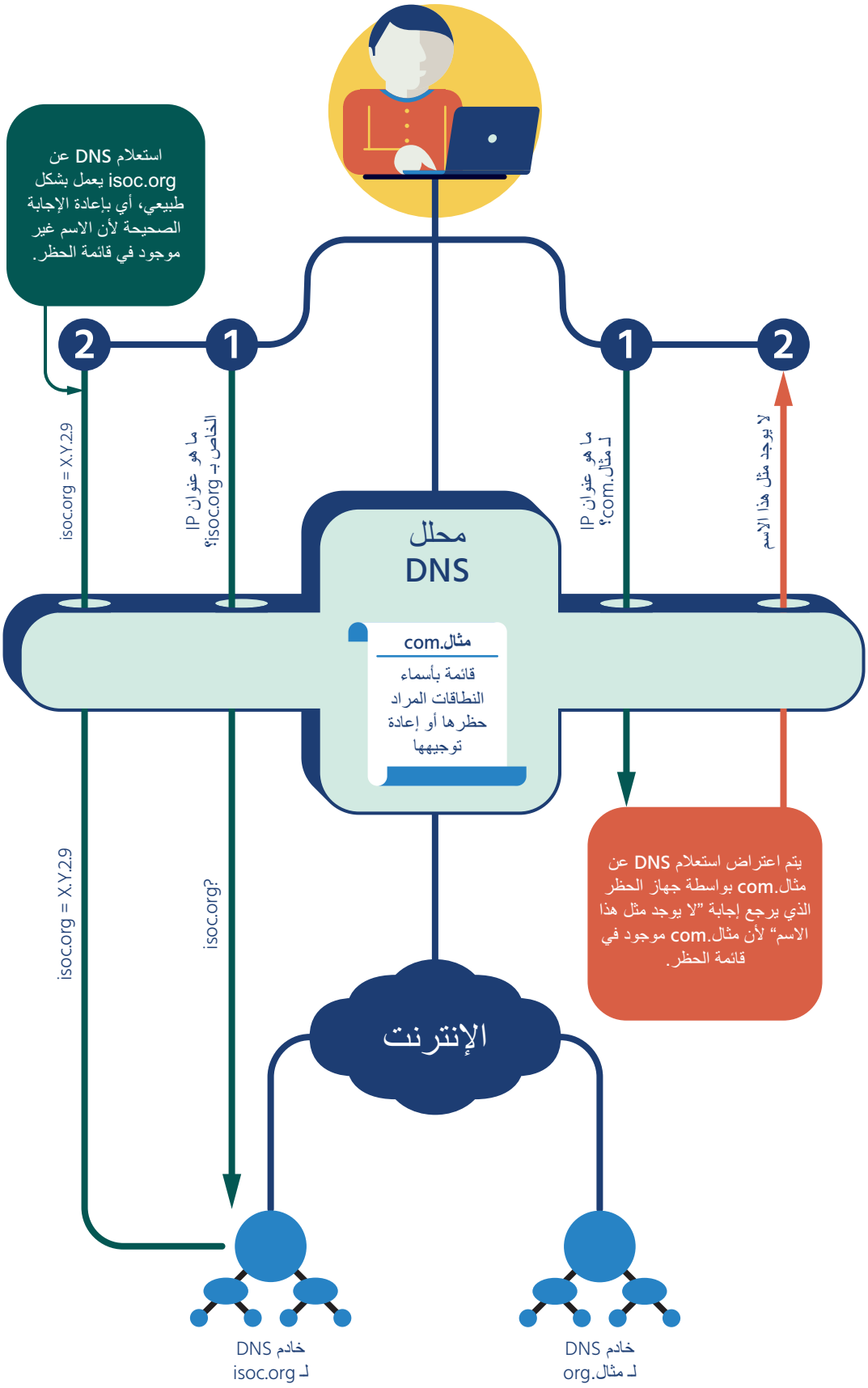
DNS هو نظام بسيط من حيث المفهوم يسمح بسلسلة من التسميات (مثل "www" و"isoc" و"org") يفصل بينها نقاط (اسم النطاق) ليتم البحث عنها في قاعدة بيانات موزعة عبر خوادم DNS متعددة. ويفضي البحث عن اسم النطاق إلى إجابة (على سبيل المثال، عنوان IP أو موقع ويب) أو تكون الإجابة أن الاسم غير موجود.

أما النوع الأكثر شيوعًا لبحث DNS فهو عناوين IP (بروتوكول الإنترنت). وهذا النوع من البحث يحدث كل مرة يكتب فيها المستخدم عنوان URL في مستعرض ويب، وذلك على سبيل المثال. وبشكل عادي، لا يُجري التطبيق الفردي (مثل مستعرض الويب) البحث الكامل، الذي يتضمن العديد من الخطوات. وبدلاً من ذلك، يستخدم التطبيق نظامًا وسيطًا يسمى "محلل" (نظرًا لأنه يحلل نتائج البحث عن اسم DNS)، الذي يتصفح قاعدة البيانات الموزعة لنظام DNS لاسترداد المعلومات المطلوبة.

في حظر المحتوى القائم على DNS، يتم تغيير التشغيل العادي للمحلل.

9 القراء المهتمون بمزيد من التفاصيل قد يرغبون في الرجوع إلى تقرير "آراء بشأن تصفية DNS" الخاص بمجتمع الإنترنت على https://www.internetsociety.org/internet-society-perspectives-domain-name-system-dns-filtering-0

الحظر القائم على DNS



في الحظر القائم على DNS، يحتوي جهاز الحظر على قائمة بأسماء DNS المراد حظرها.

لأن معظم اتصالات الإنترنت تتطلب ترجمة من اسم DNS إلى عنوان IP، فإن حظر الاستعلام وإرجاع إجابة خاطئة قد يثبط المستخدمين عن محاولة استرداد المحتوى المحظور أو الاتصال بالخدمات المحظورة بوسائل أخرى (مثل كتابة عنوان IP مباشرة).

ملخص حظر المحتوى

تقنيات حظر محتوى الإنترنت					
	الحظر القائم على عنوان IP والبروتوكول	الحظر القائم على الفحص العميق لحزم البيانات	الحظر القائم على عنوان URL	الحظر القائم على النظام الأساسي (وبالأخص محركات البحث)	الحظر القائم على DNS
عرض عام	يتم إدخال جهاز في الشبكة يقوم بالحظر اعتمادًا على عنوان IP و/أو التطبيق (على سبيل المثال، VPN)	يتم إدخال جهاز في الشبكة يقوم بالحظر اعتمادًا على الكلمات الأساسية و/أو محتوى آخر (على سبيل المثال، اسم الملف)	يتم إدخال جهاز في الشبكة يقوم باعتراض طلبات الويب ويفحص عناوين URL في ضوء قائمة حظر.	بالتعاون مع مقدمي التطبيق (مثل محركات البحث)، يتم تعديل المحتوى تبعًا للمتطلبات المحلية	في الشبكة أو مستوى ISP، يتم توجيه حركة بيانات DNS إلى خادم DNS معدل يستطيع حظر عمليات البحث لأسماء نطاقات معينة
هل هذه التقنية فعالة؟	بسبب سهولة تغيير عناوين IP ونقل المحتوى، **لا تعمل هذه التقنية بالمستوى المطلوب**. ولا تعمل بفعالية إلا إذا كان ناشر المعلومات لا يعمل بنشاط لتفادي الحظر.	عندما تكون المعلومات المحظورة سهلة التمييز، تكون فعالة للغاية وبالنسبة للحظر العام، (على سبيل المثال، "حظر محتوى البالغين") أو في مواجهة التشفير، تكون التقنية **غير فعالة إلى حد كبير**	هذه التقنية شائعة **وتعمل بفعالية عند حظر الوصول إلى فئات كاملة** من المعلومات. وتتسرب الصفحات جديدة والمواقع الصغيرة بسهولة، والأمر نفسه يسري على خوادم الويب المشفرة.	نظرًا لأنه لا يوجد احتكار في محركات البحث (على سبيل المثال) ولتغير تفضيلات المستهلكين باستمرار، **يعد هذا النوع من الحظر شكليًا إلى حد كبير ويعمل بشكل سيء**.	يتحايل ناشرو المحتوى والمستخدمون النهائيون على حظر DNS بسهولة. ولا يكون حظر DNS فعالًا إلا عندما يكون كل اسم يحتوي على قدر قليل جدًا من المحتوى، ويجب حظر هذا المحتوى بكامله. **ولكن الصعوبات التقنية والحظر المفرط وسهولة التحايل عليها يجعل منها تقنية غير فعالة.**
من يتأثر بهذه التقنية؟	أي شخص "خلف" الجهاز هو من يقع عليه التأثير.	أي شخص "خلف" الجهاز هو من يقع عليه التأثير.	المستخدمون "خلف" الجهاز، الذين يمكن الجهاز اعتراض أو تقييم حركات بيانات الويب لهم.	مستخدمو محركات البحث التي ثبتت الحظر	مستخدمو خادم DNS المعدل. يمكن إنفاذ ذلك على مستوى الشبكة أو مستوى مقدم الخدمة.
ما مدى تحديدها؟	**تؤثر على كافة المحتويات في أي خادم، سواء كان محتوى قانوني أو غير قانوني**. ويعمل هذا حتى في حال تشفير البيانات.	**تؤثر فقط على المحتوى الذي يطابق قواعد الحظر**. وتحتاج إلى وكلاء للعمل مع صفحات الويب المشفرة.	**تؤثر على صفحات الويب وعناصر الويب الفردية**. وتحتاج إلى وكلاء للعمل مع صفحات الويب المشفرة.	**تؤثر على صفحات وعناصر الويب الفردية**. عادة ما تُستخدم على مستوى URL الفردي.	**تؤثر على كافة المحتويات التي يقدمها اسم نطاق، سواء كانت قانونية أو غير قانونية**. ولا يمكن أن تُستخدم بفعالية لتوزيع المحتوى.
ما نوع هذه التقنية؟	تحظر المحتوى	تحظر المحتوى	تحظر المحتوى	تثبط الوصول وتحبطه	تثبط الوصول وتحبطه
ما هي الأضرار الجانبية الناجمة عن هذه التقنية؟	أي استهداف للخوادم الأكبر لديها معدل نتيجة إيجابية خاطئة ضخمة، ويحظر المحتوى غير القانوني والقانوني.	اعتمادًا على نوعية قواعد الحظر، يمكن أن يتراوح معدل النتيجة الإيجابية الخاطئة من منخفض جدًا إلى عال جدًا. فكتابة قواعد جيدة أمر صعب.	تعتمد تصفية عناوين URL في معظمها على الخدمات التجارية التي تصنف حركة البيانات. وبالنسبة للحظر الرئيسي، يمكن أن يكون ذلك محددًا تمامًا، ولكن معدل الأخطاء يكون مرتفعًا جدًا بالنسبة للحظر لأغراض خاصة.	يعد معدل النتيجة الإيجابية الخاطئة منخفضًا، لأن كل صفحة حظر تُطلب بشكل فردي. وتسبب مشكلة الطلبات غير المشروعة في حظر بعض المعلومات غير الملائمة.	أي استهداف لأسماء النطاقات المستخدمة من قبل خوادم أكبر لديه معدل نتيجة إيجابية خاطئة هائل، ويحظر المحتوى غير القانوني والقانوني. ويكون غير فعال عند استخدام شبكات توصيل المحتوى (أو يسبب مستوى عال للغاية من النتائج الإيجابية الخاطئة).
ما هي طرق الشائعة للتهرب منها؟	يمكن للناشرين تغيير عناوين IP أو ترحيل المحتوى أو استخدام شبكات توصيل المحتوى (CDN) للتحايل على هذه التقنية. ويتهرب مستخدمو VPN من خلال إخفاء عناوين IP.	تتهرب طبقات متعددة من التشفير بشكل فعال من هذا النوع من الحظر. وعندما تكون قواعد التصفية غير مكتوبة بشكل جيد، يمكن للتغييرات الصغيرة في النص تجاوز الحظر بسهولة.	تتهرب طبقات متعددة من التشفير بشكل فعال من هذا النوع من الحظر. وكثيرًا ما يكون استخدام طبقة التطبيقات غير القياسية تقنية تهرب فعالة.	يمكن للمستخدمين اختيار أنظمة أساسية بديلة، مثل محرك بحث مختلف، بسهولة شديدة.	يمكن للمستخدمين تجنب استخدام عمليات البحث عن DNS باستخدام الخدمات المحلية، أو يمكن إرسال استعلاماتهم إلى خادم عام غير معدل (عادة على الرغم من وجود VPN).
هل توجد آثار جانبية أو مسائل تقنية؟	إن الاحتفاظ بقوائم عناوين IP طويلة أمر صعب عرضة للخطأ، ويتطلب موارد كبيرة. وعادة ما تكون أجهزة الشبكة التي تقوم بهذا النوع من الحظر سريعة، لذا فإن المسائل المتعلقة بالأداء ليست شائعة.	تكون تكاليف أداء التصفية المدركة للمحتوى كبيرة وليست عملية في العديد من البيئات (بدون موارد هائلة). فعند استخدام الوكلاء، يمكن أن يتعرض أمن البيانات للخطر الشديد.	قد تؤدي تصفية عناوين URL إلى حدوث مشكلات في الأداء، مما يقلل من السرعة والموثوقية بشكل عام. فعند استخدام الوكلاء، يمكن أن يتعرض أمن البيانات للخطر الشديد.	تبلغ العديد من محركات البحث عن المعلومات "المتعلقة بالقمع"، والذي يخلق في حد ذاته سجلاً إلى المحتوى.	يتم اختراق أمن DNS عند نشر خادم معدل.

الخاتمة

فهم تقنيات الحظر المختلفة وتأثيراتها وآثارها الجانبية يعد ضروريًا لكل من صنّاع السياسة الذين يدرسون استخدام هذه التدابير، ومناصري الإنترنت والآخرين الذين يرغبون في التأثير على ممارسات حظر المحتوى.

جميع تقنيات الحظر تكون عرضة لعائقين رئيسيين:

1. **لا تحل المشكلة**

لا تزيل تقنيات المحتوى من الإنترنت ولا توقف النشاط غير القانوني ولا تلاحق المجرمين؛ فهي تضع ببساطة ستارًا أمام المحتوى. ويظل المحتوى الأساسي في موضعه.

2. **إلحاق أضرار إضافية جانبية**

تعاني كل تقنيات الحظر من فرط الحظر وقلة الحظر: أي الحظر أكثر مما هو مقصود، وفي نفس الوقت، الحظر أقل مما هو مقصود. وهي تتسبب أيضًا في أضرار أخرى للإنترنت بتعريض المستخدمين للخطر (لأنهم يحاولون الالتفاف على عمليات الحظر)، بتحجيم الشفافية والثقة في الإنترنت، وإبقاء الخدمات سرية والتطفل على خصوصية المستخدم. وهذه هي التكاليف التي يجب أخذها في الحسبان عند مناقشة الحظر.

التوصيات

يعتقد مجتمع الإنترنت أن الطريقة الأنسب لمنع المحتوى والأنشطة غير القانونية على الإنترنت هي مهاجمتهما في مصدرهما. ويعد استخدام عوامل التصفية لحظر الوصول إلى المحتوى عبر الإنترنت غير فعال، وعرضة لإحداث أضرار جانبية تؤثر على مستخدمي الإنترنت الصالحين.

نقترح استراتيجيتين رئيسيتين على صنّاع السياسة المعنيين بالمحتوى غير القانوني على الإنترنت:

1. **مهاجمة المشكلة من المصدر:** النهج الأقل ضررًا للإنترنت هو "مهاجمة" المحتوى والأنشطة غير القانونية في مصادرها. إن إزالة المحتوى غير القانوني من مصدره واتخاذ إجراء قانوني في حق الجناة ويتجنب التأثيرات السلبية للحظر ويكون بالغ الفعالية عند حذف المحتوى غير القانوني[10]. ويعد التعاون بين مختلف الاختصاصات القضائية وأصحاب المصلحة شرطًا أساسيًا للنجاح، نظرًا لأن المحتوى غير القانوني عبر الإنترنت يتجاوز الحدود المحلية والقانون المحلي.

هامش جانبي:
التحايل على حظر المحتوى

يجب على واضعي السياسات أن يضعوا في اعتبارهم نقطة مهمة عند النظر في حظر محتوى الإنترنت: يمكن تجاوز كل تقنيات الحظر التقني بواسطة أي مستخدم يمتلك الدوافع الكافية. وفي كثير من الحالات، هناك حاجة فقط إلى الحد الأدنى من العمل للتهرب من الحظر.

إذا تم حظر حركة المرور إلى مضيف أو اسم نطاق، يمكن استخدام أدوات مثل شبكات VPN لإخفاء حركة البيانات. وإذا تم فحص محتوى حركة البيانات، فيمكن تشفيره بحيث لا يفعّل آلية الحظر. وإذا تم إيقاف المحتوى، يمكن للمستخدمين الآخرين إعادة تحميله على خوادم أخرى. وإذا تم إزالة اسم النطاق المستخدم، فلا يزال بإمكان المستخدمين الوصول إلى المضيف إذا كانوا يعرفون عنوان IP، أو يمكنهم تحديد اسم نطاق جديد كبديل. وإذا كان محرك البحث يزيل النتائج، فهناك دائمًا محركات بحث أخرى.

المستخدمين النهائيين ليسوا الوحيدين الذين يستطيعون التهرب من الحظر. إذ قد يكون لدى ناشري المعلومات أيضًا العديد من الأساليب للتملص من تقنيات الحظر المختلفة. وإذا كان الناشر يعمل بجد بما فيه الكفاية لتوزيع المحتوى ونشره، فلا يمكن لأي تقنية حظر أن توقفه.

10 عندما تكون السلطة المحلية في نفس الاختصاص القضائي الكائن فيه مستهلك المحتوى، فإن إزالة المحتوى غير القانوني من المصدر تبدو طريقة سهلة لتفادي تعقيدات وتكلفة الإجراءات العابرة للحدود. ونقر أن إزالة المحتوى من المصدر يمثّل تحديًا في سياق الإنترنت عبر الحدود، حيث قد يكون مزودو المحتوى ومستهلكوه موجودين في اختصاصات قضائية مختلفة تخضع لقوانين مختلفة. وبرغم ذلك، نعتبر أن ذلك ينبغي ألا يكون سببًا لعدم تحديد المزيد من الحلول الفعالة التي لا تسبب ضررًا للإنترنت.

2. **إعطاء الأولوية للنهج البديلة واستخدامها:** تبعًا للظروف، يمكن أن تكون النهج المختلفة فعالة إلى حد كبير. على سبيل المثال

- التعاون الفعال بين مزودي الخدمة وسلطات إنفاذ القانون والسلطات المحلية قد يقدم وسائل إضافية لمساعدة ضحايا المحتوى غير القانوني، واتخاذ إجراء قانوني في حق الجناة[11].
- خلق مناخ من الثقة حيث يتلقى المستخدمون معلومات بشأن ما هو النشاط القانوني أو غير القانوني الذي يمكنه تحسين المراقبة الذاتية.
- في بعض الحالات (على سبيل المثال، المراقبة الأبوية)، يمكن أن يكون تشجيع المستخدمين على استخدام عوامل التصفية في أجهزتهم، بناء على موافقتهم، فعالًا وأقل إضرارًا بالإنترنت.
- على أساس طوعي أو قانوني، يمكن لبعض مواقع الويب (على سبيل المثال، مواقع المقامرة) استخدام الموقع الجغرافي لمنع الوصول من البلدان حيث تكون خدماتهم غير مسموح بها.

تقليل الآثار السلبية

تحتوي كافة تقنيات حظر المحتوى على أوجه قصور خطيرة، لا سيما في سياق الحظر القائم على اعتبارات السياسة العامة. وتتصرف جميع التقنيات بشكل سيء كما يمكن التحايل عليها. ولهذا السبب، وللأسباب المذكورة من قبل، فإننا نحذر من حظر المحتوى.

وبرغم ذلك، فإن هذه التقنيات لا تزال تستخدم. وإدراكًا لهذه الحقيقة، نقدم الإرشادات الخاصة التالية للحد من الآثار السلبية:

أ. **استبعاد جميع خيارات عدم الحظر:** أولاً وقبل كل شيء، استنفاد جميع الخيارات العملية لمعالجة المحتوى من المصدر، أو أي وسائل أخرى للحظر. ويجب عدم تطبيق حظر المحتوى نظرًا لسهولته.

ب. **التحلي بالشفافية:** يجب أن يكون هناك شفافية عن الحظر إلى جانب الأهداف الكامنة والسياسات. ويجب أن تتأكد السلطات المحلية من أن المستخدمين المتضررين لديهم الفرصة للإعراب عن القلق حيال الآثار السلبية بشأن حقوقهم ومصالحهم وفرصهم.

ج. **الوضع في الاعتبار المسؤولية تجاه الإنترنت:** يجب أن يكون الطرف المطبق للحظر على دراية بأنه يتحمل قدرًا من مسؤولية عدم التسبب في الإضرار باستقرار وأمان ومرونة الإنترنت تجاه النظام ككل. وتؤثر تقنيات الحظر بصورة عكسية على الطريقة التي يدار ويعمل بها الإنترنت بوجه العموم. وأحيانًا يكون الضرر مباشرًا وأحيانًا يكون غير مباشر. فعلى سبيل المثال، قد يتسبب المستخدمون الذين يتحايلون على الحظر في مشكلات أو تهديد أمنهم الشخصي.

د. **التفكير على المستوى العالمي، والتصرف على المستوى المحلي:** يمكن أن يكون للحظر والتصفية المحليتين آثارًا عالمية: لكن بوجه عام، سوف يقلل حظر المحتوى على المستوى المحلي قدر الإمكان من الأثر العالمي. وبشكل مثالي، يعد الحظر عند النقطة النهائية للمستخدم أكثر فعالية ويقلل من الضرر الجانبي.

و. **إشراك أصحاب المصلحة:** يجب أن تشمل عملية وضع السياسة وتنفيذها مجموعة كبيرة من أصحاب المصلحة بما في ذلك الحقوق التقنية والاقتصادية وحقوق المستهلك والمتخصصين الآخرين لضمان اتخاذ الخطوات المناسبة للتقليل من الآثار الجانبية السلبية.

ز. **إبقاء الأمر مؤقتًا:** يجب أن يكون أي إجراء حظر مؤقتًا. ويجب أن تتم إزالتها بمجرد زوال سبب الحظر. إذ يشيع نقل المحتوى القانوني تفاديًا لإجراءات الحظر، وبالرغم من ذلك غالبًا ما تظل الإجراءات في موضعها بعد نقل المحتوى بوقت طويل.

ح. **اتباع الإجراءات القانونية الواجبة:** يجب أن يدعم القانون أي أمر حظر لمحتوى غير قانوني، وأن يتم مراجعته بشكل مستقل وأن يتم استهدافه بإحكام لتحقيق هدف شرعي. ويجب إعطاء الأولوية للوسائل المتاحة الأقل تقييداً للتعامل مع النشاط غير القانوني. ويجب ألا يكون مزودو خدمات الإنترنت أو وسطاء الإنترنت الآخرين وكلاء إنفاذ قانون بحكم الواقع: ويجب ألا يطلب منهم تحديد مشروعية السلوك أو المحتوى من عدمها.

11 على سبيل المثال، يمكن أن تستخدم الشراكات مع الجهات الممولة لتحديد المعاملات غير القانونية والحد منها.

مسرد

CDN

شبكة توصيل المحتوى أو شبكة توزيع المحتوى (CDN) هي شبكة موزعة عالمية من الخوادم الوكيلة المنتشرة في مراكز البيانات المتعددة. ويكمن الهدف من شبكة توصيل المحتوى في تقديم محتوى للمستخدمين النهائيين بوفرة وأداء عاليَيْن. وتقدم شبكات توصيل المحتوى جزءًا كبيرًا من محتوى الإنترنت في الوقت الحالي، بما في ذلك كائنات الويب (النص والرسومات والبرامج النصية)، والكائنات القابلة للتنزيل (ملفات الوسائط والبرامج والمستندات)، والتطبيقات (التجارة الإلكترونية والبوابات)، ووسائط البث المباشر، ووسائط البث حسب الطلب، والشبكات الاجتماعية.
(https://en.wikipedia.org/wiki/Content_delivery_network)

محتوى

في سياق هذه الوثيقة، نستخدم "المحتوى" بوجه عام لوصف المعلومات التي يتم العثور عليها على الإنترنت. ويمكن أن يكون هذا المحتوى مستند كامل أو فقرة من نص أو صورة أو ملف فيديو أو حتى ملف صوت (مثل البودكاست). ويمكن أن يكون المحتوى في صفحات الويب المعروضة في مستعرض، أو يمكن الوصول إليه من خلال أدوات أكثر تخصصًا كتطبيق مخصص.

DNS

نظام اسم النطاق (DNS) هو نظام تسمية هرمي مركزي لأجهزة الكمبيوتر أو الخدمات أو أي موارد أخرى مرتبطة بالإنترنت أو شبكة خاصة. وهو يربط المعلومات المتنوعة بأسماء النطاق المعينة لكل كيان مشارك. والأهم من ذلك، أنه يترجم بسهولة أسماء النطاقات المحفوظة إلى عناوين IP الرقمية اللازمة لتحديد وتعريف خدمات الكمبيوتر والأجهزة مع بروتوكولات الشبكة الأساسية. ومن خلال تقديم خدمة دليل موزعة على نطاق العالم، يعتبر نظام أسماء النطاقات عنصرًا أساسيًا في وظائف الإنترنت يُستخدم منذ عام 1985.
(https://en.wikipedia.org/wiki/Domain_Name_System)

DPI

الفحص العميق لحزمالبيانات (DPI) هو شكل من أشكال تصفية حزم شبكة الحاسوب الذي يدرس جزء البيانات (وربما رأس الصفحة أيضًا) من الحزمة عند مرورها بنقطة فحص، أو البحث عن عدم الامتثال للبروتوكول، أو الفيروسات، أو البريد العشوائي، أو عمليات الاقتحام، أو معايير محددة لتقرير ما إذا كانت الحزمة قد تمر أو يتعين معالجتها بطريقة أخرى، بما في ذلك التخلص من الحزمة.
(https://en.wikipedia.org/wiki/Deep_packet_inspection)

غير قانوني

في سياق هذا البحث، نستخدم كلمة "غير قانوني" لوصف المحتوى المحظور في سياق وطني مهما كان السبب. وقد يكون هذا المحتوى غير قانوني لأنه يمثل انتهاكًا لحقوق التأليف والنشر (أو أي نوع آخر من الملكية الفكرية)، مثل الأفلام المقرصنة. ويمكن أن يكون المحتوى غير قانوني لأنه غير مقبول لأسباب أخلاقية، مثل الفحش أو المواد الإباحية المتعلقة بالأطفال. ويمكن أن يكون المحتوى غير قانوني لأن السلطات الوطنية ترغب في قمعه أو تجده هجوميًا، مثل الرسوم المتحركة التي تصور رئيس البلاد بطريقة غير محبذة. وقد يكون المحتوى غير قانوني في أحد الاختصاصات القضائية وقانونيًا تمامًا في اختصاص قضائي آخر. وقد يكون المحتوى غير قانوني في سياق (مثل الكوميديا غير اللائقة، عندما يشاهدها الأطفال) ويكون قانونيًا تمامًا في سياق آخر (كما هو الحال عندما يشاهدها البالغون)، حتى داخل الاختصاص القضائي نفسه.

عنوان IP

عنوان IP (اختصار لعنوان بروتوكول الإنترنت) عبارة عن معرف معين لكل كمبيوتر وأجهزة أخرى (مثل الطابعة أو الموجه أو جهاز الجوال أو ما إلى ذلك) متصلة بالإنترنت. ويتم استخدامه لتحديد وتعريف العقدة في الاتصالات مع العقد الأخرى على الشبكة.
(https://en.wikipedia.org/wiki/IP_address)

النتيجة السلبية الخاطئة تحدث النتيجة السلبية الخاطئة عندما لا يتم حظر المحتوى، رغم أنه كان ينبغي حظره. فعلى سبيل المثال، إذا تم حظر صيدليات غير قانونية، قد لا يتم حظر صيدلية جديدة غير قانونية إذا لم يتم إضافة الخادم إلى قائمة الحظر بعد. وهذا ما يسمى "النتيجة السلبية الخاطئة".

النتيجة الإيجابية الخاطئة تحدث النتيجة الإيجابية الخاطئة عندما يتم حظر بعض المحتويات التي يُقصد حظرها. فعلى سبيل المثال، إذا تم حظر مواد إباحية، قد يتم حظر معلومات حول طهي صدور الدجاج إذا كان الحظر يستخدم بحث بكلمات رئيسية ضعيفة الصياغة. وهذا ما يسمى "النتيجة الإيجابية الخاطئة".

TLS/SSL بروتوكول أمان طبقة النقل (TLS) وسابقه، بروتوكول طبقة المنافذ الآمنة (SSL)، غالبًا ما يشار إلى كلاهما باسم "SSL"، وهما عبارة عن بروتوكولات تشفير توفر أمن الاتصالات عبر شبكة الكمبيوتر. ويتم استخدام العديد من الإصدارات من البروتوكولات بشكل واسع في التطبيقات مثل تصفح الإنترنت، والبريد الإلكتروني، والفاكس عبر الإنترنت، والرسائل الفورية، ونقل الصوت عبر IP (VoIP). وتستخدم مواقع الويب بروتوكول أمان طبقة النقل (TLS) لتأمين جميع الاتصالات بين خوادمها ومتصفحات الويب. ويهدف بروتوكول أمان طبقة النقل (TLS) في المقام الأول إلى توفير الخصوصية وسلامة البيانات بين تطبيقين حاسوبيين متصلين.
(https://en.wikipedia.org/wiki/Transport_Layer_Security)

URL يعتبر محدد مواقع الويب (URL)، والذي كان يطلق عليه عادة عنوان الويب، مرجعًا لمورد ويب يحدد موقعه في الشبكة وآلية لاسترداده. وعادة ما تكون عناوين URL هي صفحات الويب المرجعية (https)، ولكنها تستخدم أيضًا لنقل الملفات (ftp) والبريد الإلكتروني (mailto) والوصول إلى قاعدة البيانات (JDBC) والعديد من التطبيقات الأخرى. وتعرض معظم متصفحات الويب عنوان URL لصفحة الويب أعلى الصفحة في شريط العنوان. ويمكن أن يكون عنوان URL النموذجي هوhttps://www.مثال.com/index.html، والذي يشير إلى البروتوكول (https)، واسم المضيف (www.مثال.com)، واسم الملف (index.html).
(https://en.wikipedia.org/wiki/Uniform_Resource_Locator)

VPN تمد الشبكة الخاصة الافتراضية (VPN) شبكة خاصة عبر شبكة عامة، مثل الإنترنت. فهي تمكن المستخدمين من إرسال واستقبال البيانات عبر الشبكات المشتركة أو العامة كما لو كانت أجهزتها الحاسوبية مرتبطة مباشرة بالشبكة الخاصة. ويمكن للتطبيقات التي تعمل عبر الشبكة الخاصة الافتراضية أن تستفيد من وظائف الشبكة الخاصة وأمنها وإدارتها.
(https://en.wikipedia.org/wiki/Virtual_private_network)

لمزيدٍ من الاطلاع

قد تكون المنشورات التالية ذات أهمية للقراء الذين يبحثون عن معلومات إضافيةحول هذا الموضوع.

المستندات التقنية لفرقة العمل المعنية بهندسة الإنترنت

"استطلاع تقنيات المراقبة العالمية" (IETF draft draft-hall-censorship-tech-04)
https://tools.ietf.org/html/draft-hall-censorship-tech-04

"الاعتبارات التقنية لحظر خدمات الإنترنت وتصفيتها" (RFC 7754)
https://tools.ietf.org/html/rfc7754

مستندات السياسة والاستطلاع والمعلومات الأساسية

"تصفية المحتوى غير القانوني على الإنترنت وحظره وإزالته"، المجلس الأوروبي، 2015.
http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet

"حرية التعبير دون تصفية: كيف يؤثر الحظر والتصفية على حرية التعبير"، المقالة 19، 2016.
https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf

"حرية الإنترنت 2016"، فريدوم هاوس، نوفمبر 2016.
https://freedomhouse.org/report/freedom-net/freedom-net-2016

"آراء جمعية الإنترنت بشأن تصفية نظام اسم النطاق (DNS)"، جمعية الإنترنت، 2012.
https://www.internetsociety.org/sites/default/files/Perspectives%20on%20Domain%20Name%20System%20Filtering-en.pdf

"حياد الشبكة"، جمعية الإنترنت، 2015.
http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-NetworkNeutrality-20151030.pdf

"آراء حول استجابات السياسة لانتهاك حقوق النشر على الإنترنت"، جمعية الإنترنت، 2011.
https://www.internetsociety.org/sites/default/files/bp-copyrightpolicy-20110220-en-1.pdf

شكر وتقدير

تعرب جمعية الإنترنت عن امتنانها لمساعدة جويل سنايدر من أوبوس وان في إعداد هذا البحث.

وقد أشرف على التقرير نيكولاس سيدلر وأندريه روباشيفسكي من جمعية الإنترنت.

واستفاد البحث من المراجعات والتعليقات والدعم من مجموعة من موظفي جمعية الإنترنت وهم: كونستانس بوميلار، سالي وينتورث، أولاف كولكمان، كارل غانبرغ، كريستين رونيغار، كونستانتينوس كومايتيس، ليا كيسلينغ، جويس دوغنيز، كيفن كريمر، باستيان كويست، كيفن تشيج، دان يورك، راكيل غاتو.

شكر خاص لفريق الاتصالات بجمعية الإنترنت لتشكيل الجانب المرئي من هذا البحث وتعزيز عملية إصداره وهم: جيمس وود، بيث غومبالا، ليا كيسلنغ، أليساندرا ديسانتيلانا.

وأخيرًا وليس آخرًا، تحسن البحث بشكل كبير بفضل مدخلات مجموعة متنوعة من أعضاء جمعية الإنترنت وأعضاء المنظمة وأعضاء فرديين بالإضافة إلى مدخلات مجلس أمناء جمعية الإنترنت الحالي والسابق.

Internet Society

internetsociety.org

Galerie Jean-Malbuisson 15,
CH–1204 Geneva, Switzerland
+41 22 807 1444 هاتف

1775 Wiehle Avenue, Suite 201
Reston, Virginia 20190, U.S.A.
+1 703 439 2120 هاتف