The State of Internet Censorship in Egypt

A research study by:
Open Observatory of Network Interference (OONI)
Association for Freedom of Thought and Expression (AFTE)

2nd July 2018

حالة الرقابة على الإنترنت في مصر

دراسة بحثية قام بها المرصد المفتوح لاعتراض الشبكات (OONI) ومؤسسة حرية الفكر والتعبير (AFTE).

2 يوليو 2018

قائمة المحتويات

أعد التقرير

ليونيد ايفدوكيموف (OONI)، ماريا زينو (OONI) ، محمد الطاهر (AFTE)، حسن الأزهري (AFTE)، سارة محسن (AFTE)

البلد: **مصر**

مزودو خدمة الإنترنت محل الاختبار: تم جمع القياسات من فودافون مصر (AS36935)، لينك مصر (AS24863)، تي إي داتا (AS8452) ونور (AS20928)

اختبارات المرصد المفتوح لاعتراض الشبكات: Web Connectivity test, HTTP Invalid Request Line test, HTTP Header Field Manipulation test, WhatsApp test, Facebook Messenger test, Telegram test,

Vanilla Tor test, Tor Bridge Reachability test

فترة الاختبار / التحليل: من يناير 2017 إلى مايو 2018

أساليب الرقابة: تقنية الفحص العميق للحزم (DPI) المستخدمة لإعاقة الاتصال (فشل استجابة بروتوكول نقل النص التشعبي الفائق HTTP) و التلاعب بنظام أسماء النطاقات (DNS) وحقن بروتوكول التحكم بالنقل (TCP)

أبرز النتائج

يبدو أن الرقابة على الإنترنت في مصر خلال العام الماضي، أصبحت أكثر ديناميكية وانتشارًا.

كما يبدو أن مزودي خدمة الإنترنت لا يقومون بحجب المواقع مباشرة، لكنهم يُعيقون الاتصال من خلال استخدام أجهزة الفحص العميق للحزم [Deep Packet Inspection (DPI)] ، أيضا يبدو أنهم يتدخلون في حركة مرور البيانات المُعماة التي تمر عبر بروتوكول طبقة المنافذ الآمنة (SSL) بين نقطة اتصال كلاودفير (Cloudlflare) في القاهرة وبين خواديم المواقع (الموجودة خارج مصر).

تشكل المواقع الإعلامية النسبة الأكبر بين المواقع التي وجدنا أنها محجوبة. حيث يبدو أن الحجب مفروض على أكثر من 100 رابط يخص مواقع ذات طابع إخباري، رغم أن السلطات المصرية أعلنت حجب21 موقعًا إخباريًا فقط. كما وُجد أن العديد من المواقع الوب الخاصة بحقوق الإنسان والمدونات التي تُقدّم النقد السياسي، قد تعرضت للحجب هي الأخرى.

تجاوز الرقابة على الإنترنت في مصر قد يمثل تحديًا. **يبدو أن مقدمي خدمات الإنترنت** المصريين ينفّذون تكتيكات الدفاع في العمق (defense in depth) لتصفية الشبكات، كما يشير حجب العديد من مواقع أدوات تجاوز الحجب. كما يبدو أنهم يمنعون الوصول إلى شبكة تور (Tor)، وفي بعض الحالات جسور تور. و من أجل حجب موقع حزب سياسي (حزب الحرية والعدالة في مصر)، يستخدم مقدمو خدمات الإنترنت صندوقين وسيطين مختلفين (middleboxes)، مما يضيف طبقات إضافية من الرقابة ويجعل تجاوز الحجب أكثر صعوبة.

يبدو أن مزودي خدمة الإنترنت المصريين يقومون بحملة إعلانية (Ad campaign). في عام 2016، وجدنا أن مزودي خدمات الإنترنت يستخدمون أجهزة الفحص العميق للحزم (DPI) لمراقبة روابط(HTTP) غير المُعماة وإعادة توجيهها إلى محتوى مدر للدخل، مثل الإعلانات بالعمولة (affiliate ads)، يشير تحليلنا لقياسات OONI التي تم جمعها من مصر خلال العام الماضي بقوة إلى أن هذه الحملة مستمرة حتى مارس 2018 (على الأقل). وقد تأثرت بذلك مجموعة واسعة من أنواع المواقع المختلفة، بما في ذلك المواقع الإخبارية ومواقع حقوق الإنسان ومواقع مجموعات الميم، ومواقع الأمم المتحدة (un.org و ohchr.org)

مقدمة

هذه الدراسة جزء من جهد مستمر لتحليل الرقابة على الإنترنت في مصر وفي أكثر من 200 دولة حول العالم.

تعاون المرصد المفتوح لاعتراض الشبكات (OONI) ومؤسسة حرية الفكر والتعبير في مصر (AFTE) في دراسة بحثية

مشتركة لتحليل الرقابة على الإنترنت في مصر من خلال جمع وتحليل قياسات الشبكة. الهدف من دراستنا هو توثيق الرقابة على الإنترنت في مصر من خلال تحليل معطيات البيانات.

توفر الأقسام التالية من هذا التقرير معلومات أكثر تفصيلاً عن مستويات انتشار الإنترنت، ومستويات اختراق الإنترنت في مصر، والبيئة القانونية الخاصة بالرقابة وحرية التعبير، فضلاً عن حالات الرقابة التي سبق رصدها في البلاد. الجزء المتبقي من التقرير يوثّق منهجية ونتائج هذه الدراسة.

خلفية

نطاق انتشار واستخدام الإنترنت

ارتفع معدل استخدام الإنترنت في مصر خلال السنوات الأخيرة. وفقا لوزارة الاتصالات وتكنولوجيا المعلومات، بلغ معدل انتشار الإنترنت في مصر 41.2 ٪ بحلول نهاية عام 2017. ويعتمد المستخدمون إلى حد كبير على اشتراكات الإنترنت عبر الهاتف المحمول، كما هو موضح في الجدول التالي.

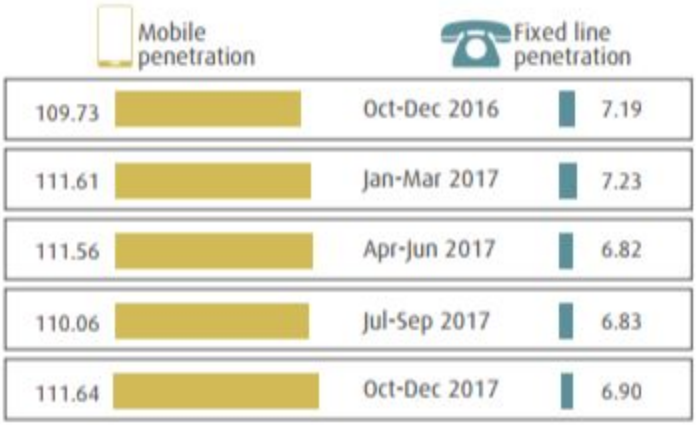
Indicators in Brief

Data item	Unit	Oct-Dec 2016	Jul-Sep2017	Oct-Dec 2017	Quarterly Growth Rate(%)	Annual Growth Rate(%)
ICT Sector:Infrastructure Indicators						
Mobile Subscriptions *	Million	97.79	99.40	101.27	1.88	3.56
Mobile Penetration **	%	109.73	110.06	111.64	1.58	1.91
Fixed Line Subscriptions	Million	6.12	6.54	6.60	1.02	7.95
Fixed Line Penetration **	%	7.19	6.83	6.90	0.07	-0.29
Mobile Internet Subscriptions	Million	28.65	32.76	32.79	0.09	14.45
USB Modem Subscriptions	Million	3.28	3.27	3.26	-0.30	-0.52
ADSL Subscribers	Million	4.44	4.95	5.20	4.94	17.1
International Internet Bandwidth	Gbps	1,134.25	1,406.12	1,536.12	9.25	35.43
Number of Post Offices	Post office	3931	3944	3946	0.05	0.38
ICT Sector's Role in Development						
Capacity Building Program Provided by ITIDA	Thousand Graduates	20.29	21.65	21.90	1.15	7.93

* Not including data of the fourth mobile service provider company (WE).
* * Growth rates are calculated as the difference between penetration rates in different time intervals.

المصدر: وزارة الاتصالات وتكنولوجيا المعلومات في جمهورية مصر العربية، نشرة مؤشرات تكنولوجيا المعلومات والاتصالات: ديسمبر 2017 (الإصدار ربع السنوي)
http://www.mcit.gov.eg/Upcont/Documents/Publications_142018000_EN_ICT_Indicators_Quarterly_Bullet in_Q4.pdf

بحلول نهاية عام 2017، استخدم معظم المصريين الإنترنت عبر هواتفهم الذكية، بينما اقتصرت اشتراكات الخطوط الثابتة على 6.9٪ فقط. خلال العام الماضي، أصبح هناك انخفاض ملحوظ في استخدام الخطوط الثابتة وارتفاع في استخدام المحمول، مما يوحي بأن المصريين سيواصلون الدخول على الإنترنت في المقام الأول باستخدام شبكات المحمول.



المصدر: وزارة الاتصالات وتكنولوجيا المعلومات، جمهورية مصر العربية ، نشرة مؤشرات تكنولوجيا المعلومات والاتصالات: ديسمبر 2017 (الإصدار ربع السنوي)
http://www.mcit.gov.eg/Upcont/Documents/Publications_142018000_EN_ICT_Indicators_Quarterly_Bulletin_Q4.pdf

لدى مصر الكثير من مقدمي خدمة الإنترنت (ISPs) ، ينظمهم الجهاز القومي لتنظيم الاتصالات(NTRA) وتتمتع شركة فودافون مصر بأكبر حصة (40.5٪) في سوق الهاتف المحمول المصري، لكن الشركة المصرية للاتصالات المملوكة للدولة تمتلك 45% من أسهم شركة فودافون مصر. تمتلك شركة أورانج مصر (المملوكة لشركة فرنسية) حصة قدرها 33٪ في سوق الهاتف المحمول، في حين تمتلك شركة اتصالات مصر (التي تملكها شركة إماراتية) حصة قدرها 24٪. أما بالنسبة لسوق النطاق العريض (bandwidth) للخطوط الثابتة، فتسيطر الشركة المصرية للاتصالات على 75٪ من سوق الـ ADSL.

بالإضافة إلى امتلاكها حصة كبيرة في فودافون مصر، تمتلك المصرية للاتصالات أيضًا كل البنية التحتية للاتصالات في مصر. فتؤجر التراخيص لمقدمي خدمة الإنترنت الرئيسيين في مصر - مثل نور، اتصالات مصر، وفودافون مصر - الذين يعيدون بيع النطاق العريض إلى مزودي خدمة الإنترنت الأصغر. ونتيجة لذلك، فإن البنية التحتية للإنترنت في مصر مركزية تمامًا.

البيئة القانونية

يتضمّن الدستور المصري عدة نصوص لحماية حرية الصحافة وحرية التعبير بشكل عام. ومع ذلك، يمكن تقييد هذه الأحكام في ظل ظروف معينة وبموجب قوانين مصرية مختلفة.

أحكام دستورية

يضمن الدستور المصري لعام 2014 الوصول إلى المعلومات، ويحمي حرية الصحافة ويحد من الرقابة. وفقا للمادة 57 من الدستور:

"تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك".

و تضمن المادة 68 من الدستور الحق في الوصول إلى المعلومات والوثائق الرسمية. وبشكل أكثر تحديدًا، تنص على ما يلي:

"المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب، والإفصاح عنها من مصادرها المختلفة، حق تكفله الدولة لكل مواطن، وتلتزم الدولة بتوفيرها وإتاحتها للمواطنين بشفافية، وينظم القانون ضوابط الحصول عليها وإتاحتها وسريتها، وقواعد إيداعها وحفظها، والتظلم من رفض إعطائها، كما يحدد عقوبة حجب المعلومات أو إعطاء معلومات مغلوطة عمداً".

استناداً إلى هذه المادة، فإن السلطات في مصري تلتزم بالكشف عن القرارات القضائية أو الإدارية المتعلقة بالرقابة. المادة 71 من الدستور تحمي حرية الصحافة وتحجب الرقابة على وسائل الإعلام (رغم أنه قد يسمح بها أثناء الحرب أو في أوقات التعبئة العامة):

"يحجب بأي وجه فرض رقابة على الصحف ووسائل الإعلام المصرية أو مصادرتها أو وقفها أو إغلاقها. ويجوز استثناء فرض رقابة محددة عليها في زَمن الحرب أو التعبئة العامة.

قانون الطوارئ

خلال حالة الطوارئ، يتم تعليق الحقوق الدستورية. و يسمح قانون الطوارئ المصري للحكومة باعتراض ومراقبة جميع الاتصالات وفرض الرقابة ومصادرة المنشورات.

وبموجب المادة 3 من هذا القانون، يمكن للسلطات أن تراقب الرسائل والصحف والمطبوعات والإصدارات والرسومات وجميع وسائل التعبير الأخرى قبل نشرها. كما أنهم مخولون بمراقبة ومصادرة هذه المواد وإغلاق الأماكن التي تطبع فيها هذه المطبوعات (مثل مكاتب الصحف). يمكن أن تُستخدم المادة 3 من قانون الطوارئ في مصر لتبرير حجب المواقع.

عاشت مصر في حالة طوارئ منذ عام 1958 (عندما صدر قانون الطوارئ لأول مرة)، باستثناء بعض الفترات القصيرة التي رفُعت فيها. في السنوات الأخيرة ، منذ يناير 2011، استمرت أطول فترة بدون حالة الطوارئ لمدة 13 شهراً، من يوليو 2012 إلى أغسطس 2013 . خلال العقود الماضية، كانت مصر تقريباً في حالة الطوارئ دائما من خلال استمرار إصدار القرارات التي تمددها. وفي الآونة الأخيرة، أعلنت الحكومة المصرية حالة الطوارئ في أبريل 2017، في أعقاب تفجيرين لكنيستين أدى إلى مقتل 44 شخصًا على الأقل. بعد ذلك بعام، في أبريل 2018، وافق مجلس النواب المصري على قرار أصدره الرئيس عبد الفتاح السيسي، لتمديد حالة الطوارئ لمدة ثلاثة أشهر أخرى.

قانون مكافحة الإرهاب

قبل ثلاث سنوات، في عام 2015، تبنت مصر قانونًا لمكافحة الإرهاب يشمل فرض غرامة على نشر تقارير تتناقض مع الروايات الرسمية عن هجمات المسلحين. وقد جادل منتقدو القانون بأنه من الممكن استخدام ذلك لإغلاق الصحف الصغيرة وردع الصحف الأكبر من تغطية الهجمات والعمليات ضد المقاتلين المسلحين.

بموجب المادة 29 من هذا القانون، يُسمح للنائب العام (أو سلطة التحقيق ذات الصلة) بحجب مواقع الإنترنت التي ترتكب جرائم جنائية، مثل التحريض على العنف أو نشر رسائل إرهابية.

قانون تنظيم الاتصالات

تتم إدارة الاتصالات في مصر مركزيا، مما يمكِّن من فرض رقابة مركزية على الإنترنت.

تسمح المادة 67 من قانون تنظيم الاتصالات في مصر للسلطات بإدارة جميع خدمات وشبكات الاتصالات من جميع المشغلين ومقدمي الخدمات في حالة الكوارث البيئية، أو التعبئة العامة، أو من أجل الحفاظ على الأمن القومي. في مثل هذه الحالات، قد يمكّن هذا القانون السلطات من تطبيق الرقابة على الإنترنت بطريقة مركزية. , وفقا لمؤسسة حرية الفكر والتعبير، أشارت السلطات المصرية إلى هذا القانون للرقابة على وقطع الاتصالات وخدمات الإنترنت خلال الثورة المصرية في يناير 2011 بحجة اعتبارات الأمن القومي.

وتمديدًا للمادة 67، تهدف المادة 68 من القانون إلى إعفاء مقدمي الخدمات من نطاق المسؤولية وحتى تعويضهم عن أي أضرار قد تحدث نتيجة لإدارة الحكومة للشبكات. بالإضافة لذلك، فقد وافقت لجنة الاتصالات البرلمانية المصرية مؤخراً على المادة 31 من مشروع قانون الجريمة الإكترونية. تهدف هذه المادة إلى معاقبة مقدمي خدمة الإنترنت الذين يمتنعون عن حجب المواقع التي "تهدد الأمن القومي" وفقًا لأوامر المحكمة.

قانون جرائم الإنترنت

وافق البرلمان المصري مؤخرًا على قانون الجرائم الإلكترونية.

تخول المادة 7 من القانون لسلطة التحقيق صلاحية حجب المواقع إذا ارتأت أن المحتوى المنشور على هذه المواقع يشكل جريمة أو تهديدًا للأمن القومي أو يعرض أمن البلاد أو اقتصادها الوطني للخطر. تقدم هيئة التحقيق المسألة إلى المحكمة المختصة في غضون 24 ساعة وتصدر المحكمة قرارها خلال فترة لا تتجاوز 72 ساعة إما بالقبول أو الرفض.

ثم تتوسع المادة 7 في منح السلطة لإصدار قرار الحجب، فتمنح سلطات الضبط والتحري (الشرطة) الحق في إبلاغ الجهاز القومي لتنظيم الاتصالات بإخطار مقدمي الخدمة على الفور بالحجب المؤقت للمواقع. يجب تنفيذ الأمر فورًا عند استلامه. كما هو الحال مع جميع أحكام مشروع قانون جرائم الإنترنت، الذي يتضمن مصطلحات غامضة يمكن أن تشمل أي شيء، والتي تمنح سلطة إصدار أمر الحجب إلى سلطات الضبط والتحري في "حالات الطوارئ الناجمة عن الخطر أو الضرر الوشيك".

وتجدر الإشارة إلى أن سلطات الضبط والتحري لديها سلطة إصدار قرار بتنفيذ الحجب دون الحاجة إلى إذن مسبق. ثم يتم تقديم القرار من قبل هيئات التحقيق إلى المحكمة في غضون 24 ساعة؛ ثم تصدر المحكمة قرارها في فترة لا تتجاوز 72 ساعة إما بالقبول أو الرفض، ويتم إنفاذ و تطبيق قرار سلطات التحقيق بعد صدور قرار من المحكمة المختصة، وهو قرار يعتبر إجرائيا.

لا يقدم القانون أي تعريف أو توضيح لما قد تعتبره سلطات التحقيق يُعرّض أمن البلاد واقتصاده للخطر. وقد وُجهت هذه الاتهامات في السابق ضد العديد من المتظاهرين والنشطاء في التحقيقات والمحاكمات. واعتبرت الدعوات إلى المظاهرات تهديداً للأمن القومي. على سبيل المثال في حالة القضية رقم 173 ، المعروفة إعلاميًا بقضية "التمويل الأجنبي" اعتبرت أنشطة منظمات المجتمع المدني المستقلة تهديدًا للأمن القومي وسلامة البلاد. وفي حين أن القانون لا يحدد طبيعة التهديد لأمن البلاد واقتصادها، فإنه يضع تعريفاً واسعاً للأمن القومي يشمل جميع جوانب استقلال واستقرار وأمن الوطن ووحدته وسلامة أراضيه وشؤون الرئاسة، ومجلس الدفاع ومجلس الأمن القومي والقوات المسلحة والإنتاج الحربي ووزارة الداخلية والمخابرات العامة وهيئة الرقابة الإدارية والأجهزة التابعة لتلك الهيئات. ولا يشمل هذا التعريف كل ما تنشره أي من الكيانات المذكورة على مواقع التواصل الاجتماعي أو المواقع الإخبارية أو أي مواقع تنشر محتوى يتعارض مع سياسات السلطة التنفيذية.

على الرغم من أن المادة 5 من المذكرة التوضيحية تحمي البيانات الشخصية للمستخدمين، فإن الأحكام التالية من القانون ترسخ الرقابة الشاملة على جميع مستخدمي خدمات الاتصالات في مصر. حيث تتطلب المادة 2 من القانون من شركات الاتصالات الاحتفاظ وتخزين بيانات استخدام العملاء لمدة 180 يومًا، بما في ذلك البيانات التي تتيح تحديد هوية المستخدم والبيانات المتعلقة بمحتوى نظام المعلومات وتحركات المستخدم والأجهزة المستخدمة. وهذا يعني أن مزودي خدمات

الاتصالات لديهم بيانات تصف جميع ممارسات المستخدم، بما في ذلك المكالمات الهاتفية والرسائل النصية، وجميع البيانات ذات الصلة، والمواقع التي تمت زيارتها والتطبيقات المستخدمة على الهواتف الذكية وأجهزة الحواسيب.

كما تُلزم المادة 5 شركات الاتصالات بأي قرار للاحتفاظ "ببيانات أخرى يتم تحديدها بقرار" من مجلس إدارة الجهاز القومي لتنظيم الاتصالات، وهو ما يعني أن مزودي خدمات الاتصالات ملزمون بجمع والاحتفاظ بالبيانات غير المنصوص عليها في القانون، فقط على أساس قرارات إدارية يصدرها الجهاز القومي لتنظيم الاتصالات. تمنح المادة أيضا لسلطات الأمن القومي الحق في الاطلاع على هذه البيانات وتُلزم مقدمي خدمات الاتصالات بتقديم المساعدة الفنية لذلك. وتنص المادة على أنه على مقدّمي الخدمات ومرؤوسيهم، في حالة طلب أجهزة الأمن القومي وحسب الحاجة، أن يزودوا تلك السلطات بجميع التسهيلات التقنية المتاحة حتى يتمكنوا من ممارسة سلطتهم وفقاً للقانون. ويحدد القانون أجهزة الأمن القومي لتشمل الرئاسة والقوات المسلحة ووزارة الداخلية والمخابرات العامة وهيئة الرقابة الإدارية. ولا تتناول المادة 5 أي تفاصيل تربط المراقبة بأي من الجرائم المذكورة في القانون، ولكنها تفرض الرقابة الشاملة على جميع المستخدمين في مصر.

وبينما يعاني المواطنون المصريون بالفعل من العديد من المشاكل بسبب الاضطرار إلى الكشف عن بياناتهم الشخصية في ممارساتهم اليومية المعتادة، تُوسّع المادة من سلطات جمع بيانات المستخدم، التي تتطلب من مزودي خدمات تكنولوجيا المعلومات ووكلائهم والموزعين الذين يقومون بتسويق هذه الخدمات الحصول على بيانات المستخدم. هذه الممارسة موجودة بالفعل وتتسبب في فوضى في استخدام البيانات الشخصية للمواطنين. لا يوجد في مصر أي قوانين تتعلق بحماية البيانات الشخصية، وخلال العام الماضي، قامت مؤسسة حرية الفكر والتعبير بتوثيق عدة حالات استخدم فيها بعض الموزعين بيانات شخصية للمستخدمين دون علمهم، بما في ذلك بيع خطوط الهواتف المحمولة. وكنتيجة لذلك، في كثير من الحالات، تم اختراق الحسابات الشخصية على الشبكات الاجتماعية والبريد الإلكتروني، إضافة إلى جميع الخدمات المرتبطة بها مع تزايد استخدام تكنولوجيا المعلومات والاتصالات في الأعمال التجارية والمعاملات المالية.

في نفس السياق، يتناول نص المادة 4 من القانون تبادل البيانات والمعلومات بين مصر والدول الأجنبية من خلال وزارات الخارجية والتعاون الدولي في إطار الاتفاقيات الدولية والإقليمية والثنائية أو تطبيق مبدأ المعاملة بالمثل، دون تحديد شروط هذا التبادل للمعلومات، خاصة فيما يتعلق بوجود قوانين لحماية البيانات في البلدان الأخرى أو الشروط المتعلقة بنطاق أو فترة الاحتفاظ بالمعلومات أو معالجتها.

قانون الوصول إلى المعلومات

منذ النص على الحق في الوصول إلى المعلومات في الدستور المصري الصادر في عام 2012 والدستور الحالي الصادر في عام 2014، تم طرح عدد من المسودات بشأن قانون الوصول إلى المعلومات.

خلال الممارسات الحكومية الأخيرة، بما في ذلك حجب المواقع، شكّل المجلس الأعلى للإعلام لجنة (إعداد مشروع قانون الوصول إلى المعلومات) لصياغة قانون للوصول إلى المعلومات وفقا للنص الدستوري المنصوص عليه في

المادة 68 من الدستور المصري. انتهت اللجنة من صياغة القانون في أكتوبر 2017، حيث تألف من 28 مادة تنظم مفهوم الحق في الوصول إلى المعلومات، ونطاق الاستثناءات المتعلقة بالمعلومات والبيانات التي لا يمكن الوصول إليها، وتشكيل مجلس أعلى للمعلومات، وطبيعة الجرائم والجرائم المتعلقة بالوصول إلى المعلومات وعقوباتها. ويُذكر أنه لم تتم مناقشة المسودة منذ تقديمها حتى الآن.

حالات الرقابة على الإنترنت التي تم الإبلاغ عنها

على عكس دول أخرى في المنطقة، تم الإبلاغ عن عدد قليل من أحداث الرقابة على الإنترنت في مصر في السنوات التي أعقبت ثورة 2011. ومع ذلك، تغيرت الأمور في أواخر عام 2015. وإلى جانب المملكة العربية السعودية والإمارات العربية المتحدة، ورد أن مصر حجبت الوصول إلى موقع "العربي الجديد"، وهو موقع إخباري مملوك لقطر. وقد تم تبرير هذا الحجب على أساس أن الموقع "يستخدم كبوق للإخوان المسلمين" في ضوء تصاعد التوتر في المنطقة.

لم تؤكد بيانات قياس الشبكة التي تم جمعها من خلال استخدام برمجية OONIProbe على حجب موقع العربي فحسب، بل أظهرت أيضًا أنه تم حجب مجال بديل (alarabyaljadeed.co.uk) الذي تم وضعه للتحايل على الرقابة. ذكر المرصد المفتوح لاعتراض الشبكات(OONI) أن حجب موقع العربي أدى إلى أضرار جانبية، حيث نتج عن ذلك حجب المواقع الأخرى المستضافة على نفس شبكة توصيل المحتوى (CDN) أيضا.

بعد ذلك بوقت قصير، بدأت مصر في حجب مجموعة متنوعة من مواقع الإعلام. في 24 مايو 2017، أمرت الحكومة المصرية مقدمي خدمات الإنترنت بحجب 21 موقعًا إخباريًا بحجة دعم الإرهاب ونشر الأخبار الكاذبة.و من خلال جمع وتحليل قياسات الشبكة، تأكد المرصد المفتوح لاعتراض الشبكات (OONI) من حجب عشرة مواقع إخبارية - بما في ذلك الأخبار المحلية والدولية، مثل مدى مصر والجزيرة. كما وجد المرصد أن مصر حجبت أيضا شبكة المجهولية تور (Tor)، ونطاق Tor، وجسور Tor، وموقع الويب الخاص بالمرصد المفتوح لاعتراض الشبكات(OONI) نفسه - وهو نطاق فرعي من نطاق مشروع تور.

لم تكن هذه هي المرة الأولى التي لاحظ فيها المرصد التلاعب في الدخول إلى شبكة تور في مصر. في عام 2016، أبلغ المرصد عن محاولات مقدمي خدمات الإنترنت المصريين منع الوصول إلى شبكة تور.

في محاولة لتحديد جميع المواقع الإخبارية الـ21 المحجوبة ولمزيد من البحث، جمعت AFTE المزيد من قياسات الشبكة من خلال استخدام برمجية OONIProbe عبر عدة مقدمي خدمات الإنترنت في مصر. ثم قاموا بنشر تقريرين بحثيين حول حجب 496 موقعًا على الأقل، مما يشير إلى أن الرقابة على الإنترنت في مصر أصبحت ممارسة منتشرة. لا تقتصر المواقع المحجوبة على المواقع الإخبارية فقط، بل أيضا مواقع حقوق الإنسان، وأدوات تجاوز الحجب، والمدونات، ومنصات النشر، ومواقع الحركات السياسية، والشبكات الاجتماعية، ومواقع ويكي، وغيرها من أنواع المواقع.

وفقا لمؤسسة حرية الفكر والتعبير فإن حجب المواقع الإعلامية ينتهك المادة 57 من الدستور، التي تنص على أنه لا يجوز تعليق وسائل الاتصال العامة بشكل تعسفي. وأكدت مؤسسة حرية الفكر والتعبير على أن الحجب ينتهك قرارات عدد من

المحاكم الإدارية ، فضلا عن الإعلان العالمي لحقوق الإنسان وعدد من قرارات ومواثيق الأمم المتحدة الملزمة للحكومة المصرية.

في الآونة الأخيرة، نشرت مؤسسة حرية الفكر والتعبير تقريرًا بحثيًا آخر حول حجب صفحات الجوال المسرّعة (AMP) في مصر، مما أثر على ملايين المواقع الإلكترونية الأخرى التي تستخدمه. يعمل AMP على تحسين أداء صفحات الويب على الهواتف المحمولة، مما يوفر تجربة أسرع وأفضل لمستخدمي الهواتف الذكية. في مصر، اعتمد العديد من أصحاب المواقع الإلكترونية المحجوبة على الـ AMP كاستراتيجية للتحايل على الرقابة. نظرًا لأن AMP يعرض روابط بديلة للروابط الأصلية التي تظهر في نتائج محرك بحث جوجل، حيث يتم إعادة توجيه المستخدمين إلى نطاق بديل، مما يؤدي إلى التحايل على حجب الموقع الأصلي. من خلال حجب AMP، لا تجعل السلطات المصرية التحايل على الرقابة على المواقع المحجوبة أكثر صعوبة فحسب، ولكنها تؤثر أيضًا على ملايين المواقع الأخرى التي تستخدم AMP فقط لغرض توفير أداء أفضل على الويب لمستخدمي الهواتف الذكية.هذه واحدة من العديد من الحالات التي أدت فيها ممارسات الرقابة في مصر إلى أضرار جانبية.

في عام 2016، سجل المرصد المفتوح لاعتراض الشبكات(OONI) إبطاء بروتوكول نقل النص التشعبي الآمن (HTTPS) للخدمات التي استضافها مركز بيانات تابع لشركة DigitalOcean موجود في فرانكفورت، مما أدى إلى عدم إمكانية الوصول إلى العديد من الروابط. وكجزء من هذا التقرير، كشف المرصد المفتوح لاعتراض الشبكات(OONI) أيضًا عن وجود حملة إعلانية. حيث وجد أن الشركة المصرية للاتصالات المملوكة للدولة تستخدم أجهزة الفحص العميق للحزم (DPI) أو أجهزة شبكات شبيهة لعمل هجمات من النوع الرجل في الوسط (Man-in-the-Middle) وذلك بهدف حقن محتوى مدر للدخل (إعلانات بالعمولة) أو لأغراض خبيثة (البرمجيات الخبيثة)

في الآونة الأخيرة، توسع مختبر المواطن Citizen Lab في هذا النوع من البحث من خلال التحقيق في استخدام أجهزة الفحص العميق للحزم (DPI) ، تم انتهاجها من قبل شركة Sandvine / Procera لأغراض خبيثة أو مشكوك فيها ، واستُخدمت في كل من مصر وتركيا وسوريا. وكجزء من بحثهم، وجدوا أنه يتم استخدام صناديق وسيطة (middleboxes) في مصر لاختراق الاتصالات غير المُعمّاة للمستخدمين وإعادة توجيهها إلى المحتوى المدر للدخل، مثل الإعلانات بالعمولة وأكواد برمجية لتعدين العملات الرقمية المعماة. كما وجد "مختبر المواطن" أن الأجهزة، التي تتطابق مع بصمة Sandvine PacketLogic، كانت تستخدم لحجب عشرات المواقع السياسية ومواقع حقوق الإنسان والأخبار في مصر، بما في ذلك هيومن رايتس ووتش، ومراسلون بلا حدود، والجزيرة، ومدى مصر، هفبنجتون بوست العربية.

المنهجية: قياس الرقابة على الإنترنت في مصر

لقياس الرقابة على الإنترنت في مصر، استخدمنا برنامج(OONI Probe) بشكل يومي عبر العديد من نقاط الخدمة المحلية. برنامج OONI Probe هو برنامج حر ومفتوح المصدر مصمم لقياس أشكال مختلفة من اعتراض الشبكات.

تشمل اختبارات OONI Probe الرئيسية التي أجريناها كجزء من هذه الدراسة ما يلي:

Web Connectivity
HTTP Invalid Request Line
HTTP Header Field Manipulation
Vanilla Tor
Tor Bridge Reachability
WhatsApp
Facebook Messenger
Telegram

و حيث أن الحكومة المصرية أمرت بحجب 21 موقعًا إخباريًا، فإن اختبار "Web Connectivity test " كان أساسًا لهذا البحث لجمع بيانات قياس أداء الشبكة لكشف المواقع التي تعرضت للحجب وكيفية حجبها وأي مقدمين لخدمة الإنترنت يقومون بالحجب.

تم تصميم اختبار (Web Connectivity test) لقياس ما إذا كان يتم حجب مواقع الويب من خلال التلاعب في نظام أسماء النطاقات (DNS) أو حجب حزمة بروتوكولات الإنترنت (TCP / IP) أو بواسطة (HTTP transparent proxy). يتم إجراء هذا الاختبار تلقائيًا من خلال نقطتي اتصال مختلفتين، الأول من جهاز المستخدِم والثانية من نقطة رصد غير خاضعة للرقابة، إذا كانت النتائج من كلتا نقطتي المقارنة متطابقتين، فمن المرجح أن يكون موقع الويب المختبر قابلاً للوصول إليه. وإذا اختلفت النتائج، تعتبر نتيجة القياس "غير طبيعية".

تؤكد منهجية OONI الحالية فقط على حجب موقع ما في حالة عرض صفحة وب تُخبر المستخدم بأن الموقع محجوب، و في الحالات التي لا يعرض فيها مقدمو خدمات الإنترنت هذه النوعية من الصفحات؛ يتم تحليل قياسات الشبكة ذات الصلة عبر فترة من الزمن، وذلك بفحص ما إذا كانت الأنواع المحددة من حالات الفشل في الدخول إلى الموقع المعني مستمرة أم لا، إضافة إلى أسباب حدوث هذا الفشل (بمعنى استبعاد النتائج الإيجابية غير الحقيقية).

كان الاختبار يقتصر في الغالب على عناوين الروابط المضمنة في قوائم الاختبار العالمية والمصرية لـ"مختبر المواطن" وهي قوائم تتكون من مجموعة الروابط لمختلفة التي تقع ضمن 30 فئة والتي يتم اختبارها من حيث الرقابة عليها بواسطة مشاريع قياس مثل OONI. خلال هذا البحث، قمنا بتحديث قائمة الاختبارات المصرية عدة مرات لضمان أن ما يتم اختباره هو فعلا المواقع المحجوبة. وكجزء من هذه الدراسة، تم قياس 1808 عنوان رابط، مُتَضمّنة في قوائم الاختبار العالمية والمصرية لـ"مختبر المواطن".

في محاولة لتحديد المعدات التي تم استخدامها لممارسة الرقابة على الإنترنت في مصر، أجرينا اختبار HTTP Invalid Request Line واختبار HTTP Header Field Manipulation . وهما اختباران تم تصميمهما بهدف تحديد وجود صناديق وسيطة (middleboxes). ويُذكر أنه في مرات سابقة مكّن هذان الاختباران من تحديد معدات الرقابة في بلدان مختلفة حول العالم.

بالإضافة إلى اختبارات OONI Probe، قمنا أيضًا بإجراء اختبارات زمن الوصل " latency tests" وهو اختبار يُشير

إلى مقدار الوقت الذي المُستغرق للحصول على حزمة من البيانات من نقطة معينة إلى أخرى، واختبارات أخرى لقياس الشبكة عبر جهاز راسبيري باي في مصر. ولرصد إمكانية الوصول إلى منصات المراسلة الفورية الشائعة خلال فترة من الوقت، أجرينا اختبارات OONI على WhatsApp و Facebook Messenger و Telegram، وهي اختبارها تم تصميمها لقياس إمكانية الوصول إلى هذه التطبيقات وواجهات الويب الخاصة بها.

في ضوء زيادة معدلات الرقابة على مدار العام الماضي، قررنا رصد إمكانية الوصول إلى أدوات تجاوز الحجب والرقابة على الإنترنت، وهناك العديد من مواقع أدوات تجاوز الرقابة المدرجة في قائمة الاختبار العالمية ل"مختبر المواطن"، والتي قمنا بقياسها من خلال اختبار (Web Connectivity test)، أيضًا اختبارات Vanilla Tor و Tor Bridge Reachability، والتي تم تصميمها لقياس حجب شبكة Tor وجسور Tor.
جُمعت بيانات قياسات الشبكة من خلال كل هذه الاختبارات، و بعد ذلك تم معالجة هذه البيانات وتحليلها بناءً على مجموعة موحدة من الاستدلالات لكشف الرقابة على الإنترنت والتلاعب في حركة مرور البيانات. وقمنا بتحليل كل قياسات شبكة OONI Probe التي تم جمعها من مصر خلال الفترة من يناير 2017 إلى مايو 2018.

تحديات الدراسة

أظهرت نتائج هذه الدراسة بعض التحديات.
يرتبط التحدي الأول بفترة الاختبار. حيث تتضمن هذه الدراسة تحليلاً لمئات الآلاف من قياسات الشبكة التي تم جمعها من الشبكات في مصر خلال الفترة من يناير 2017 إلى مايو 2018. إلا أنه لم يتم فحص عمليات الرقابة التي قد تكون حدثت قبل و / أو بعد فترة التحليل كجزء من هذه الدراسة.
يرتبط التحدي الآخر في هذه الدراسة بكمية وأنواع الروابط التي اُختيرت من حيث الرقابة عليها. أُجري اختبار (Web Connectivity test) لقياس إمكانية الوصول إلى 685 عنوان URL هم الأكثر ملائمة للسياق المصري و 1،123 موقعًا ذي وزن دولي. اُختيرت كل هذه الروابط وتصنيفها بالتعاون مع أفراد من المجتمع على مدار السنوات الماضية. نحن نقر بأن بعض الروابط قد تكون صنفت على نحو خاطئ، وربما يكون اختيار الروابط متحيزًا، وأن عينة اختبار الروابط قد تستبعد العديد من المواقع الأخرى المحجوبة في مصر. ولذلك، فإننا نشجع الباحثين وأفراد المجتمع على مواصلة مراجعة قوائم الاختبار هذه والإسهام فيها للمساعدة في تحسين الأبحاث والتحليلات المستقبلية.
وأخيرًا، في حين جُمعت قياسات الشبكة من نقاط مراقبة محلية متعددة في مصر، لم تُشغّل اختبارات برمجية OONI على نحو ثابت عبر جميع الشبكات. لذلك قمنا باقتصار معظم تحليلنا على الشبكات الأكثر استخداما في جمع القياسات (ما يسمح بتحليل البيانات بشكل أكثر دقة خلال فترة من الزمن) : فودافون مصر (AS36935)، لينك دوت نت (AS24863)، تي إي داتا (AS8452) و نور (AS20928).

النتائج

مواقع الوب المحجوبة

لا يبدو أن مزودي خدمة الإنترنت المصريين هم من يقومون بحجب الصفحات (على الأقل ليس لأي من المواقع التي تم اختبارها)، مما يحد من قدرتنا على تأكيد أحداث الرقابة بثقة مطلقة.

لفحص حجب مواقع الويب، قمنا بتحليل كل قياسات اتصال الإنترنت الخاصة بشبكة OONI والتي تم جمعها من نقاط الرصد المحلية في مصر في الفترة ما بين يناير 2017 ومارس 2018. وكجزء من تحليلنا، فحصنا المواقع التي أظهرت تشوهات في الشبكة، سواء كانت تلك التشوهات ثابتة ومستمرة مع مرور الوقت أم لا، وما إذا كانت تلك المواقع لديها معدلات تعطّل عالمية عالية (كجزء من الجهود لاستبعاد النتائج الإيجابية غير الحقيقية). بشكل عام، أظهر 1،054 رابط تشوهات في أداء الشبكة وعلامات على التدخل في الشبكة طوال فترة اختبار هذه الدراسة. ومع ذلك، كان بالإمكان الدخول إلى العديد من هذه المواقع في بعض الأوقات خلال فترة اختبارها، مما يشير إلى أن بعض حالات الفشل في الدخول إلى الموقع كانت إما إيجابيات كاذبة أو أن هذه المواقع تعرضت للحجب المؤقت فقط.

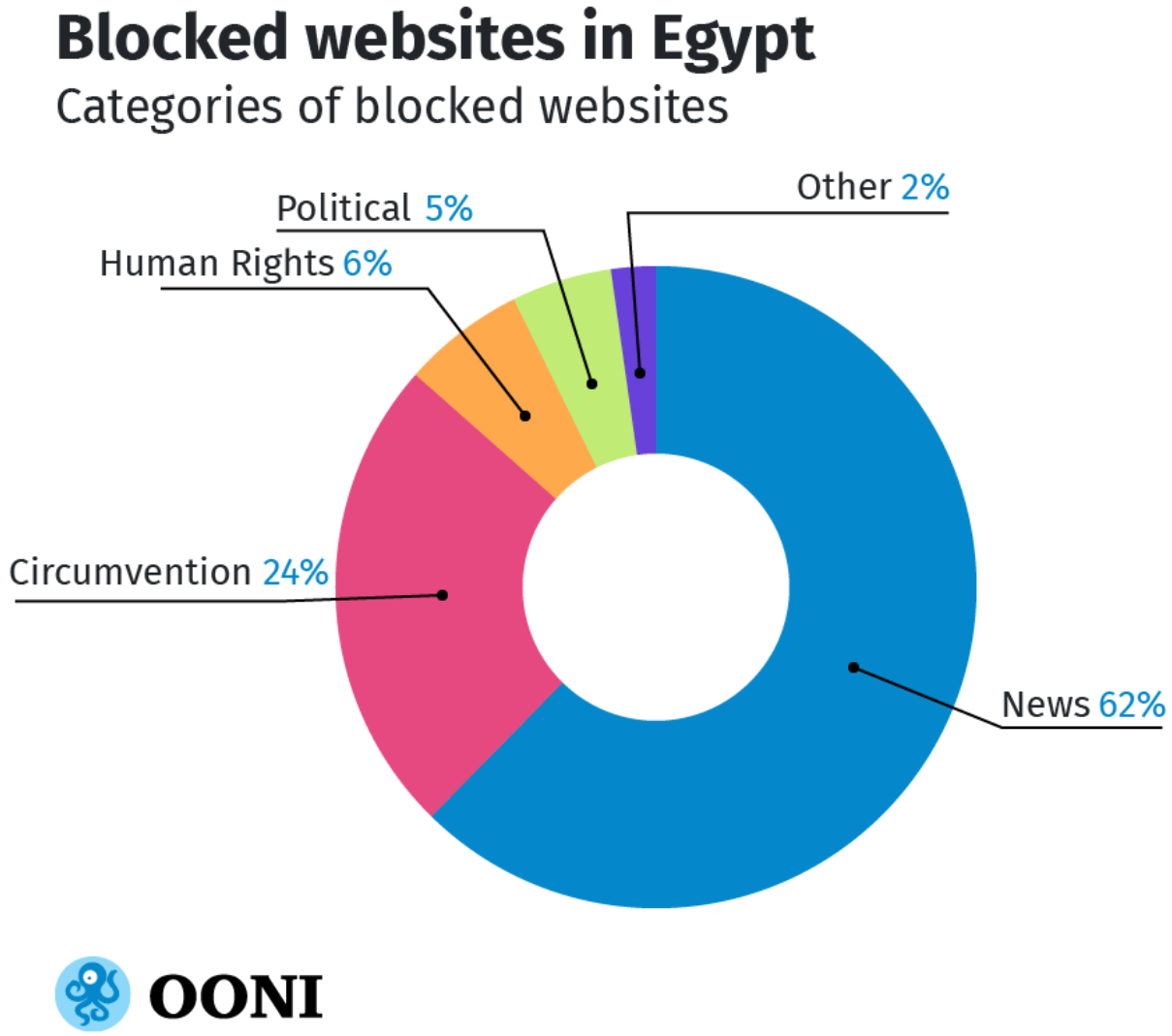
ضيّقنا نطاق تحليلنا على الروابط التي أظهرت استمرارية في كمية كبيرة من التشوهات في الشبكة (على سبيل المثال فشل بروتوكول HTTP) بالمقارنة مع إجمالي عدد المرات التي تم اختبارها خلال وقت الدراسة. قمنا بعد ذلك بتصفية العديد من الروابط التي انتهت صلاحيتها أو نطاقاتها. ربما حُجبت هذه الروابط ، لكننا قررنا استبعادها من هذه الدراسة لأنها، في كل الأحوال، لم تعد تعمل (مما يحد من تأثيرها المحتمل على الرقابة). هكذا تبقى لنا 181 عنوان URL أظهرت باستمرار نفس أنواع التشوهات في معظم الأوقات التي تم اختبارها فيها عبر العديد من مزودي خدمة الإنترنت على مدار فترة الدراسة، مما يشير بقوة إلى أنها كانت غير متاح الوصول إليها في مصر.

وشمل الـ181 رابط ثلاث نطاقات إسرائيلية (isa.gov.il, iaf.org.il, mod.gov.il) لا يبدو أنها تعرضت للحجب من قبل مقدمي خدمة الإنترنت المصريين، وإنما من قبل إسرائيل. لا يوجد استراتيجية مشتركة للثلاث مواقع تُوضّح كيفية حجبهم، حيث لا يستجيب اسم الخادوم (nameserver) الخاص بـ isa.gov.il إلى عناوين IPs المصرية، كما أن الوصول إلى iaf.org.il محظور في مصر عناوين الـIPs، بينما يبدو أنه يتعذر الوصول إلى موقع mod.gov.il في مصر بسبب القيود ذات الأساس الجغرافي.

باستثناء هذه المواقع الإسرائيلية الثلاثة، يبدو أنه حُجب 178 رابط على الأرجح من قبل مقدمي خدمة الإنترنت المصريين، نظراً إلى كونها كانت محل اختبار لمئات المرات عبر شبكات متعددة وفي كل مرة كشفت عن نسبة عالية من أوجه فشل الوصول لها. ويبدو أن هذه المواقع يتم حجبها في المقام الأول من خلال استخدام تقنية الفحص العميق للحزم Deep Packet Inspection (DPI) التي تم استخدامها لإعاقة الاتصالات، مما يؤدي إلى فشل استجابة HTTP.

يبدو أن الرقابة على الإنترنت في مصر خلال العام الماضي أصبحت منتشرة بدرجة كبيرة حيث أن العديد من أنواع المواقع

قد حُجبت. يوضح الرسم البياني أدناه أنواع المواقع التي أظهرت أكبر قدر من الأداء الشبكي غير الطبيعي، وبالتالي يُحتمل أن تكون قد حُجبت.



كانت معظم المواقع الخاضعة للرقابة هي المواقع الإخبارية ، يليها عدد من مواقع أدوات تجاوز الحجب، ومواقع حقوق الإنسان، والعديد من المدونات والمواقع التي يتضمن محتواها نقدا سياسيا.

في مايو 2017، أمرت الحكومة المصرية بحجب 21 موقعًا إخباريًا، لكن تحليلنا يشير إلى أن الأرجح أنه تم حجب أكثر من 100 موقع إخباري على مدار العام الماضي. كذلك مثّل عدد كبير من المواقع التي تُقدّم محتوى متعلق بحقوق الإنسان والآراء التي تعبر عن النقد السياسي نسبة عالية من حالات الأداء غير الطبيعي على الشبكة، مما يُشير إلى أن الرقابة قد تكون ذات دوافع سياسية.

كون العديد من مواقع أدوات تجاوز الحجب قد أظهرت أيضا معدلا عاليا من المشاكل على الشبكة، فإن ذلك يرجح أن مقدمي خدمات الإنترنت في مصر قد حاولوا تعزيز الرقابة من خلال جعل تجاوز الحجب أكثر صعوبة.

تجدر الإشارة إلى أن المخطط أعلاه يحمل أوجه قصور، لاسيما أنه يُشير إلى كمية وأنواع مواقع الوب التي تم اختبارها كجزء من هذه الدراسة. في حال اُختيرت عينة مختلفة من المواقع، فمن المحتمل أن يكون الشكل مختلفًا. ومع ذلك، فإن الهدف من هذا الشكل هو توضيح أنواع المواقع التي شملت أكبر قدر من التشوهات ضمن حدود مواقع الويب المُحدّدة التي اختُبرت.

تبحث الأقسام التالية بمزيد من العمق في فئات المواقع الأربعة (الأخبار وحقوق الإنسان والنقد السياسي و تجاوز الرقابة) التي أظهرت أعلى نسبة من الأداء غير الطبيعي على الشبكة كجزء من هذه الدراسة، والتي لذلك يرجح أن تكون قد تعرضت للحجب أثناء فترة الاختبار والتحليل لهذه الدراسة.

المواقع الإخبارية

تُشكّل المواقع الإعلامية الغالبية العظمى من المواقع التي وجدنا أنها محظورة كجزء من هذه الدراسة.

من بين الـ 178 رابط المحجوبين، كان 111 منها ينتمي إلى المواقع ذات الطابع الإخباري. وقد تم اختبار هذه الروابط مئات المرات، وفي كل مرة أظهرت نسبة عالية من حالات فشل HTTP طوال فترة الاختبار. القائمة الكاملة للمواقع الإخبارية المحظورة، والتي توضح عدد مرات اختبارها مقابل عدد المرات التي أظهرت فيها حالات فشل HTTP، متاحة **هنا**.

تتضمن الروابط المحجوبة مواقع إخبارية مصرية محلية، بالإضافة إلى مواقع إعلامية دولية. وتشمل هذه المواقع: مدى مصر، الجزيرة، شبكة رصد الإخبارية، ساسا بوست، العربي الجديد، ديلي نيوز إيجيبت، هافينغتون بوست بالعربية، أخبار البورصة، المصريون ومصر العربية، وغيرها الكثير. بشكل عام، يبدو أن أكثر من 100 موقع إعلامي قد تم حجبه طوال فترة الاختبار، وتقتصر هذه النتيجة على عينة صغيرة نسبيا من المواقع الإعلام التي اختُبرت.

تجدر الإشارة إلى أننا عثرنا على العديد من المواقع الإخبارية المحجوبة التركية مثل turkpress.co و turk.life و arab-turkey.com و الايرانية alalam.ir ، مما يشير إلى أن المخاوف السياسية والأمنية قد أثرت على الأرجح على قرارات الرقابة. كما تتضمن المواقع الاخبارية المحجوبة صحيفة ساخرة (alahraam.com) وموقع أخبار مملوك لقطر (qtv.qa)، ضمن مواقع إخبارية إقليمية ودولية أخرى.

كذلك حُجب موقع جريدة الأخبار اللبنانية بعد نشر أنباء متعلقة باستقالة مدير المخابرات العامة المصرية. كما حُجب موقع "في الفن"، وهو أكبر موقع يقدم أخبار السينما، بعد نشر أخبار عن ضرب تركي آل شيخ (مستشار في الديوان الملكي في المملكة العربية السعودية) لمطربة مصرية. كذلك حُجب موقع القاهرة 24 الإخباري بعد نشره تقريرا عن الهجوم على هشام جنينه، أحد معارضي النظام الحالي.

تعذّر الوصول إلى الموقع الإخباري "صوت الأمة" مؤقتًا في يونيو 2017. وبالنظر إلى القياسات ، فقد يكون الموقع قد تعرض لهجمات الحرمان من الخدمات (DDoSed). كما أن عددًا من المواقع الإعلامية الأخرى لم يكن من الممكن

الوصول إليها بشكل مؤقت طوال فترة الاختبار. تظهر أحدث قياسات OONI أنه يمكن الوصول إلى بعض المواقع الإعلامية المحجوبة في السابق (مثل مدى مصر)، بينما تظل مواقع إخبارية الأخرى (خاصة الدولية منها) محجوب (مثل الجزيرة).

في محاولة لتجاوز الرقابة، استخدمت بعض المواقع الإلكترونية المحجوبة نطاقات بديلة، لكن ذلك لم يكن فعالًا دائمًا.

استخدمت صحيفة المصريون نطاق elmesryoon.com بدلاً من almesryoon.com وأظهرت قياسات OONI الأخيرة أن الوصول إليه أصبح متاحا (على شبكة واحدة حيث تم اختباره). من ناحية أخرى، استخدمت ديلي نيوز ايجيبت نطاق thedailynewsegypt.com بدلاً من dailynewsegypt.com، ولكن يبدو أن مقدمي خدمة الإنترنت في مصر قاموا بحجب هذا النطاق أيضا.

لدراسة تأثير عمليات الرقابة هذه، أجرت مؤسسة حرية الفكر والتعبير مقابلات مع بعض العاملين في المؤسسات الإعلامية المصرية التي حُجبت مواقعها. تقول لينا عطا الله، رئيسة تحرير موقع مدى مصر (التي تم حجبها لأول مرة في مايو 2017):

"كنا نعمل بشكل طبيعي وفجأة لم نتمكن من الوصول إلى موقع مدى. في الوقت نفسه، ظهرت أنباء على مواقع مؤيدة للنظام بأنه تم حجب مجموعة من مواقع الوب. وفي نهاية المطاف، أصبح واضحًا أن سياسة الحجب كانت سياسة منهجية ولا تقتصر على مجموعة من المواقع، حاولنا التواصل مع هيئات مختلفة، مثل نقابة الصحفيين، والمجلس الأعلى لتنظيم الإعلام، والجهاز القومي لتنظيم الاتصالات. وأنكر كل طرف مسئوليته عن الحجب. حتى الآن، لا يوجد اتصال مباشر مع أي سلطة أو هيئة رسمية، ولا يوجد من أعلن مسئوليته عن الحجب. وفي نفس الوقت، نواصل العمل ونستخدم المنصات البديلة، مثل الشبكات الاجتماعية. "

كما فوجئ العاملون في جريدة مصر العربية بحجب موقعهم. يقول رئيس التحرير، عادل صبري:

"يوم 24 مايو 2017، رأينا فجأة حملة على برامج التوك شو تطالب بحجب مواقع وب، كما نشر خبر على موقع جريدة "اليوم السابع"، قائلاً إنه تم حجب 21 موقعًا، بما في ذلك موقع مصر العربية ".

يقول عادل صبري من مصر العربية:
هذا الحجب منع 70% من جمهور الموقع من الوصول إليه. وقد كان لذلك آثار اقتصادية على أدائنا، حيث قامت بعض الشركات والبنوك بسحب إعلاناتهم من على موقعنا. كذلك أدى حجب موقعنا إلى خوف الكثير من المصادر من التعامل مع صحفيينا"

وتظهر أحدث قياسات OONI أن هذا الموقع الإخباري لا يزال محجوبا في مصر.

وبالمثل، فإن حجب الموقع الإخباري "البداية" كان له تأثير على جمهوره وعلى عمل صحفيوه. يقول رئيس التحرير خالد البلشي:

"كان عدد قراء موقعنا الإخباري يصل في العادة إلى عدة آلاف في اليوم. بعد الحجب، أنتج فريقنا محتوى لا يمكن الوصول إليه من قبل الغالبية العظمى من جمهورنا، وهو أمر محبط بشكل عام".

إلا أن ملابسات حجب البداية كانت مختلفة مقارنة بالمواقع الإخبارية المصرية الأخرى. يقول خالد البلشي:

"تلقيت اتصالاً من زميل يعمل في صحيفة قريبة من الدولة قال لي إن هناك تعليمات لمهاجمتي. لقد وجدت مقالا يهينني بسبب مقال لم أكتبه. وعندما أنكرت أنني كاتب هذا المقال، تلقيت الأخبار من زميل لي أنه تم حجب موقع البداية."

منذ ذلك الحين، قدم خالد البلشي شكوى إلى نقابة الصحفيين والمجلس الأعلى لتنظيم الإعلام رداً على حجب الموقع. يقول:

"بعد أن حُجبت"البداية"، حجبت السلطات أيضا موقع "مصريات" الذي يقدم محتوى مرتبط بالنساء، وتديره نفيسة الصباغ. أعتقد أن الموقع تم حجبه فقط لأن رئيسة التحرير هي زوجتي، حيث أن الموقع ليس سياسيا ".

وبحسب لينا عطا الله من "مدى مصر"، يمكن تفسير حجب المواقع الإعلامية بسياقين:

"الأول هو سياق المجال العام الذي تحاول السلطات الحد منه، والثاني مرتبط بالإنترنت كمساحة افتراضية تسمح بتداول المعلومات. أعتقد أن هناك مجموعة من الممارسات التي تقوم بها السلطات لاحتواء المساحة المفتوحة التي يوفرها الإنترنت، وحجب المواقع الإلكترونية جزء منه. "

كذلك يقول خالد البلشي من "البداية" أن حجب المواقع هو جزء من عقلية نظام لا يقبل أصواتاً مخالفة لما تقوله السلطات.

"هذا الحجب يتماشى مع السياسات الحالية للدولة، تماماً كما أغلقت منظمات المجتمع المدني، وقيدت حركة العمال، وأغلق المجال العام وعُرقلت وسائل الإعلام".

حُجب موقع *كورابيا لأول مرة في يوليو 2017*، وهو موقع إخباري يغطي أخبار كرة القدم محليا وعالميا. وبحسب محرري *الموقع*:"يعمل في المؤسسة أكثر من مائة صحفي ومراسل ومحرر كلهم أصبحوا مهددين بعد أن وصلنا جميعاً لطريق مسدود ودخلنا مرة أخرى في نفق مظلم، لا نرى نهايته ولا نعلم من المسؤول عن هذه القرارات. "

قبل بضعة أشهر، أعلنت كورابيا على حسابها الرسمي على فيسبوك أنها ستعلق موقعها على الويب. وتظهر أحدث قياسات OONI أن موقع كورابيا لا يزال محجوبا، على الرغم من تعليق أنشطته.

و أعلن موقع "البديل" الإخباري المحجوب أنه لن يُعلّق العمل بموقعه فحسب، بل أيضا كافة منصاته على وسائل التواصل الاجتماعي وأنه لن ينشر أي محتوى بعد الآن، سواء كان مكتوبًا أو مرئيًا. كما علق الموقع الإخباري المحجوب "البداية" أيضا عمله في الشهور الأخيرة، ولكن دون إعلان رسمي.

أُقيمت ثلاث دعاوى قضائية ،نُظرت جميعها أمام محكمة القضاء الإداري بالقاهرة،الأولي أقامتها مؤسسة حرية الفكر والتعبير وما زالت الدعوى منظورة أمام المحكمة في أنتظار صدور تقرير قانوني حول موضوع القضية والثانية رُفعت من قبل موقع مدى مصر والثالثة من قبل قناة الشرق التليفزيونية. وقد تم رفع الدعاوى ضد وزارة الاتصالات وتكنولوجيا المعلومات والهيئة القومية لتنظيم الاتصالات. وتطالب الدعاوى القضائية السلطات بتوضيح سبب حجب مواقعها والكشف عن الجهات المسئولة عن الرقابة. في 22 أبريل عام 2018، رفضت المحكمة دعوى قناة الشرق لأن القناة غير مسجلة قانونًا (وبالتالي لا يحق لها رفع دعوى قضائية). ولا تزال دعوى "مدى مصر" قيد النظر.

على الرغم من رفض الدعوى القضائية التي رفعتها قناة الشرق، إلا أن الجهاز القومي لتنظيم الاتصالات كشفت أن حجب

موقعها الإلكتروني جاء بناءً على طلب من لجنة مراقبة وتنظيم أموال جماعة الإخوان المسلمين. وشمل الطلب الاستيلاء على الكيانات والأموال التابعة للمجموعة، فضلاً عن حجب 16 موقعاً و16 قناة تلفزيونية وجريدة "المصريون".

حقوق الإنسان

تشير قياسات OONI إلى أن مواقع حقوق الإنسان قد حُجبت هي الأخرى في مصر.

الجدول التالي يلخص مقدار التشوهات في الشبكة التي ظهرت في كل موقع مقارنة بعدد المرات التي تم اختبارها فيه. تشير النسبة العالية من التشوهات، إلى جانب سهولة الوصول إلى تلك المواقع من نقاط الرصد العالمية، وإلى أن المواقع المدرجة في الجدول أدناه قد حجبت في مصر.

الروابط	عدد التشوهات	عدد مرات الاختبار
http://www.sinaihr.org	165	210
http://www.qantara.de	161	186
http://liberties.aljazeera.com/	153	196
http://www.ec-rf.org	152	177
http://www.mom-rsf.org	150	177
http://www.jatoeg.org	137	173
https://www.reporter-ohne-grenzen.de	136	151
https://www.sinaihr.org/	122	159
https://www.hrw.org/	116	176
http://www.anhri.net	86	212

منظمة سيناء لحقوق الإنسان منظمة غير حكومية تراقب وتوثق انتهاكات حقوق الإنسان في منطقة سيناء المصرية. قد يكون وراء حجب موقعهم دوافع سياسية، نظراً للصراع الدائر في شبه جزيرة سيناء بين المتشددين الإسلاميين وقوات الأمن المصرية.

ومن مواقع حقوق الإنسان الأخرى المحجوبة في مصر الشبكة العربية لمعلومات حقوق الإنسان، وهيومان رايتس ووتش، ومنظمة مراسلون بلا حدود، والمفوضية المصرية للحقوق والحريات، ومرصد الصحفيين ضد التعذيب. يبدو أن حجب هيومن رايتس ووتش قد بدأ بحلول الأول من أكتوبر / تشرين الأول 2017، وقد يكون الدافع وراء ذلك هو نشر تقرير عن التعذيب في السجون المصرية.

يقول محمد لطفي، المدير التنفيذي للمفوضية المصرية للحقوق والحريات (ECRF)

"تم حجب موقعنا في صباح يوم 5 سبتمبر 2017. كنا أطلقنا للتو حملة ونشرنا تقريرًا عن حوادث "الاختفاء القسري" في مصر، قبل بضعة أيام من الحجب. حاولنا أن نتعامل على الفور مع الوضع ونقلنا محتوانا إلى خادوم ونطاق آخر غير محجوب بعد أسبوعين من الحجب ".

وبحسب لطفي:

"السلطات لديها مشكلة مع تداول المعلومات على الإنترنت ولذلك فهي تحاول السيطرة عليها بعد أن قد سيطروا بالفعل على وسائل الإعلام والصحف التقليدية. لا أعتقد أن السلطة ستنجح في ذلك ".

النقد السياسي

وجدنا أن العديد من المواقع الإلكترونية والمدونات التي تعبر عن أفكار سياسية تعرضت للحجب خلال فترة الاختبار.

الجدول التالي يوضح كم تشوهات الشبكة التي وجدت في كل موقع مقارنة بعدد المرات التي تم اختبارها فيه.

الروابط	عدد التشوهات	عدد مرات الاختبار
http://baheyya.blogspot.com	152	212
http://www.manalaa.net	138	207
http://medium.com	86	184
http://ikhwanonline.com/	355	426
http://6april.org	172	205
http://fakartany.com	167	197
http://www.ikhwanonline.com/new/Default.aspx	161	207
http://www.gwady.net	160	198
http://revsoc.me	158	206

كانت إحدى المدونات الأولى في مصر - مدونة منال وعلاء - من بين المواقع المحجوبة. دعمت هذه المدونة أنشطة التدوين منذ إنشائها في عام 2004، واستضافت مدونات مصرية أخرى وقدمت الدعم الفني عند بدء التدوين في مصر. وهناك مدونة أخرى تقدم التعليقات والتحليلات على السياسة المصرية كانت من بين تلك التي تم حجبها، إلى جانب منصة التدوين الشهيرة medium.com وموقع إلكتروني يناقش مجموعة متنوعة من القضايا السياسية المصرية.

في عام 2008، نشأت حركة شباب 6 أبريل كمجموعة ناشطة مصرية لدعم العمال الذين كانوا يخططون للإضراب في 6 أبريل. لكن محكمة مصرية حجبت أنشطتها قبل أربع سنوات. وكان موقعهم من بين المواقع التي حُجبت، إلى جانب موقع آخر يقدم محتوى الاشتراكي. ويبدو أن موقع fakartany.com قد تم حجبه باستخدام القاعدة المعتادة.

ويبدو أن موقع fakartany.com الذي يعمل كمساحة تفكير افتراضية قد تم حجبه باستخدام القاعدة المعتادة التي تقوم بالحجب بناءًا على رقم التعريفي الخاص ببروتوكول الإنترنت (IP) في تقريبا نفس موقع الاتصال حيث تم رصد أجهزة الفحص العميق للحزم (DPI) - بناءًا على اختبارات من أجهزة راسبيري باي في مصر - على عكس مواقع الوب الأخرى، لم يتم رصد حقن RST، ولكن تم إسقاط الحزم. هذا منطقي من الناحية الهندسية، للحد من الضغط على أجهزة الفحص العميق للحزم (DPI)، أو لحجب خدمة متصلة بالرقم التعريفي (IP) ذات اتصال HTTP/HTTPS غير طبيعي. هذه الحالة تسلط الضوء على بعض التفاوت في قواعد تصفية الشبكة المستخدمة من قبل مزودي خدمة الانترنت في مصر.

مواقع أدوات تجاوز الحجب

تم العثور على عدد من المواقع التي تقدم خدمات وسيطة و أدوات لتجاوز الحجب وقد تعرضت هي ذاتها للحجب، مما يجعل تجاوز الرقابة أكثر صعوبة في مصر. الجدول التالي يلخص النتائج:

الروابط	عدد التشوهات	عدد مرات الاختبار
http://www.http-tunnel.com	187	393
https://ooni.torproject.org	168	184
https://explorer.ooni.torproject.org	168	190
http://www.hsselite.com	165	199
https://bridges.torproject.org	163	188
https://www.torproject.org	150	166
https://www.hotspotshield.com/	148	179
http://www.hotspotshield.com	147	179
https://www.thehiddenwiki.org	134	161
http://www.anonymsurfen.com	132	398
http://anonymizer.secuser.com	127	420
https://www.hotspotshield.com	121	162
http://www.zensur.freerk.com	119	382
http://www.xroxy.com	109	385
http://www.jmarshall.com/tools/cgiproxy/	107	387
http://www.suedeproxy.info	106	177
http://www.inetprivacy.com	106	397
http://www.ultimate-anonymity.com	104	380
http://www.stupidcensorship.com	101	385
http://www.webproxyfree.net	93	177
http://www.saoudiproxy.info	92	178
https://psiphon.ca/	86	189
https://www.anonymizer.com/	83	178
https://psiphon.ca	80	143
https://freenetproject.org/	79	190
http://www.vpnbook.com	76	178
http://www.unblockweb.co	76	165

http://www.proxy-list.org	76	187
http://www.hola.org	75	187
http://www.ninjaweb.xyz	75	163
http://www.anonymizer.com	74	166
http://www.unblockfreeproxy.com	72	165
http://www.orangeproxy.net	72	165
http://www.hidester.com	71	159
http://www.unblockytproxy.com	71	187
http://www.dolopo.net	71	182
http://www.freeproxyserver.co	71	162
http://www.northghost.com	71	174
http://www.cactusvpn.com	71	162

كما أظهرت عدة مواقع أخرى لتجاوز الحجب تشوهات في الشبكة أثناء الاختبار، ولكننا اقتصرنا في النتائج على تلك التي قدمت أعلى نسبة من التشوهات بالمقارنة مع عدد مرات اختبارها خلال فترة هذه الدراسة.

شملت المواقع المحجوبة عددا من أدوات تجاوز الحجب، مثل torproject.org و hotspotshield.com و psiphon.ca. كما حُجبت أيضا نطاقات فرعية من torproject.org مثل bridges.torproject.org و ooni.torproject.org أيضًا.

لا يبدو أن حجب الشركات المصرية المزودة لخدمة الانترنت قَصُر على مواقع الانترنت المتعلقة بتجاوز الحجب فقط، بل امتدت لتشمل حجب شبكة تور.

حجب تور

توفر شبكة تور (Tor network) تصفح الإنترنت دون الكشف عن هوية المستخدم وتحمي الخصوصية وتتجاوز الرقابة، باستطاعة المستخدمين أن يتحايلوا على الحجب وان يتصلوا بشبكة تور من خلال جسور تور (Tor bridges). ولذلك تم استهدافها من أجهزة الرقابة في عديد من الحكومات حول العالم.

في إطار هذه الدراسة قمنا بتحليل قياسات أداء الشبكة التي تم جمعها من مصر من خلال استخدام اختبارات OONI's Vanilla Tor وقابلية الوصول إلى جسور تور، المصممة لقياس حجب شبكة تور والجسور الافتراضية لمتصفح تور.

جُمعت معظم قياسات Vanilla Tor في الأساس من شبكتين لينك دوت نت (AS24863) و تي إي داتا (AS8452)، و تشير هذه القياسات إلى أنه لا يمكن الوصول إلى شبكة Tor، نظرًا لأن الاختبارات لم تكن قادرة على تشغيل اتصالات شبكة Tor في غضون 300 ثانية.

في الشهور الأخيرة، أظهر أكثر من 460 قياس جُمعت من هذه الشبكات استمرار عدم القدرة على الاتصال بشبكةTor ، مما يشير بقوة إلى حجب الوصول إليها. وبالمثل، تشير القياسات التي تم جمعها من اتصالات مصر (AS36992)، وموبينيل (AS37069) وفودافون (AS36935) إلى أن الوصول إلى شبكة Tor محجوب، حيث أن العديد من محاولات الاتصال لم تنجح خلال العام ونصف العام الماضيين. على الأرجح يتم تعطيل تمهيد الاتصال بشبكة تور من خلال حجب الطلبات إلى بعض خواديم تور.

جُمعت القليل من القياسات لإمكانية الوصول إلى الجسور من مصر، مما يحد من قدرتنا على فحص حجبها المحتمل بشكل أكبر خلال فترة التحليل وعبر الشبكات. جُمعت هذه القياسات في يونيو 2017 من شبكات تي إي داتا (AS8452) و فودافون (AS36935). يبدو أن فودافون تحجب تقنية obfs4 وهو جزء من متصفح تور، حيث أن جميع محاولات الاتصال كانت غير ناجحة (على الرغم من أنه لا يزال من غير الواضح ما إذا كانت الجسور *الخاصة* تعمل أم لا). توضح جميع القياسات التي تم جمعها من تي إي داتا أن obfs4 يعمل.

استراتيجية "الدفاع في العمق" لتنقية الشبكة

ربما يكون خبراء الأمن على دراية بمفهوم "الدفاع في العمق" الذي توضع فيه عدة طبقات من الطبقات الأمنية (الدفاع) في جميع مكونات نظام تكنولوجيا المعلومات. بشكل عام تهدف استراتيجية "الدفاع في العمق" إلى زيادة حماية النظام في حال إخفاق طبقة من طبقات الحماية أو إستغلال ثغرة أمنية في إحداها.

تُشير الاختبارات التي أُجريت عن طريق راسبيري باي المستخدم في مصر إلى أن مقدمي خدمات الإنترنت يطبقون استراتيجية "الدفاع في العمق" لتصفية الشبكات، لا سيما فيما يتعلق بحجب موقع fj-p.com وهو موقع حزب الحرية والعدالة في مصر.

عند محاولة الدخول على موقع http://www.fj-p.com، يُعاد توجيه المستخدم إلى http://fj-p.com ، وهو موقع مُستضاف في مكان غير معلوم من خلال خواديم توزيع المحتوى التابعة لكلاودفلاير. كل من http://www.fj-p.com و http://fj-p.com محجوبان ، ولكن يبدو أنهما محجوبان بواسطة آليات مختلفة.

لقد سبق أن وجدنا صندوق وسيط (middlebox) في مصر، يحمل بصمة (IPID 0x1234).لكن أحدث قياس أظهر لنا وجود صندوق وسيط آخر يحمل بصمة أخرى هي (IPID 0x0000). وكلا الصندوقين يقعان ضمن الشبكة المصرية ذاتها، إلا أن زمن الوصول إلى الصندوقين يختلف قليلاً: حيث يبلغ 33 مللي ثانية بالنسبة للصندوق الأول، في حين يقل عن ذلك (30 مللي ثانية) بالنسبة للصندوق الثاني.

تتبع مسار الحزم (traceroute) لا يُمكّن من الوصول بدقة إلى عناوين الـ IP للصناديق الوسيطة، لكنه يساعد على فهم المسار المحتمل لطلب HTTP "الخاضع للرقابة" عبر الشبكة.

```
```

```
HOST: lepidopter          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???   10.x.y.z       0.0%    10    0.6   0.6   0.6   0.7   0.0
  2. AS???   10.x.a.b       0.0%    10    1.0   0.9   0.9   1.0   0.0
  3. AS???   ???           100.0%    10    0.0   0.0   0.0   0.0   0.0
  4. AS20928 bng.rams.ca (217.139.253.19)
                            0.0%    10   38.8  33.9  29.7  38.8   3.1
  5. AS???   172.17.51.73   0.0%    10  116.5  44.1  32.4 116.5  25.6
  6. AS2914  185.84.18.93   0.0%    10   65.8  66.5  63.6  70.1   1.7
  ...
```

عند مقارنة الصندوقين وجدنا أن 0x1234 لا يقوم بضبط خاصية DF (عدم التقطيع) الخاص برأس الحزمة المحقونة (TCP RST)، بينما يفعل 0x000. صندوق 0x1234 يبدو أنه يضبط خاصية مدى حياة الطرد على الشبكة (TTL) لـ ٦٤ (يرى المستخدم ٥٩) بينما 0x0000 يبدو أنه يضبط نفس الخاصية لرقم ٣٢ (المستخدم يرى ٢٨). هذه الأرقام هي مجرد افتراضات مبنية على أن هذه الأرقام في الأغلب عبارة عن نتائج رفع للرقم ٢. مسافة القفزات أيضًا متوازنة مع زمن الوصول، حيث نعتقد أن 0x1234 يقوم بـ ٥ قفزات بزمن وصول ٣٣ مللي ثانية، بينما يقوم 0x0000 بـ ٤ قفزات بزمن وصول ٣٠ ثانية.

الرقم الخاص بحجم النافذة الخاص ببروتوكول التحكم بالنقل (TCP) هو أيضًا ثابت ومختلف بين الصندوقين. الصندوق 0x1234 يضبط حجم النافذة لـ 32120 بينما صندوق 0x0000 يقوم بضبط حجم النافذة لـ 229. قيمة حجم النافذة لا يهم بالنسبة لحزمة RST، لكنه حقل إجباري خاص برأس حزمة بروتوكول التحكم بالنقل (TCP).

حزمة RST التي يحقنها صندوق 0x1234 لا تحتوي على حمولة، بينما الحزمة التي يحقنها صندوق 0x0000 تحتوي على 22 بايت بقيمة صفر (هذا ليس Ethernet Padding ولكنها عدد حقيقي من البايت ذات القيمة صفر تبعا لقيمة حجم الحزمة.)

بالإضافة إلى ذلك، إرسال طلبين ببروتوكول نقل النص الفائق (HTTP requests) لعنوان عشوائي (مثال، أحد عناوين جوجل: 216.58.206.14) يقوم بتفعيل نوعين مختلفين من جدران الحماية \ الصناديق الوسيطة، كل منهما مضبوط بطريقة مختلفة قليلا. تجربة إرسال طلبين HTTP مختلفين لعنوان واحد خاص بجوجل هو للتأكد من وجود الصناديق الوسيطة على نفس الطريق الاتصالي ما بين العميل والمستضيف، أي أنهم ليسوا مجرد صناديق وسيطة مختلفة على طرق

اتصالية مختلفة.

كل هذا يرجّح وجود صندوقان وسطيان مختلفان يقوما بتصفية الشبكة على هذا الطريق الاتصالي، محفّزة تبعا لقواعد مختلفة قليلا، حيث ان طلب لعنوان http://www.fj-p.com يقوم بتحفيز الصندوق 0x0000 بينما طلب لعنوان http://fj-p.com يقوم بتحفيز الصندوق 0x1234.

هذا يبدو أنه استراتيجية "دفاع في العمق" مطبّقة على الرقابة، ومؤكد بواسطة مراقبة مسار حزم بروتوكول TCP باستخدام طلب HTTP. الطلب لعنوان http://www.fj-p.com (الذي يقوم بتحفيز الصندوق 0x0000 وهو الأقرب) يتلقى حزمة RST حيث أن قيمة مدة حياة الطرد على الشبكة (TTL) الخاصة بالعميل قيمتها 5، بينما الطلب لعنوان http://fj-p.com (الذي يقوم بتحفيز الصندوق 0x1234 وهو ابعد بـ 3 إلى 4 مللي من الثانية، ويُفترض أن المسار إليه يحتوي على قفزة واحدة أطول) يتلقى حزمة RST ، حيث أن قيمة مدة حياة الطرد على الشبكة (TTL) الخاصة بالعميل قيمتها 6 (وهو ما تم تأكيده عن باستخدام سلسلة قصيرة من الاختبارات).

بالإضافة إلى ذلك، لا يبدو أن الصندوق 0x0000 يقوم بإعادة دمج طلبات HTTP في معظم الحالات. التجارب الإضافية على العنوان http://www.fj-p.com تشير إلى أن في حالة أن فعل GET الخاص بطلب الـ HTTP منقسم في الوسط (مثل `GE || T ...`) لا يوجد حزمة RST عادية عند القيمة 5 لمدة حياة الطرد على الشبكة (TTL)، بينما يوجد حزمة RST بقيمة TTL تساوي 6 من الصندوق 0x12345. هذا يشير بقوة إلى أن هذان الصندوقان يتصرفان بطريقة مختلفة عندما يتم انقسام فعل طلب HTTP.

ومع ذلك يبدوا أن الصندوقين يقومان بجمع حقول الرأس `Host`. عندما يتم قَسم قيمة هذا الحقل، حيث أن القيمة `Host:www.f || j-p.com` قامت بتحفيز الصندوق 0x0000 بينما القيمة `Host: fj-p. || com` قامت بتفعيل الصندوق 0x1234 (كما هو متوقّع).

باختصار، الصندوقين الوسيطين يستبدلا الطلبات الأصلية بحزم RST عند توجيهها إلى الخواديم (حيث يتم الحفاظ على حقل TTL الذي تم تعيينه منقل العميل أثناء إعادة توجيه الحزمة). وهذا يشير إلى أن كلا الصندوقين يقعا في مسار الاتصال (man-in-the-middle) وليس على جانب المسار (man-on-the-side) ، وهذا يقودنا للاعتقاد بأن مقدمي خدمات الإنترنت في مصر يطبقون تكتيكات "الدفاع في العمق" لتصفية الشبكة.

التشويش على حركة مرور البيانات عبر بروتوكول طبقة المنافذ الآمنة (SSL) إلى كلاودفير

يبدو أنه تم تصفية مرور البيانات بين نقطة اتصال كلاودفلاير في القاهرة والخواديم كلاودفلير المتواجدة خارج مصر. كشفت مئات من قياساتOONI للشبكة أخطاء محددة في كلاودفلاير (مثل 525، والتي تحدث حين تفشل مصادقات SSL إلى Cloudflare) ، مما يشير إلى أن مقدمي خدمات الإنترنت في مصر يحجبون المواقع التي تستخدم كلاودفلاير عن طريق التدخل في حركة مرور البيانات المعماة عبر بروتوكول طبقة المنافذ الآمنة بين خواديم كلاودفلاير لتوزيع المحتوى والخواديم التي تستضيف مواقع الوب.

لقد استبعدنا مواقع التي تعتمد على بروتوكول نقل النص التشعبي غير المعماة (HTTP) التي أظهرت مثل تلك التشوهات (مثل zenvpn.net و tunnelbear.com) ، وذلك في حالة العبث بمسار الاتصال بين العميل و كلاودفلاير، وقصرنا النتائج التي توصلنا إليها على المواقع التي تستخدم برتوكول نقل النص التشعبي الآمن(HTTPS) المُعمى (وذلك يمكننا من تأكيد الحجب بمزيد من الثقة). تبقى لدينا مواقع أداتي تجاوز الرقابة psiphon.ca و purevpn.com، و موقع الأخبار ultrasawt.com، الذي يبدو أن حجبهم تم بواسطة شكل ما من أشكال عرقلة اتصال بروتوكول طبقة المنافذ الآمنة بين خواديم المواقع و خواديم كلاودفلاير لتوزيع المحتوى.

الحملة الإعلانية

أدت تشوهات الشبكة التي تم الإبلاغ عنها في مصر عام 2016 إلى قيام OONI بإجراء تحقيق في الأمر، أدى إلى نشر تقرير بحثي كشف النقاب عن الوجود السري لما يبدو أنه حملة إعلانية. ووجد تحقيق OONI أن شركة واحدة على الأقل من مقدمي خدمات الإنترنت، وهي الشركة المصرية للاتصالات (TE)، كانت تستخدم تقنية Deep Packet Inspection (DPI) لإجراء هجمات لإعادة توجيه المستخدمين (الذين يحاولون الوصول إلى مواقع معينة، مثل المواد الإباحية ومواقع الجنس) لإعلانات بالعمولة أو برامج خبيثة.

قبل بضعة أشهر، نشر موقع (Citizen Lab) تقريرًا بحثيًا استند إلى تحقيقات OONI، كشف النقاب عن نطاق وحجم استخدام مصر لأجهزة DPI لتعدين العملات الرقمية بشكل سري من خلال الإعلانات بالعمولة والترويج لاستخدام العملة الرقمية المعماة (cryptocurrency) . وبشكل أكثر تحديدًا، وجدوا أن حقن الإعلان الذي كشفه OONI في عام 2016 كان على الأرجح نتيجة لأجهزة (Sandvine PacketLogic) وأن 17 من مقدمي خدمات الإنترنت المصريين (على الأقل) قاموا بهذا الحقن. كما وجدوا أن مقدمي خدمة الإنترنت أعادوا توجيه اتصالات المستخدمين غير المعماة (HTTPS) إلى أكواد برمجية لتعدين العملات الرقمية المعماة بالإضافة إلى محتوى مدر للدخل، مثل الإعلانات بالعمولة.

يتضمن تحليلنا لجميع قياسات شبكة OONI Probe التي تم جمعها من مصر خلال العام الماضي المئات من القياسات (التي تم جمعها من شركات مزودي خدمات متعددين) والتي تكشف إعادة توجيه اتصالات HTTP غير المعماة إلى الإعلانات بالعمولة و أكواد برمجية لتعدين العملات الرقمية المعماة، مما يشير إلى وجود حملة إعلانية.

لا يبدو أن مقدمي خدمة الإنترنت المصريين لديهم سياسة مشتركة فيما يتعلق بكيفية تنفيذ عمليات إعادة التوجيه. في بعض الحالات، يبدو أنها تنفذ سلسلة من عمليات إعادة توجيه HTTP، بينما في حالات أخرى، تقوم بتنفيذ عمليات إعادة توجيه

تعتمد على أكواد جافا سكريبت (والتي كانت أحيانًا مبهمة). وفي بعض الحالات الأخرى، يبدو أن عمليات إعادة التوجيه تتم مباشرة من خلال أجهزة الفحص العميق للحزم.

الجدول التالي يلخص كمية عمليات إعادة التوجيه التي عثرنا عليها لكل (ASN) في كل شهر بين يونيو 2017 و مارس 2018 (وبعدها لم نعثر على عمليات إعادة توجيه أخرى في قياسات OONI.

كذلك نعرض عينة من بعض الروابط المتأثرة وعمليات إعادة التوجيه في كل شهر، إضافة إلى إجمالي الاختبارات التي تظهر عمليات إعادة توجيه لكل ASN.

Traffic Sinks	Sample of Affected URLs	Affected ASNs & Redirect Count	Date
go.pub2srv[.]com, vidz4fun[.]com (via ceesty.com), rapidyl[.]net	islamic-relief.org, wilpf.org, 4genderjustice.org and 31 more.	28 — LINKdotNET, 23 — TE Data, 4 — Etisalat	**2017-06**
rapidyl[.]net	2 “dead” websites	23 — TE Data, 13 — LINKdotNET, 1 — Noor	**2017-07**
rapidyl[.]net	garem.org, ppsmo.org, and 9 more	54 — TE Data, 15 — LINKdotNET, 2 — Noor	**2017-08**
rapidyl[.]net	anpbolivia.com, crazyshit.com, ppsmo.org, and 4 more	30 — TE Data, 7 — LINKdotNET, 1 — Noor	**2017-09**
rapidyl[.]net	ppsmo.org and 2 more	32 — TE Data	**2017-10**

hitcpm[.]com (via vidz4fun), rapidyl[.]net, hitcpm[.]com	2 “dead” websites	29 — TE Data, 6 — LINKdotNET, 3 — Vodafone	**2017-11**
infads-1372369412.eu-west-1.elb.amazonaws[.]com, ylx-4.com, hitcpm[.]com	euthanasia.cc, sakhr.com, womeninblack.org, stshenouda.com and 34 more	60 — TE Data, 7 — LINKdotNET, 3 — Noor	**2017-12**
infads-1372369412.eu-west-1.elb.amazonaws[.]com, ylx-4.com	89.com, likud.org.il, and 4 more	3 — Vodafone, 2 — TE Data, 1 — LINKdotNET, 1 — Noor	**2018-01**
conceau[.]co, ylx-4[.]com (new ID)	bglad.com, guerrillagirls.com, and 2 more	3 — LINKdotNET, 2 — TE Data	**2018-02**
ylx-4[.]com	bglad.com and one more	2 — TE Data, 1 — LINKdotNET	**2018-03**

من الجدول أعلاه، يتضح أن خمسة من مقدمي خدمات الإنترنت المصريين (على الأقل) قاموا بحملة إعلانية بين يونيو 2017 و مارس 2018: Link Egypt و Telecom Egypt و Etisalat Misr و Noor و Vodafone.

استنادًا إلى قياسات OONI، أعاد مقدمو خدمات الإنترنت هؤلاء توجيه روابط HTTP غير المعماة إلى مواقع تستضيف خدمات الإعلانات بالعمولة. يتضمن الجدول أعلاه بعض الروابط المتأثرة لكل شهر، بما في ذلك: جمعية السجناء الفلسطينيين، والرابطة النسائية الدولية للسلام والحرية، ومبادرات المرأة من أجل العدالة بين الجنسين، والنساء في السواد.

تتوفر **هنا** معلومات تفصيلية مستندة إلى تحليلنا، والتي تعرض كل المواقع المتأثرة وعمليات إعادة التوجيه. لقد تأثرت مجموعة واسعة من المواقع المختلفة، بما في ذلك المواقع الإخبارية ومواقع حقوق الإنسان ومواقع مجتمع الميم ومواقع الـ

VPNوالمواقع الإسرائيلية والمواقع الإباحية. بل يبدو أن مقدمي خدمة الإنترنت المصريين يعيدون توجيه المستخدمين الذين يحاولون الوصول إلى مواقع الويب الخاصة بالأمم المتحدة، مثل un.org و ohchr.org.

ومن المثير للاهتمام أننا لم نعثر على أي عمليات إعادة توجيه أو آثار لحملة إعلانية بعد 9 مارس 2018، وهو التاريخ الذي تزامن مع نشر تقرير Citizen Lab البحثي حول هذا الأمر. ومع ذلك، لا يزال من غير الواضح ما إذا كانت الحملة الإعلانية قد انتهت أم لا، لا سيما أن غياب إعادة التوجيه في القياسات الأخيرة يمكن أن يُعزى إلى عدد آخر من العوامل.

على سبيل المثال يوضح الجدول أعلاه أن الروابط المختلفة قد تأثرت عبر الوقت، وأن عمليات إعادة التوجيه لم تحدث سوى لبعض الروابط لبضعة أشهر. ولذلك، لا يمكننا استبعاد إمكانية حدوث عمليات إعادة التوجيه لروابط أخرى لم يتم اختبارها على مدار الأشهر القليلة الماضية. حيث تقتصر نتائجنا على كم ونوع الروابط التي تم اختبارها خلال هذه الدراسة، فضلاً عن عنصر الانتقائية في اختيار الروابط (راجع أقسام منهجية و حدود الدراسة)

تجدر الإشارة إلى عمليات إعادة التوجيه التي وجدناها في قياساتOONI Probe ليست كلها ضارة أو تستهدف الربح. حيث قام مقدمو خدمة الإنترنت المصريون أيضا ببث إخطارات لإعلام المستخدمين بأنهم يستخدمون متصفحات قديمة (دون اقتراح متصفح معين، ولكن مع إعادة التوجيه إلى https://browsehappy.com/) وتذكيرهم بتحديث حساباتهم.

تحديد مكان الصناديق الوسيطة middleboxes

على مدار العام الماضي، أصبحت عملية تحديد أماكن الصناديق الوسيطة، كجزء من الحملات الإعلانية في مصر، أمرا أكثر صعوبة. في عام 2016، أفادت OONI أن تحليل زمن الاستجابة أظهر أن أدوات أجهزة الفحص العميق للحزم (DPI) كانت تُعيد التوجيه *قبل* أن يرسل موقع الويب رد الـ HTTP الخاص به، دون إنهاء الجلسة إلى الخدوم (وبالتالي إرسال أخطاء "Time Timeout 408") ساعد هذا في دحض فرضية المواقع التي يُحتمل أن تكون مصابة ببرامج ضارة كجزء من عمليات إعادة التوجيه إلى محتوى ضار.

إلا أن تقرير Citizen Lab الأخير يوضح أن عمليات إعادة التوجيه تم إرسالها عند استلام استجابة HTTP، بدلاً من استلام طلب HTTP ، مما يشير إلى أن مقدمي خدمات الإنترنت المصريين قد يكونوا بدلوا أدواتهم خلال العام ونصف العام الماضي، و يثير ذلك السؤال عما إذا كان ذلك من أجل ضبط الأدوات لتجنب الاكتشاف القائم على زمن الاستجابة.

نظرًا لأننا لم نعثر على عمليات إعادة توجيه في قياسات OONI الأخيرة بعد شهر مارس 2018 (كما هو مذكور في القسم السابق)، فإن قدرتنا على المزيد من التدقيق كانت محدودة.

الخلاصة

خلال العام الماضي، يبدو أن الرقابة على الإنترنت في مصر أصبحت أكثر ديناميكية وتطوراً وانتشاراً.

طوال فترة الاختبار أظهر أكثر من 1000 رابط نوعا ما من الاضطراب على الشبكة، اتصفت 178 منها باستمرار نسبة

عالية من حالات فشل بروتوكول نقل النص التشعبي (HTTP)، مما يشير بقوة إلى أنه تم حجبها. وبدلاً من حجب الصفحات مباشرة، يبدو أن مقدمي خدمة الإنترنت المصريين يحجبون المواقع في المقام الأول من خلال استخدام تقنية Deep Packet Inspection (DPI) التي تعيد توجيه الاتصالات. ويبدو أن الحجب أصاب كلا من المواقع التي تستخدم بروتوكول بروتوكول نقل النص التشعبي (HTTP) بروتوكول نقل النص التشعبي الآمن (HTTPS)

في بعض الحالات، يبدو أن مقدمي خدمات الإنترنت يسقطون حزما، مما يشير إلى تنوع في قواعد التصفية. في حالات أخرى، يبدو أن مقدمي خدمات الإنترنت يتدخلون في حركة مرور طبقة المنافذ الآمنة (SSL) بين موقع تواجد الكلاودفير في القاهرة والخوادم لمواقع الويب خارج مصر. تشير قياسات الكمون (Latency) على مدار العام والنصف الماضي أيضًا إلى أن مقدمي خدمات الإنترنت المصريين قد يكونوا بدلوا أدوات التصفية (Filtering) الخاصة بهم، مما يجعل الكشف عن الصناديق الوسيطة أمرا أكثر صعوبة.

يبدو أن أكثر من 100 رابط خاص بالمؤسسات الإعلامية قد تم حجبها، على الرغم من أن السلطات المصرية أمرت بحجب 21 موقعًا إخباريًا فقط في العام الماضي. وتشمل هذه المواقع الإخبارية مواقع مصرية (مثل مدى مصر والمصريون ومصر العربية وديلي نيوز إيجيبت)، بالإضافة إلى المواقع إعلامية الدولية (مثل الجزيرة وهافينغتون بوست العربية). في محاولة للالتفاف على الرقابة، استخدمت بعض المؤسسات الإعلامية المصرية نطاقات بديلة، لكن (في حالات قليلة) تم حجبها كذلك.

من خلال المقابلات، أفاد عاملون في المواقع الإعلامية المصرية المحجوبة بأن الرقابة كان لها تأثير كبير على عملهم. بالإضافة إلى عدم قدرتهم على النشر وفقدانهم قطاعا من جمهورهم، كان للرقابة تأثير مالي على أعمالهم ومنعت المصادر من السعي إلى التواصل مع الصحفيين. عدد من المؤسسات الإعلامية المصرية علق أعماله تماما نتيجة الرقابة المستمرة على الإنترنت.

يبدو أن العديد من المواقع الإلكترونية الأخرى، غير الإعلامية، قد تم حجبها أيضًا. وتشمل هذه المواقع مواقع حقوق الإنسان (مثل هيومن رايتس ووتش، ومنظمة مراسلون بلا حدود، والشبكة العربية لمعلومات حقوق الإنسان، والمفوضية المصرية للحقوق والحريات، ومرصد الصحفيين ضد التعذيب) والمواقع التي تقدم نقدا سياسيا (مثل حركة شباب 6 أبريل) مما يثير مسألة ما إذا كانت قرارات الرقابة مدفوعة سياسيا.

يبدو أن مقدمي خدمات الإنترنت المصريين يطبقون تكتيكات "الدفاع في العمق" لتصفية الشبكات من خلال إنشاء طبقات متعددة من الرقابة التي تجعل التحايل أكثر صعوبة. ما يشير إلي ذلك، جزئيا، هو عملية حجب العديد من مواقع تجاوز على الرقابة، مثل: hotspotshield.com، torproject.org و psiphon.ca فضلا عن حجب واسع النطاق لشبكة Tor. ، وفي بعض الحالات، يبدو أن جسور Tor محجوبة كذلك

ما يبرز بوضوح كاستراتيجية "دفاع في العمق" هو حجب موقع حزب الحرية والعدالة في مصر (FJP). تشير اختباراتنا إلي أنه تم حجب نسختين من هذا الموقع، هما (http://www.fj-p.com و http://fj-p.com) بواسطة صندوقين وسيطين مختلفين. وبذلك، أضاف مقدمو خدمات الإنترنت المصريون طبقات إضافية من الرقابة، لضمان أن يحتاج تجاوز على الحجب المزيد من الجهد.

في حين لا يزال المبرر القانوني وراء حجب جميع هذه المواقع غير واضح، إلا انه يمكن على الأرجح أن يعزى إلى عدد من القوانين المصرية، مثل المادة 3 من قانون الطوارئ أو المادة 29 من قانون مكافحة الإرهاب. كما يشير إلى ذلك ما نشر في مايو 2017 بحجب بعض المواقع الإعلامية على أساس أنها "تدعم الإرهاب والأكاذيب"، بالاستناد إلى هذه القوانين. وعلاوة على ذلك، كشف الجهاز القومي لتنظيم الاتصالات عن حجب موقع قناة "الشروق" على الإنترنت بناءً على طلب من لجنة التحفظ وإدارة أموال جماعة الإخوان المحظورة . تضمن هذا الطلب أيضًا حجبًا لعدد من المواقع الإعلامية الأخرى.

بخلاف الرقابة، يبدو أن مقدمي خدمة الإنترنت المصريين يقومون بحملة إعلانية أيضًا. تظهر المئات من قياسات شبكة OONI Probe (التي تم جمعها من ASNs متعددة) إعادة توجيه اتصالات HTTP غير المعماة إلى إعلانات بالعمولة و أكواد برمجية لتعدين العملات الرقمية المعماة. يبدو أن مقدمي خدمة الإنترنت المصريين يستخدمون أجهزة الفحص العميق للحزم DPI (أو أدوات مماثلة) لاختراق الاتصالات غير المعماة وحقن عمليات إعادة التوجيه، و لا يبدو أن لديهم سياسة مشتركة فيما يتعلق بكيفية تنفيذ عمليات إعادة التوجيه هذه. لقد تأثرت مجموعة واسعة من الروابط المختلفة، بما في ذلك جمعية السجناء الفلسطينيين، ومبادرات النساء من أجل العدالة بين الجنسين، ومواقع الميم، ومواقع الـ VPN، والمواقع الإسرائيلية، بل وحتى المواقع الخاصة بالأمم المتحدة، مثل un.org و ohchr.org. .

في حين أن بعض القوانين المصرية قد تبرر الرقابة التي تم الكشف عنها في هذه الدراسة، إلا أن تبرير الحملة الإعلانية يظل غير واضح. كان الهدف من هذه الدراسة هو فحص الرقابة من خلال تحليل قياسات الشبكة، دعما للجهود البحثية المستقبلية وللنقاش العام.

شكر

نشكر جميع المتطوعين في مصر الذين أداروا ويواصلون تشغيلOONI Probe، مما جعل هذا البحث ممكنًا.