حرية استخدام برمجيات الإنترنت والأنشطة المحظورة

دعم حقوق الإنسان دون تمكين المجرمين

ساشا رومانوسكي (Sasha Romanosky)، مارتن سي ليبيكي (Martin C. Libicki)، زيف مينكلمان (Zev Winkelman)، أوليسيا تكاشيفا (Olesya Tkacheva)

RAND CORPORATION

NATIONAL SECURITY RESEARCH DIVISION RAND

حرية استخدام برمجيات الإنترنت والأنشطة المحظورة

دعم حقوق الإنسان دون تمكين المجرمين

ساشا رومانوسكي (Sasha Romanosky)، مارتن سي ليبيكي (Martin C. Libicki)،
زيف مينكلمان (Zev Winkelman)، أوليسيا تكاشيفا (Olesya Tkacheva)

مُعد لوزارة الخارجية الأمريكية

بيانات النشر المفهرسة لدى مكتبة الكونجرس

الرقم المعياريّ الدولي للكتاب: 978-0-8330-9110-9

تم النشر بواسطة Corporation RAND، Monica Santa، Calif.

مؤسسة RAND هي منظمة بحثية تعكف على تطوير حلول للتحديات التي تواجه السياسات العامة وذلك للمساعدة في جعل المجتمعات في جميع أنحاء العالم أكثر أمانًا وسلامةً وصحةً وازدهارًا. مؤسسة RAND هي مؤسسة غير ربحية وحيادية وملتزمة بالصالح العام.

لا تعكس منشورات مؤسسة RAND بالضرورة آراء عملاء ورعاة الأبحاث الذين يتعاملون معها.

تمهيد

أجريت هذه الدراسة في مركز سياسات الدفاع والأمن الدولي التابع لمعهد أبحاث RAND للأمن القومي لصالح وزارة الخارجية الأمريكية، مكتب الديمقراطية وحقوق الإنسان والعمل، وذلك بناءً على طلب من الكونجرس الأمريكي. وقد أجرى معهد أبحاث RAND للأمن القومي بحوثًا وتحليلات بشأن موضوعات الدفاع والأمن القومي للولايات المتحدة والمجتمعات والمؤسسات المتحالفة معها والمعنية بالدفاع والسياسة الخارجية والأمن الداخلي ومجموعات الاستخبارات وغيرها من المنظمات غير الحكومية التي تدعم تحليل الدفاع والأمن القومي.

لمزيدٍ من المعلومات حول مركز سياسات الدفاع والأمن الدولي يرجى زيارة الموقع الإلكتروني http://www.rand.org/nsrd/ndri/centers/isdp.html أو الاتصال بالمدير (معلومات الاتصال مسجلة في صفحة الويب).

المحتويات

الأشكال والجدول

الأشكال

الجداول

الملخص

يقدم مكتب الديمقراطية وحقوق الإنسان والعمل التمويل لمحفظة رئيسية (والمشار إليها لاحقًا بعبارة "المحفظة") تهدف إلى "تعزيز الحريات الأساسية وحقوق الإنسان، وحرية تدفق المعلومات على الإنترنت".[1] ويتحقق هذا الهدف من خلال تمويل أنواع مختلفة من المشاريع، صُمِمَ كل منها بغية "تعزيز الحقوق والحفاظ على كرامة فئات السكان الضعيفة والأكثر عرضةً للخطر ... [والتي] تشمل النساء والمثليين وثنائيي الجنس والمتحولين جنسيًا (LGBT) وكذلك الأقليات الدينية والعرقية، والأشخاص ذوي الإعاقة".[2]

على سبيل المثال، يدعم مكتب الديمقراطية وحقوق الإنسان والعمل بعض التقنيات التي توفر وصولًا حرًا ومفتوحًا إلى المعلومات على الإنترنت وتجاوز الرقابة المفروضة على معلومات الإنترنت، هذا فضلًا عن تقنيات الاتصالات الآمنة التي تساعد على حماية شبكة الإنترنت ورسائل المحمول من المراقبة والتنصت. إضافة إلى ذلك، يدعم مكتب الديمقراطية وحقوق الإنسان والعمل جهود التدريب وبرامج السلامة الرقمية التي توفر معلومات مهمة، ومساعدة جوهرية للنشطاء المعرضين للخطر بنسبة عالية وأولئك الذين يعيشون في دول قمعية. كما يسعى المكتب جاهدًا لدعم (1) المشاريع البحثية التي تقيم فعالية جهود حرية الإنترنت و(2) جهود التأييد التي من شأنها تمكين المجتمع المدني من توعية صناع السياسات الوطنية والدولية بشأن التهديدات التي تواجه الوصول الحر والمفتوح للمعلومات، فضلًا عن الحلول المحتملة للحد من المخاطر. وعلاوة على ذلك، يُشجِّع المكتب بقوة وفعالية تطوير التقنيات التي

[1] راجع وزارة الخارجية الأمريكية، الإنسان، وحرية استخدام الإنترنت "بيان البرنامج السنوي لحرية استخدام الإنترنت الصادر عن مكتب الديمقراطية وحقوق الإنسان والعمل"، صفحة إنترنت، 2 يونيو / حزيران 2014.

[2] وزارة الخارجية الأمريكية، 2014.

تتوافر باعتبارها برمجيات مفتوحة المصدر والمشروعات التي تؤسس وتعزز شراكات قوية مع المنظمات المحلية وجماعات حقوق الإنسان.[3]

وفيما يتعلق بتخصيص الأموال لمكتب الديمقراطية وحقوق الإنسان والعمل (إضافةً إلى الوكالات الحكومية الأخرى التي تقدم مساعدات خارجية لحرية الإنترنت)، أعرب الكونجرس تشريعيًا عن مخاوفه المتمثلة في أن تلك المشاريع قد تُستخدم بواسطة المجرمين لمواصلة ارتكاب أنشطة غير مشروعة وتهربهم من العدالة. على سبيل المثال،

> يشترط أيضًا أن تخضع تقنيات المراوغة والتحايل والبرامج المدعومة بواسطة الأموال الموفرة بمقتضى هذا القانون، للمراجعة، بحيث تشمل تقييمًا للحماية من استخدام أي تقنيات من هذا القبيل في أغراض غير مشروعة ... بما يشمل تقييم نتائج استخدام تلك البرامج، والتدابير الاحترازية في مواجهة استخدام تقنية المراوغة والتحايل في أغراض غير مشروعة أو غير قانونية.[4]

ولقد طلب مكتب الديمقراطية وحقوق الإنسان والعمل من مؤسسة [RAND] فحص ودراسة محفظة المكتب لتحديد نطاق إمكانية استخدام المشروعات التي يمولها في أغراض غير مشروعة - وعلى وجه التحديد، تقرير ما إذا كانت مشاركة المكتب قد أدت إلى زيادة احتمالات الاستخدام غير المشروع.[5] يُرجى الملاحظة أن هذا التقرير لا يقدم تقييمًا صريحًا للفوائد التي تعود بها تلك المشاريع على استيفاء وتحقيق أهداف حقوق الإنسان، وإن كان العمل السابق لمؤسسة [RAND] قد أدى هذا الغرض تحديدًا.[6] جُمِعَت معلومات حول كل مشروع من خلال مجموعة المعلومات المعلنة والمتاحة للجمهور؛ وذلك من خلال لقاءات شخصية ومحادثات عبر الهاتف والبريد الإلكتروني مع الجهات المستفيدة؛ كما قدم مكتب الديمقراطية وحقوق الإنسان والعمل بعض الوثائق والمستندات.

---

[3] وزارة الخارجية الأمريكية، 2014.

[4] مجلس النواب الأمريكي، تقرير المجلس *331-112* -- قانون البنية العسكرية وشؤون المحاربين القدماء والمخصصات الوكالات ذات الصلة لعام *2012*، 2012

[5] في هذه الوثيقة، أخذنا في الاعتبار استخدام عبارة النشاط غير المشروع كمرادفة لعبارة "النشاط الإجرامي" (كما هما مقرر في قانون الولايات المتحدة).

[6] راجع Ryan Henry, Stacie L. Pettyjohn, and Erin York, Portfolio Assessment of Department of State Internet Freedom Program: An Annotated Briefing, Santa Monica, Calif.: RAND Corporation, WR-1035-DOS, 2014.

ولقد طبقنا منهجية صُممت خصيصًا بهدف تقديم نتائج موثوقة وقابلة للتكرار. بدايةً، نضع وصفًا للتكنولوجيا التي يقوم عليها البرنامج، أو الخدمة التي يقدمها وفائدتها في تعزيز مهمة ورسالة مكتب الديمقراطية وحقوق الإنسان والعمل المتمثلة في تعزيز حرية الإنترنت في سائر أنحاء العالم. بعدئذٍ، نجري الاختبار التالي، المؤلف من ثلاثة أجزاء، كوسيلة لدراسة إمكانية استخدام التكنولوجيا أو الخدمة في أغراض غير مشروعة: هل توفر حلًا لمشكلة اتصال المجرمين؟ هل تمنح للمجرمين ميزة مهمة؟ هل يستطيع المجرمون الوصول إلى الأداة بسهولة ويسر؟ أخيرًا، وبناءً على نتائج الاختبار، نقيم ما إذا كانت مشاركة المكتب قد أفضت إلى زيادة احتمال استغلال المشروع في أغراض غير مشروعة.

نظرًا للطبيعة الحساسة للعديد من المبادرات الحاصلة على تمويل -والمخاوف بشأن سلامة نشطاء حقوق الإنسان الذين يستفيدون من تلك المشاريع- حذفنا الأسماء الحقيقية للمشاريع مع استثناء وحيد هو (Tor: الشبكة المجهولية). واستعضنا عن ذلك بدراسة مجموعات من الخدمات والتقنيات ذات الصلة. المجموعات الخاضعة للفحص والدراسة هي: السلامة الرقمية، ومضادات هجوم حجب الخدمة [DDoS]، والشبكات المتداخلة، والوكلاء / الشبكات الظاهرية الخاصة [VPNs]، والاتصالات المتنقلة الآمنة، والشبكة المجهولية [Tor]، وفئة أخيرة تصف مشروعين إضافيين. يرجى الملاحظة أننا نقدم تحليلًا موسعًا للشبكة المجهولية [Tor] نظرًا لقدراتها الفريدة واستخدامها واسع النطاق.

ولقد استنتجنا من التحليل الذي أجريناه أنه ليس من المرجح أن تتيح مشروعات السلامة الرقمية والمشروعات المضادة لهجوم حجب الخدمة القيام بنشاط غير مشروع، نظرًا لأنها إما توفر مواد تدريب بسيطة أو تستوجب علاقات مباشرة مع العملاء بما يجعلها مُقيدة بشدة لأي استخدام غير مشروع للخدمات.

وتوفر مشروعات الشبكات المتداخلة تطبيقات متنقلة تؤدي إلى تمكين بنى تحتية للشبكة المتخصصة ذات النطاق الترددي المنخفض عبر مناطق جغرافية صغيرة. ورغم أنه من الممكن نظريًا استخدامها لتيسير أي نشاط غير مشروع، إلا أنه من المرجح أن يلجأ أي مجرم يسعى لعدم الكشف عن هويته أو تشفيرها إلى تقنيات بديلة. وهناك أيضًا العديد من تطبيقات الشبكة الشعرية المتنافسة، وبالتالي، تشير هذه العوامل مجتمعةً إلى عدم ترجيح استخدام مشروعات الشبكة الشعرية في أغراض غير مشروعة.

وتسمح مشروعات الوكيل / الشبكة الظاهرية الخاصة للمستخدمين بتوجيه حركتهم على الإنترنت من خلال حاسب متصل بالشبكة عبر وسيط، من أجل تجاوز الرقابة والتمتع بحرية الوصول إلى خدمات الإنترنت العامة. ورغم أن هذه التقنيات قد تقوم بتشفير الاتصال بين المستخدم وخادم الترحيل، إلا أنها لا تضمن الإخفاء

المحكم للهوية، نظرًا لإمكانية قيام مُشَغِّل خادم الترحيل بمراقبة الرسائل. من جهة أخرى، يمكن للدول القمعية حجب خدمة الشبكة الظاهرية الخاصة، مما يخفض مستوى اندفاع الجهات الإجرامية لاستخدام هذه التقنيات. ولئن كان أداء الشبكات الظاهرية الخاصة، بوجهٍ عام، يجعلها جاذبة ومغرية لبعض المجرمين، إلا أن انتشار حلول الشبكات الظاهرية الخاصة غير الموجودة في الولايات المتحدة الأمريكية يشير إلى أنه ليس من المرجح أن تستخدم تلك المشروعات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل في أغراض غير مشروعة.

توفر مشاريع الاتصالات المتنقلة الآمنة قدرات نصية وصوتية وخدمات تراسل مؤمنة. وبينما تعرض خدمة تشفير الرسائل ميزة السرية، إلا أن إخفاء اسم المُرسِل ليس الميزة الأساسية فيها. ويتطلب أي نشاط غير مشروع تقنيات إضافية للتأكد من استحالة الربط بين المُرسِل وبين الرسالة التي أرسلها (عدم قابلية الربط). وثمة تقنيات بديلة تقدم ميزات مماثلة، مما يقلل احتمال استخدام مشاريع الاتصالات المتنقلة الآمنة في أغراض غير مشروعة.

يساعد مشروع الشبكة المجهولية [Tor] المستخدمين في تجاوز الرقابة وتجنب خطر كشف الهوية بفعل بنيته الموزعة وتشفيره متعدد الطبقات. ومع ذلك، فهذه الحماية ليست مطلقة. إذ يبقى مستخدمو هذه التقنية بهدف تحقيق أغراض غير مشروعة عرضة لارتكاب أخطاء والكشف عن هويتهم بأساليب التحقيق القانونية. علاوةً على ذلك، فإن بطء الأداء الذي تسببه البنية الموزعة قد يكفي لردع أي نشاط ذي نطاق ترددي عالي. ويشير فحص البيانات المتوفرة إلى أن جزءًا كبيرًا من حركة الشبكة المجهولية [Tor] هي حركة تقليدية (غير مُشفَّرة)، وكذلك حركة تبادل الملفات من نظير إلى نظير [P2P] (والتي تكون بعضها ملفات محفوظة الحقوق). وتُظهِر بيانات أخرى أن الوجهات الأكثر شيوعًا لحركة الشبكة المجهولية [Tor] هي البحث ووسائط التواصل الاجتماعي ومواقع مشاركة الملفات، في حين أن نسبة مستخدميها في الولايات المتحدة لا تتعدى 13 % من إجمالي الطلبات على الشبكة المجهولية. وليست خدمات الترجمة وبرامج التوعية وتمكين أنشطة حقوق الإنسان وتعزيز الشفافية، من خلال بيانات التعريف، إلا بضعة تدابير احترازية تستخدمها الشبكة المجهولية [Tor] لضمان الاستخدام الأمثل لهذه التقنية. وفيما قد تزيد شعبية وتطور هذا المشروع من احتمال استخدامه في أغراض غير مشروعة، لا توفر هذه التقنية قدرات جديدة غير القدرات التي كانت توفرها قبل تلقي أي تمويل من مكتب الديمقراطية وحقوق الإنسان والعمل. ومن ثم يمكننا استنتاج أن تمويل المكتب للشبكة المجهولية [Tor] لم يؤدِّ إلى زيادة احتمال استخدام هذا المشروع في أغراض غير مشروعة.

أخيرًا، ندرس مشروعين آخرين يتلقيان تمويل في إطار حافظة مكتب الديمقراطية وحقوق الإنسان والعمل: يوفر أولهما تطبيقًا للهاتف النقال وجهاز الحاسب، وهو مفيد للتخزين الآمن عبر الإنترنت، بينما يهدف الثاني إلى توفير خصوصية الإنترنت من نظام التشغيل القابل للتمهيد والتحميل على محرك الأقراص المحمول [USB]. ويتوافر مع كل مجموعة من تلك المجموعات عدد من الحلول البديلة التي من شأنها منع زيادة احتمال استخدام هذه الأدوات في أغراض غير مشروعة.

باختصار، خلص هذا البحث إلى أنه لا يوجد، في معظم الحالات، سوى عدد قليل من الأدلة على أن الأدوات المموَّلة في إطار هذا البرنامج تساعد على تنفيذ أنشطة غير مشروعة من الناحية المادية، في مقابل الأدوات الموجودة مسبقًا أو غير المشمولة في المحفظة. في المقابل، يجد هذا البحث أن هذه الأدوات تقدم، بل وقدمت بالفعل، قدرات وإمكانات بالغة الأهمية لمستخدمي الإنترنت (غير المجرمين منهم) - نشطاء حقوق الإنسان تحديدًا - إما لأنها متاحة مجانًا وسهلة الاستخدام ومسوقة ومتاحة فقط لأنصار حقوق الإنسان، أو لأنها تعمل باللغة الأصلية للمستخدم. علاوةً على ذلك، ونظرًا للوفرة والتنوع في أدوات وتقنيات الخصوصية والأمن والوسائط الاجتماعية الأخرى، ثمة بدائل عديدة يرجح أن تكون أكثر ملاءمة للاستخدام في الأنشطة الإجرامية، إما بسبب انخفاض المراقبة وإمكانات إنفاذ القانون أو بسبب قلة القيود المفروضة على إتاحتها أو نظرًا لكونها أعدت خصيصًا من قبل المجرمين لتناسب احتياجاتهم الخاصة.

شكر وعرفان

يود الكتَّاب التقدم بخالص الشكر إلى ريان هنري (Ryan Henry)، وسيث جونز (Seth Jones)، وستاسي بيتيجون (Stacie Ettyjohn) وستة من أجهزة الشرطة والمباحث، ومحامي وزارة العدل السابق مُغفَل الاسم وباحث قانوني مُغفَل الاسم وكثير من خبراء الأمن والخصوصية وحرية الإنترنت، وذلك على إسهاماتهم وأفكارهم القيمة.

الاختصارات

DDoS	هجوم حجب الخدمة الموزعة
DRL	مكتب الديمقراطية وحقوق الإنسان والعمل (وزارة الخارجية الأمريكية)
FBI	مكتب التحقيقات الفيدرالي
LGBT	المثليون وثنائيو الجنس والمتحولون جنسيًا
NGO	مؤسسة غير حكومية
P2P	نظير إلى نظير
Tor	التوجيه البصلي "شبكة مجهولية"
VPN	شبكة ظاهرية خاصة

مقدمة

يمول مكتب الديمقراطية وحقوق الإنسان والعمل التابع لوزارة الخارجية الأمريكية مشروعًا ضخمًا يهدف إلى تعزيز حرية استخدام الإنترنت (يُعرف باسم "الحافظة") حيث توجه أموال الحافظة إلى تمويل مجموعة من الأدوات (والخدمات المصاحبة لها) بغية مقاومة جهود الحظر التي تبذلها الحكومات القمعية لتقييد المحتويات المتاحة على الإنترنت أو الاستخدام العام للإنترنت، بالإضافة إلى محاولة تلك الحكومات لمقاضاة الأفراد ممن يقتصر جرمهم على ممارسة أحد الأركان الرئيسة لحرية التعبير التي نصت عليها المادة 19 من إعلان الأمم المتحدة لحقوق الإنسان.[1] ولقد أعرب الكونجرس تشريعيًا عن قلقه بشأن استخدام الأموال المخصصة لهذا الغرض من مكتب الديمقراطية وحقوق الإنسان والعمل، وطلب "توصيف سبل الوقاية التي تتخذها الهيئات والوكالات المعنية لضمان عدم استخدام تلك البرامج في أغراض إجرامية".[2] وتم توجيه طلب إلى مؤسسة RAND للقيام بفحص وتقييم المحفظة لتحديد النطاق المحتمل لاستخدام تلك الأموال في أغراض إجرامية وتقديم توصياتها بالمعايير التي يفضل استخدامها مستقبلًا لتقييم البرامج.[3]

بناءً على ذلك، قمنا بفحص مزايا تلك الأدوات ودورها في تعزيز حرية استخدام الإنترنت؛ واحتمال استخدامها في أغراض إجرامية؛ وتقديم الأدلة التي تثبت الاستخدام

[1] لكل شخص الحق في حرية الرأي والتعبير، ويشمل هذا الحق حرية اعتناق الآراء دون أي تدخل، واستقاء الأنباء والأفكار وتلقيها والتأثير فيها بأية وسيلة كانت دون تقيد بالحدود الجغرافية.

[2] مجلس الشيوخ الأمريكي تقرير مجلس الشيوخ رقم *113-81* بشأن قانون وزارة الخارجية للشئون الخارجية والبرامج ذات الصلة لعام *2014*، 2014.

[3] واقتصر تقييمنا على حرية استخدام الإنترنت، عوضًا عن المفهوم الأشمل لقيم الولايات المتحدة مثل الحقوق الاجتماعية ومكافحة التمييز.

غير الشرعي لها، حيث أمكن.[4] وخلال عملنا، أخذنا في الاعتبار مدى إمكانية دعم الأدوات، التي سبقت برنامج مكتب الديمقراطية وحقوق الإنسان والعمل، أو تطورت من دون الاستفادة منه، لممارسات غير شرعية. أخيرًا، درسنا التدابير الوقائية الممكنة، والتي من شأنها إحباط محاولات استخدام التقنيات المذكورة لأغراض إجرامية.

[4] في حين يشكل فهم سياق حقوق الإنسان الذي تنطوي عليه تلك الأدوات ركنًا هامًا تقدير استخداماتها المحتملة، إلا أنه يعتبر أيضًا محورًا رئيسيًا لتحليل الاستخدامات الإجرامية المحتملة لتلك الأدوات.

ما الهدف من أدوات حرية استخدام الإنترنت؟

تهدف جهود حماية حرية استخدام الإنترنت إلى تعزيز الديمقراطية وحقوق الإنسان في جميع أنحاء العالم، من خلال تأمين وصول آمن إلى شبكة الإنترنت العالمية. وتُنفَّذ هذه الجهود عبر مجموعة مختلفة من المبادرات تشمل التعليم والتدريب وحملات التوعية، وتكنولوجيا المعلومات والبرمجيات، التي تعمل متضافرة لتوفير مصادر مفتوحة وحرة للاتصال بالإنترنت، من دون الخضوع للرقابة أو التنصت أو آثار ممارسات الحكومات القمعية. فعلى سبيل المثال، يساعد بعض تلك التطبيقات شائعة الاستخدام في ضمان سلامة وأمان وخصوصية مستخدمي الإنترنت (ونعني بمصطلح "مستخدمي الإنترنت"، في هذا التقرير، مستخدمي الإنترنت من غير المجرمين) عن طريق إخفاء المصدر الأساسي لاتصالاتهم ونقلها عبر أجهزة خوادم وسيطة عبر العالم، وتشفير رسائلهم.

ينتفع الكثير من الناس من إمكانيات حماية الخصوصية والأمان التي توفرها الأدوات التي يناقشها هذا التقرير.

فعلى سبيل المثال، يستخدم المُعارضون ونشطاء حقوق الإنسان تلك الأدوات لتبادل المعلومات حول التنكيل والقمع الذي يتعرضون له. كما يستخدم الصحفيون هذه التقنيات في تحميل ملفات الفيديو التي يوثّقون من خلالها انتهاكات حقوق الإنسان وجرائم الحرب. ويستخدم الأفراد الذي يقعون تحت وطأة أنظمة قمعية قاسية هذه الأدوات للتحايل على الرقابة التي تفرضها الحكومة ليستطيعوا الوصول إلى الإنترنت.[1]

[1] فعلى سبيل المثال، أقرت دولة غامبيا مؤخرًا قانون لفرض عقوبة جنائية تصل إلى 100,000 دولار أمريكي والحبس لمدة 15 عامًا على من يستخدمون الإنترنت في "نشر أخبار كاذبة ضد الحكومة، وإثارة التمرد والتشجيع على أعمال العنف، والتحريض على معارضة ومهاجمة الشخصيات السياسية والعامة". أنظر مقالة Modou S. Joof, "'Internet Is Being Used as a Platform for Nefarious and Satanic Purposes,'" Front Page International, July 28, 2013.

بينما يستخدم آخرون تلك الأدوات لمنع الكشف عن هوياتهم الرقمية، والتي قد يتم تسريبها أو تتبعها أثناء تصفحهم للإنترنت. وليس لدى هؤلاء الأفراد ما يخفونه، كونهم لا يمارسون أي أنشطة غير شرعية - ولكن لديهم حساسية عالية تجاه ما يتعلق بالخصوصية، ويفضلون عدم تتبع أنشطتهم من تصفح الأخبار وشبكات التواصل الاجتماعي أو خدمات التجارة الإلكترونية عبر الإنترنت.

تفضل المنظمات الأكاديمية والإخبارية استخدام تلك الأدوات في إجراء الأبحاث واللقاءات وعند رغبتها في نقل الوثائق التي تحتوي على معلومات حول ممارسات فساد في الشركات والحكومات، من دون الكشف عن مصدرها. كما تلجأ الأقليات الدينية والمثليون وثنائيو الجنس والمتحولون جنسيًا (LGBT) والأقليات العرقية إلى استخدام التقنيات الخاصة لحماية سلامتهم والتواصل بحرية دون الكشف عن هوياتهم، وذلك لخوفهم من التعرض للأذى إذا كُشف عن هوياتهم.

ويستخدم ضباط ومسؤولو تطبيق القانون في الولايات المتحدة، وفي جميع أنحاء العالم، تلك الأدوات للعمل خفيةً خلال عملهم لإيجاد المجرمين وتتبعهم واعتقالهم. تتيح مزايا إغفال الهوية في تلك الأدوات للعملاء إمكانية إخفاء المصدر الرئيسي لاتصالاتهم عند الاتصال عبر الشبكات الحكومية.

أخيرًا، تعمل العديد من المنظمات غير الحكومية الأمريكية والدولية على تدريب ودعم مجموعات دولية، والتي تعمل بدورها على تدريب مواطنين محليين على كيفية الاستخدام الآمن والصحيح للإنترنت. فعلى سبيل المثال، تعمل إحدى المنظمات الأمريكية غير الحكومية على توفير حواسب محمولة آمنة لمجموعات محلية في دول أجنبية، وتكون مزودة بمعلومات حول الرسائل الإلكترونية المشفرة، وتشفير محتويات الأقراص الصلبة، وأدوات حماية كلمات المرور القوية بهدف حماية سلامة الحواسب الإلكترونية والمعلومات المخزنة عليها.

أكد الدليل التجريبي أن هناك إقبالًا شديدًا على استخدام تقنيات حماية حرية استخدام الإنترنت وخصوصًا بعد اندلاع العديد من الأحداث الدرامية مثل الثورات. وفي بعض الحالات، أظهرت البيانات أيضًا تراجعًا كبيرًا في أنشطة الإنترنت بسبب الضوابط الرقابية التي تفرضها الحكومة. فعلى سبيل المثال، أظهرت البيانات الواردة في تقارير إحدى الأدوات المضادة للرقابة في النشاط اليومي للمستخدم (مقاسًا بعدد الطلبات المقدمة من المستخدم عبر شبكة الإنترنت) ارتفاعًا واضحًا في تونس، حيث ارتفع من خمسة ملايين نقرة إلى أكثر من 30 مليون نتيجة في يناير 2011، عندما بدأ النشطاء والصحافيون في نشر رسائلهم عبر العالم. وبالمثل، ارتفع النشاط اليومي للمستخدمين الليبيين من بضعة مئات الآلاف إلى ما يقارب 30 مليون نقرة خلال الفترة من منتصف فبراير حتى مارس 2011 (إبان الثورة ضد العقيد معمر القذافي) وقبل

انقطاعه تمامًا بشكل مفاجئ. كما شهدت الثورة المصرية المنحى نفسه -حيث ارتفعت النتائج من بضعة ملايين إلى أكثر من 60 مليون نقرة يوميًا. ويمكن الحصول على نماذج مشابهة من فيتنام وباكستان والصين.

يوضح الشكل رقم 2.1 نتائج اختبارات Tor (أو ما يعرف باسم The Onion Router) لنشاط استخدام الإنترنت في مصر وليبيا خلال عام 2011. يوضح الجانب الأيمن استخدام ما شهده ارتفاع عدد مستخدمي برنامج Tor في مصر من 500 مستخدم يوميًا ليصل إلى 2000 في أوائل عام 2011. وقد تزامن هذا التزايد مع اندلاع أحداث ثورة 25 يناير، والتي أدت إلى الإطاحة بالرئيس حسني مبارك.[2] ويوضح الجانب الأيسر من الشكل رقم 1 عدد مستخدمي Tor في ليبيا، والذي شهد تزايدًا في أوائل عام 2011، حيث ارتفع من حوالي 50 مستخدم يوميًا ليصل إلى 300. وقد حدث هذا الارتفاع الكبير إبان اندلاع الحرب الأهلية في ليبيا اعتبارًا من 16 فبراير 2011، والتي انتهت بمقتل العقيد معمر القذافي.[3] كما يظهر الجانبان أيضًا انخفاضًا لاحقًا في تصفح الإنترنت غير المشفّر عن جهة الرقابة الحكومية.

على الرغم من تصميم مشروعات حرية استخدام الإنترنت وتطويرها وتوزيعها بهدف حماية وتعزيز حقوق الإنسان والحريات في جميع أنحاء العالم، إلا أنه يمكن أن يُساء استخدامها في أنشطة غير شرعية - كما هو الحال مع جميع وسائل التكنولوجيا. فالتكنولوجيا التي تساعد سيارات الإسعاف على الإسراع للوصول إلى المستشفى لإنقاذ الأرواح، تُتاح، هي ذاتها، لسيارات ناهبي البنوك أثناء هروبهم. والتكنولوجيا التي تمكن المتمردين في الدول الفاشية من التواصل فيما بينهم لدراسة واستعراض حدود الحريات في تلك الدول، تسمح أيضًا لممارسي الأنشطة الإجرامية بالتواصل فيما بينهم، كالاتجار بالمخدرات، على سبيل المثال، في الدول الديمقراطية التي تحترم سيادة القانون. وهذا هو الحال أيضًا مع التكنولوجيا والخدمات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل.

فعلى سبيل المثال، يستخدم عملاء الاستخبارات الذين يعملون في مناطق خاضعة لسلطة حكومات أجنبية، أساليب الحماية والسرية ذاتها لتنفيذ مهام الاستطلاع ومكافحة التجسس لجمع المعلومات حول العقوبات الاقتصادية ومكافحة انتشار الأسلحة النووية.[4] عادةً ما يكون الناشطون مموَّلين بشكل جيد وعلى قدر عال من المهارة

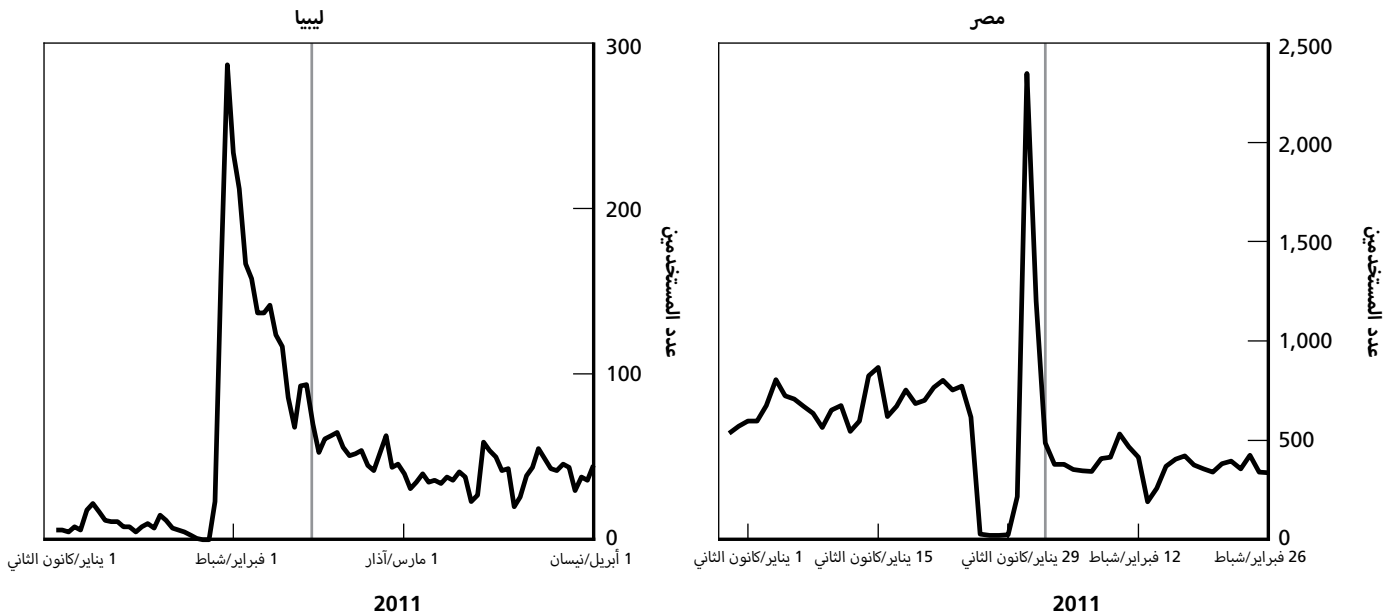
---

[2] "Timeline: الثورة المصرية," شبكة الجزيرة, 14 فبراير/شباط 2011.

[3] "Libyan Uprising One-Year Anniversary: Timeline," *The Telegraph*, February 17, 2012.

[4] Siobhan Gorman, "Iran-Based Cyberspies Targeting U.S. Officials, Report Alleges," *Wall Street Journal*, May 29, 2014.

الشكل1.2
الاستخدام المقدّر لمتصفحTor في مصر وليبيا، 2011



المصدر: مشروعTor، "المقاييس" بتاريخ 30 يونيو/حزيران 2014

ملحوظة: يعبر الخط الرأسي في الشكل عن25 يناير/كانون الثاني في مصر. في القسم الخاص بليبيا، فيعبر ذلك الخط عن 16 فبراير.

والخبرة في استخدامهم لتقنيات وأدوات وأساليب الرقابة والتجسس، بالإضافة إلى قدرتهم الفائقة على إخفاء أنشطتهم.[5]

كما يستخدم الإرهابيون تلك الأدوات لأنهم على استعداد للتضحية بالأداء (سرعة الاتصال) للحصول على فرصة تواصل أكثر سرّية وأمانًا. وقد أصبحت المجموعات الإرهابية، خلال العقد المنصرم، أكثر حنكة ودهاءً في استخدام تقنيات التشفير. وبينما لم يقم مخططو ومنفذو هجمات 11 سبتمبر/أيلول 2001 بتشفير اتصالاتهم،[6] نجد أن أعضاء تنظيم القاعدة الحاليين قد نجحوا في بناء أدوات حماية الخصوصية الخاصة وذلك لعدم ثقتهم في الأدوات التي تطورها الشركات الغربية.[7]

كما يلجأ مروجو الأفلام الإباحية للأطفال إلى استخدام أنواع كثيرة ومختلفة من البرمجيات لبث وعرض الصور غير المشروعة دون اكتشافهم. ونظرًا لكون حيازة مواد إباحية للأطفال هو فعل إجرامي، فإن لعنصري السرية والخصوصية في أدوات الاتصال المستخدمة في ترويجها أهمية بالغة. لا تهتم المواقع الإباحية التي تروج لإباحية الأطفال بالشهرة والانتشار عبر الإنترنت وذلك نظرًا لما تحققه من إيرادات مرتفعة. فبدلًا من استخدام العناوين على الشبكة أو أسماء المواقع، يتم استخدام كلمات البحث المفتاحية التي تعمل كرموز مشفرة شائعة في المجتمعات التي تستغل الأطفال جنسيًا.[8]

يلجأ أعضاء المنظمات الإجرامية لاستخدام العديد من الأساليب الرقمية المعقدة لإخفاء أنشطتهم حتى أنهم يستخدمون أساليب الاتصال التقليدية، بعيدًا عن التقنيات، كنقل المعلومات عن طريق أشخاص معينة في أماكن نائية.

قد يكون لدى سارقي المعلومات الشخصية من أجل تحقيق مكاسب مالية مجرد متطلبات بسيطة لإخفاء صفقاتهم، وذلك عبر استخدام خدمات رسائل فورية مشوشة، وشبكات خاصة افتراضية مشفرة، وحتى أدوات التواصل الاجتماعي المتاحة للعامة.

---

[5] على سبيل المثال، اطلع على أحدث الروايات المتعلقة بالصين وإيران وروسيا: Shane Harris, "حصري: تقرير من داخل مقر المباحث الفدرالية لمكافحة التجسس الإلكتروني من الصين" *Foreign Policy* بتاريخ 27 مايو/أيّار 2014.

[6] Emil Protalinski، "أسامة بن لادن لم يستخدم التشفير: نشر 17 وثيقة"، منشور على مدونة *ZDNet.com* بتاريخ 3 مايو/أيّار 2012.

[7] Recorded Future "كيف يستخدم تنظيم القاعدة التشفير بعد أحداث سنودن (الجزء الأول) صادر بتاريخ 8 مايو/أيّار 2014أ؛ Recorded Future، "كيف يستخدم تنظيم القاعدة التشفير بعد أحداث سنودون (الجزء الثاني) - تحليل جديد بالتعاون مع ReversingLabs" صادر بتاريخ 1 أغسطس/آب 2014 ب.

[8] Patrick Forde and Andrew Patterson, "أنشطة استغلال الأطفال جنسيًا عبر الإنترنت," *Australian Institute of Criminology:* التوجهات والقضايا المتعلقة بالجريمة وتطبيق العدالة على المجرمين, الإصدار 97، نوفمبر/تشرين الثاني 1998.

أدوات حرية استخدام الإنترنت هي تدابير وقائية لمكافحة القمع

منذ سنوات مضت، كان من المأمول أن يتحول الإنترنت إلى تكنولوجيا اتصال تتيح لمستخدميها في جميع أنحاء العالم إمكانية الوصول إلى المعلومات التي لم تكن متاحة من قبل سوى لدى وسائط الجهة الواحدة التي تخاطب جهات متعددة (على النقيض من وسائط التواصل الاجتماعي، والتي تتميز بأسلوب التواصل من فرد إلى آخر). قد تخضع هذه الوسائط لسيطرة هيئات تابعة للدولة (مثل: التلفزيون) أو تخضع للإدارة المادية (مثل: التهديد بمصادرة المواد المطبوعة). ووفقًا لما قاله أوائل المتحمسين للإنترنت، بأن الفضاء الإلكتروني سيكون نطاقًا خاليًا من أي تدخل للحكومة، حيث أن أي قيود أو تدخلات منها ستكون بمثابة تضليل لدور الإنترنت الروتيني الموجه. ثم بدأ عصر من الحريات والتفاهم العالمي بالظهور.

على الرغم من عدم تحرك الحكومات القمعية في العالم للاستجابة الفورية لما وفره الإنترنت من دفعة للحريات، إلا أنها استفاقت لذلك الآن وواجهته بطرق مختلفة:

- في بعض الحالات (مثل: كوبا، وكوريا الشمالية) تعمل الحكومات على تقييد الدخول إلى مواقع إلكترونية معينة، إما على الإطلاق أو في ظروف خاصة، وذلك بفرض رسوم وتكاليف أو فرض حظر على الجميع (تقريبًا). بينما تعمل دول أخرى على تقييد الدخول إلى مواقع إلكترونية محددة في أوقات معينة (كما حدث في مصر إبان ثورة الربيع العربي) أو أماكن معينة (حيث يجتمع الناس لممارسة حرياتهم في التجمع). عملت كل من الأردن وروسيا مؤخرًا على زيادة جهودهما في تقييد الوصول إلى الإنترنت.[1]

[1] Sanja Kelly, Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz and Ashley Greco-Stoner, eds., *الحرية على الإنترنت 2013: تقييم شامل للإنترنت والوسائط الرقمية*، Freedom House، بتاريخ 3 أكتوبر/تشرين الأول 2013.

- أنشأت بعض الدول الأكثر تطورًا (مثل: الصين، وإيران) وحدات انتقائية في مواقع محددة (مثل: أخبار Google) وغيرها من المحتويات المتوفرة على الإنترنت (مثل: أي ذكر لموقع "Tiananmen Square"). كما تعمل تلك الدول على استخدام مواقع شهيرة وحظر وصول أي شخص إليها مستخدمة هجمات حظر الخدمة الموزعة (DDoS).
- بينما تخترق بعض الحكومات الأخرى (مثل: روسيا البيضاء، فيتنام، البحرين) خدمات وتكنولوجيا الإنترنت للتعرف على المتمردين والخصوم السياسيين، إما بطريقة مباشرة (كتتبع نشاط Facebook بالصداقة) أو بالتخفي (عن طريق مهاجمة وإصابة حواسب المتمردين ببرمجيات تجسس ضارة).[2]
- تُجرم الكثير من الحكومات (مثل: تركيا، بنجلادش، أذربيجان) التعبير عن التمرد والانشقاق، وتستخدم الإنترنت كاداة مراقبة.[3]

إن التدابير المضادة لتلك التي تفرضها تلك الحكومات تعتبر اللبنة الأولى والأساسية في برنامج ضمان حرية استخدام الإنترنت: فهي التدابير الوقائية التي من شأنها تحسين توفير خدمة الإنترنت (في جميع الأماكن وجميع الأوقات)، والتحايل على الرقابة، ومكافحة DDoS، وتحسين مستويات حماية الحواسب الشخصية، و/أو زيادة سرية الاتصالات.

وتعتبر كل واحدة من التدابير الوقائية هذه بمثابة استجابة لما تفرضه الحكومات من قيود ضد الراغبين في ممارسة حقوقهم الإنسانية. ومن المؤكد أنه إن لم يتم فرض التدابير القمعية هذه منذ البداية، لما كانت هناك حاجة لوضع خطة ضمان حرية استخدام الإنترنت.[4]

ولم يكن الهدف من غالبية تلك التدابير القمعية التي فرضتها الحكومات أن تقضي على الأنشطة (التي تعتبرها الولايات المتحدة) غير شرعية. قد يتصور البعض أن الحكومات لا تفرض قيودًا على الاستخدامات اليومية للإنترنت بهدف القضاء على الجرائم على سبيل المثال. وبالمثل، وعلى الرغم من قيام الحكومة بحجب بعض المواقع التي تدعم ما يمكن اعتباره أنشطة إجرامية (لا بشكل غير معقول تمامًا) مثل

---

[2] Kelly et al., 2013.

[3] Kelly et al., 2013.

[4] تعمل بعض تقنيات حماية حرية استخدام الإنترنت على حماية حقوق بعض الأقليات (مثل مجتمع المثليين والمتحولين جنسيًا)، مرتكنة على أسباب منطقية تستدعي حجب الهوية - حتى في ظل غياب أي تدابير تفرضها الحكومة ضدهم (مثل أي قانون يجرم ممارسات جنسية بعينها).

(المواد الإباحية للبالغين)، إلا أن المواقع التي تدعم ما تعتبره الولايات المتحدة أنشطة إجرامية لا تحتل بؤرة تركيز ما تفرضه تلك الحكومات من رقابة. وبالمثل، لا يعتبر DDoS المنهج الأكثر انتشارًا والذي تتبعه الحكومات لمكافحة الأنشطة الإجرامية. كما هو الحال مع استخدام الحكومات القمعية لبرمجيات التجسس لاكتشاف الأنشطة الإجرامية في الدول الغربية، فعندما يحدث هذا، فإنه لا يحدث بصفة منتظمة. ويعتبر اعتراض الاتصالات لجمع الأدلة الجنائية هو الوسيلة الوحيدة المتاحة للحكومات، والذي يمكنه أن يشكل تهديدًا كبيرًا لكل من المجرمين ونشطاء حقوق الإنسان على حد السواء.

وينبغي مراعاة ذلك عند التمييز بين استخدام أدوات مكتب الديمقراطية وحقوق الإنسان والعمل لتحسين مستوى حرية استخدام الإنترنت وبين تخريب تلك الأدوات لدعم الأنشطة غير الشرعية. أي أنه من بين التدابير الوقائية الخمسة التي توفرها أدوات مكتب الديمقراطية وحقوق الإنسان والعمل (والتي يعتبر بعضها وسيلة توجيه أكثر من كونها وسيلة وقاية) فإن الأماكن التي يزداد احتمال ارتكاب الجرائم فيها هي بين تلك الأدوات التي تحجب هوية مستخدميها، والمعلومات المنقولة بينهم.

كيف يمكن أن يؤثر تمويل مكتب الديمقراطية وحقوق الإنسان والعمل على سلوكيات المجرمين ومستخدمي الإنترنت؟

ننتقل الآن إلى استعراض الإطار النظري المعني بدراسة الفروق بين نوعين من مستخدمي أدوات حرية استخدام الإنترنت، وهما: مستخدمو الإنترنت والمجرمون. فكلتا المجموعتين تسعيان للتواصل الآمن ولحماية هوياتهما وتجنب الوقوع تحت وطأة أي عواقب وخيمة.

وكثير من أدوات حرية استخدام الإنترنت توفر باقة مختلفة من الإمكانيات مثل المراوغة والتشفير والتستر. فضلًا عن ذلك، يتوفر بعض تلك الأدوات مجانًا، بينما يتوفر البعض الآخر بمقابل مادي؛ ويكون بعض تلك الأدوات ذات مصدر مفتوح والبعض الآخر ليس كذلك؛ ويتوفر بعضها بشكل قانوني، بينما لا يمكن الحصول على البعض الآخر إلا عبر قنوات غير شرعية. ونظرًا لكون مكتب الديمقراطية وحقوق الإنسان والعمل ليس هو المورد الوحيد[1] لأدوات حرية استخدام الإنترنت، فيمكننا تقسيم تلك الأدوات إلى ما يموله وما لا يموله مكتب الديمقراطية وحقوق الإنسان والعمل. ونفترض أيضًا أن كلًا من مستخدمي الإنترنت والمجرمين يستغلون منافع خليط مجموعتي الأدوات تلك.[2]

بيد أن كل مجموعة تواجه العديد من العقبات في سبيل استخدامهم لتلك الأدوات بحرية ودونما قيد. فبالنسبة لمستخدمي الإنترنت، فعادة ما يكون وصولهم واختياراتهم لتلك الأدوات محدودًا، إما بسبب تكلفتها أو افتقارهم للتدريب والتعليم، أو حتى لتوفر تلك الأدوات. أما بالنسبة للمجرمين، فيواجهون سبل الحماية ومزايا التصميم التي تحول دون استخدام الأدوات التي يمولها مكتب الديمقراطية وحقوق

[1] إننا نستخدم مصطلح المورد للتعبير الشائع عن منتج إحدى السلع المُعتادة. لذا لا يعتبر مكتب الديمقراطية وحقوق الإنسان والعمل هو القائم بعملية "التوريد" الفعلية، بل يعمل على تمويل أنشطة تطويرها.

[2] ليس هناك تركيبة معينة من الخدمات والأدوات يمكن اعتبارها محور رئيسي لهذه الدراسة، بل إن لكل نوع من المستخدمين أفضليات محددة ويحقق منها منفعة خاصة باستخدامه الأدوات هذه.

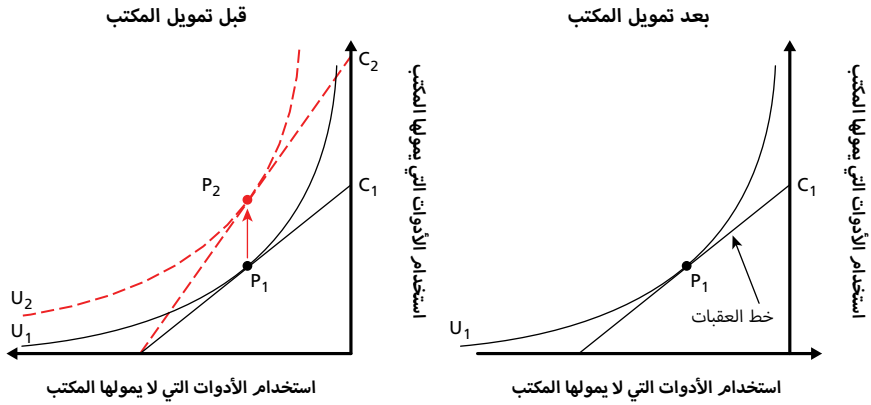
الإنسان والعمل في الأغراض غير المشروعة. فعلى سبيل المثال، وفي الكثير من الحالات، لا يتم توزيع أو توفير الخدمة أو التقنية إلا لمن يعرفهم المشاركون في البرنامج بصفة شخصية.

نبدأ أولًا بدراسة عمليات المقايضة التي تجريها كل مجموعة من الأفراد عند اختيارهم من بين الأدوات التي يمولها والتي لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل، ثم نقيّم تأثير تمويل المكتب على اختيارات كل مجموعة على حدة.

يوضح الشكل 4.1 التغير في الأدوات التي جرّبها مستخدمو الإنترنت قبل (القسم الأيمن) وبعد (القسم الأيسر) تمويل مكتب الديمقراطية وحقوق الإنسان والعمل. تعبّر المحاور الأفقية X عن مستوى استخدام الأدوات التي لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل، بينما تمثل المحاور الرأسية Y مستوى استخدام الأدوات التي يمولها المكتب.[3]

وسنبدأ بدراسة القسم الأيمن من الشكل 4.1. يعبر المنحنى (U_1) عن الحد الأقصى للمنفعة (الانتفاع) التي يحققها مستخدمو الإنترنت عند اختيارهم لاستخدام مزيج من الأدوات التي يمولها مكتب الديمقراطية وحقوق الإنسان (المحور الأفقي X) والأدوات التي (سيمولها) المكتب (على المحور الرأسي Y).[4] كلما ابتعد الجانب الخارجي عن نقطة

الشكل 4.1
أثر تمويل مكتب الديمقراطية وحقوق الإنسان والعمل على مستخدمي الإنترنت



RAND *RR1151-4.1*

[3] ولنفترض ضمنيًا أنه تم توفر الأدوات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل عن طريق آخر غير تمويل المكتب لها.

[4] وللتعبير عن ذلك رسميًا، نستخدم منحنى السواء هذا لتمثيل استهلاك نوعين من السلع العادية.

الأصل بزاوية 45 درجة، ازدادت المنفعة المتحققة. ولكن يخضع الحد الأقصى لانتفاع مستخدمي الإنترنت لتحديات عملية يواجهونها في سبيل الحصول على أدوات حماية حرية استخدام الإنترنت وشرائها واستخدامها. ويعبر الخط المستقيم C_1 عن تلك العقبات (ويعرف باسم: خط العقبات). ويعبر المماس لتلك المنحنيات (عند النقطة P_1) عن الحد الأقصى المحتمل للمنفعة، بالإضافة إلى القيم النسبية للأدوات المستخدمة.

بينما نستعرض في القسم الأيسر من الشكل، الآثار الرئيسة لتمويل مكتب الديمقراطية وحقوق الإنسان والعمل على مستخدمي الإنترنت. إن تمويل أدوات حرية استخدام الإنترنت يتيح فرصة أفضل للوصول إلى التكنولوجيا والخدمات، ويمكن تلك الفئة من الدخول إلى مصادر المعلومات والتواصل بحرية فيما بينهم، بطريقة تضمن الحماية الشخصية والسلامة الرقمية، وذلك من بين العديد من المزايا والمنافع الأخرى. ويسهم التمويل المقدم من مكتب الديمقراطية وحقوق الإنسان والعمل في تخفيف وطأة تلك القيود على فئة مستخدمي الإنترنت (وهو ما يكافئ تخفيض سعر استخدام الأدوات تلك)، مما يدفعها لاستهلاك عدد أكبر من الأدوات التي يمولها المكتب وتحقيق إجمالي منفعة نهائي أكبر. ففي نموذجنا المطروح، ساهم تمويل مكتب الديمقراطية وحقوق الإنسان والعمل في زيادة القدرة على الوصول إلى الأدوات التي يمولها، ومن ثم انتقل خط العقبات C_1 إلى الخط C_2، كما هو واضح في الشكل.[5] ولقد مكنها هذا التحسن في المصادر المتاحة من الاستمتاع بارتفاع المنفعة (الانتقال من النقطة P_1 إلى النقطة P_2) كما هو واضح بالانتقال من المنحنى U_1 إلى المنحنى U_2.[6]

ثم انتقلنا بعد ذلك إلى دراسة آثار تمويل مكتب الديمقراطية وحقوق الإنسان والعمل على اهتمامات المجرمين، كما هو موضح في الشكل 4.2.

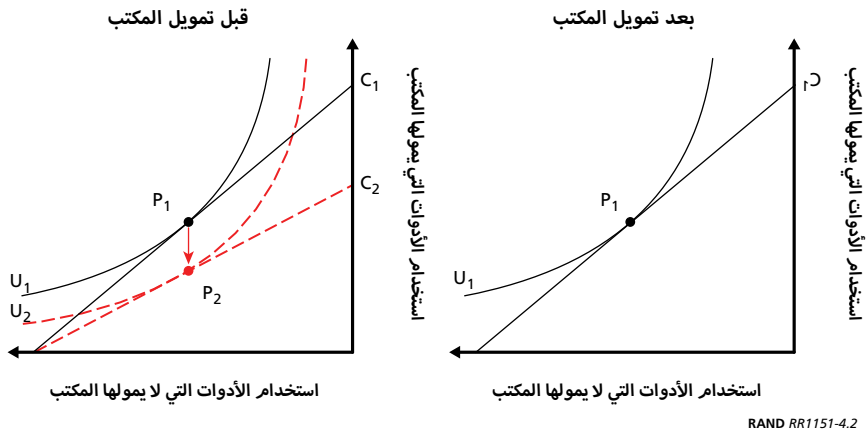
وكما هو الحال في الشكل رقم 4.1، يعبر القسم الأيمن من الشكل 4.2 عن المنفعة النظرية التي يحققها المجرم قبل تمويل مكتب الديمقراطية وحقوق الإنسان والعمل. حيث يعبر المنحنى U_1، عن التشابه بين الأدوات عندما يستخدمها المجرم كبدائل ممتزجة للاستمتاع بحرية استخدام الإنترنت (والتي يستغلها، في هذه الظروف، لارتكاب الجرائم). ويواجه المجرمون، شأنهم شأن جميع المستخدمين، العديد من

---

[5] ونفترض أن الأدوات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل ليس لها أي تأثير على خصائص ومميزات الأدوات التي لا يمولها المكتب.

[6] لاحظ أن تمويل مكتب الديمقراطية وحقوق الإنسان والعمل يؤدي، وبالمعنى الدقيق للكلمة، إلى انخفاض تكلفة تبني استخدام الأدوات التي يمولها المكتب مقارنة بالأدوات الأخرى التي لا يمولها. ولهذا التغير العديد من الآثار على منحنى العقبات، والتي قد تكون إما بتغير محوره أو نقله. وهذا ما نعبر عنه في الحقيقة بآثار الدخل و الاستبدال؛ وعلى أي حال، فقد قمنا بتبسيط التحليل، لغرض إتمام هذا البحث، لتوضيح كيفية تغيير وضع منحنى العقبات بكل بساطة.

الشكل 4.2
أثر تمويل مكتب الديمقراطية وحقوق الإنسان والعمل على الجهات الإجرامية



RAND *RR1151-4.2*

العقبات سواء من خلال الوقت أو الميزانية أو إمكانية الحصول على واستخدام تلك التكنولوجيا والخدمات (ويمثلها خط العقبات المستقيم، C_1). ولهذا، فهو يحقق أقصى منفعة عند نقطة التماس بين هذين المنحنيين، كما هو موضح بالنقطة P_1.

يوضح القسم الأيسر معدلات التغير في استخدام الأدوات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل، وما يترتب عليها من انخفاض في إجمالي المنفعة. في البداية، عندما يحتمل أن يوفر تمويل الأدوات الممثل بالمحور الرأسي Y منفعة مبدئية للمجرم (كما تفعل تمامًا مع مستخدمي الإنترنت)، فإن تواجد سبل الحماية ومزايا التصميم يعمل على تقييد وحظر استخدام تلك الأدوات والخدمات المستخدمة من قبل المجرمين. ويترتب على ذلك حدوث تغير في العقبات التي يواجهها المجرمون بانتقال الخط C_1 إلى الخط C_2. ومع توفر العقبات الجديدة، تنخفض المنفعة الإجمالية التي يحققها المجرمون من النقطة P_1 إلى النقطة P_2 نتيجة لتطبيق للتدابير الوقائية تلك.

توضح هذه الأشكال كيف يمكن لتمويل أدوات حرية استخدام الانترنت (المزودة بالتدابير الوقائية المناسبة) أن ينجح في تحسين منافع مستخدمي الإنترنت دون ارتباط ذلك بزيادة، أو ربما إنقاص، ما يحققه المجرمون من منافع. علاوة على ذلك، يمكن للمرء القول بأن توفر العديد من أدوات الحماية وحفظ الخصوصية سيضعف من إقبال المجرمين على استخدام الأدوات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل، وذلك لضعف مزايا استخدام تلك الأدوات كما هو الحال مع الأدوات الأخرى.

هل يسعى المجرمون ومستخدمو الإنترنت إلى الحصول على الأمور ذاتها من أدوات حرية استخدام الإنترنت؟

تبدأ الخطوة التالية في طريق فهم استخدامات وسبل إساءة استخدام أدوات حرية الإنترنت من التعرف على الاختلافات بين احتياجات كل من مستخدمي الإنترنت والمجرمين. لذا سنتناول في هذا الفصل دراسة الاختلافات المحتملة في تفضيل أعضاء كلا المجموعتين للمزايا التكنولوجية التي تتمتع بها أدوات حرية الإنترنت. ولفعل ذلك، علينا البدء بدراسة استبيانات المدونين.

تحول مستخدمو الإنترنت إلى أدوات حرية الإنترنت، في الغالب، بهدف الوصول إلى المواقع المحجوبة، مثل Facebook و Twitter، أو بهدف نشر محتويات سياسية حساسة لمجموعة كبيرة من المتلقين.[1] عندما وجه سؤال للمدونين من مختلف أنحاء العالم بخصوص الأهمية النسبية للخصوصية مقابل مزايا المراوغة والتخفي في الأداة، فقد كانت نسبة من يلجؤون إلى استخدام أدوات حرية الإنترنت بغرض المراوغة (54 بالمائة) أكبر ممن يلجؤون لاستخدامها لأغراض حماية الخصوصية (45 بالمائة).[2] ففي نهاية المطاف، يتخلى المدونون عن شهرتهم نظير الحصول على حماية لهوياتهم. ونظرًا لأنه في أغلب الحالات لا يُعتد بالمنشورات والتغريدات إلا عندما يكون جمهور المتلقين على علم وثقة بمصدرها، فإن احتمالية أن تلاقي المنشورات مجهولة المصدر صدى كبيرًا عند الجمهور العريض تكون منخفضة للغاية، ما لم يتم إعادة نشر تلك المنشورات عبر وسائط ومنافذ ذائعة الصيت.

ونظرًا لتوفر العديد من الأدوات التي تمكن من الوصول إلى المحتويات والمواقع المحجوبة مع حماية الخصوصية في الوقت نفسه، فإنه من الضروري التعرف على كيفية

[1] Robert Faris, John Palfrey, Ethan Zuckerman, Hal Roberts, and Jillian York, *International Bloggers and Internet Control: Full Survey Results*, Cambridge, Mass.: Harvard University Berkman Center for Internet and Society, August 18, 2011.

[2] Faris et al., 2011.

اختيار مستخدمي الإنترنت ما يستخدمونه من أدوات حماية حرية الإنترنت البديلة. ولقد قدمت الاستبيانات أدلة تفيد باحتمالية وجود تفاوت في التفضيلات مع اختلاف الدول وأنواع المستخدمين. فعلى سبيل المثال، اختلف تصنيف أهمية أدوات حماية حرية الإنترنت لدى المدونين الدوليين عن التصنيف الذي قدمه مستخدمو الإنترنت في الصين. حيث أفاد المدونون أن "الخصوصية" و "سهولة إيجاد الملفات وتحميلها" و"سهولة التثبيت" هي أهم ثلاثة عناصر.[3] بينما أفاد مستخدمو الإنترنت في الصين (الذين كانت غالبيتهم من الطلاب) أن "الموثوقية" و "سرعة الاتصال" و "سهولة التثبيت" هي العناصر الأكثر أهمية. كما اتضح أن مستخدمي الإنترنت في الصين ينجذبون إلى أدوات حرية الإنترنت المدمجة في المنصات التجارية - كأدوات Google و Amazon - وذلك لأن التكلفة الاقتصادية لحجب تلك المواقع باهظة للغاية، لذا أحجمت السلطات الصينية عن حجبها.[4]

وقد خلصت تلك الاستبيانات إلى التوصل إلى مجموعة متعددة من النتائج الهامة. نظرًا لأن غالبية المحتويات التي يسعى مستخدمو الإنترنت للحصول عليها تكون متاحة على النطاقات العامة (أي: المواقع الإلكترونية معلومة العناوين)، فلا يحتاج المستخدمون إلى تنسيق اختياراتهم لأدوات حرية الإنترنت سواء مع خوادم الموقع أو مع غيرهم من مستخدمي الإنترنت الذي يسعون أيضًا لتصفح تلك المواقع. كما يتواصل مستخدمو الإنترنت فيما بينهم عبر النطاقات العامة أيضًا مع استهداف مجموعة كبيرة من الجمهور المتلقي. ولقد لاحظ أحد النشطاء السعوديين أن خدمات Twitter قد مكنته من تحويل محادثات حول "المطبخ" أجراها مع مجموعة صغيرة من الأصدقاء إلى نقاش عام. على الرغم من رغبة الكثير من المشاركين في المحادثات العامة في حماية هوياتهم لتجنب الوقوع تحت طائلة العقوبات التي تفرضها السلطات، إلا أن مضمون نقاشهم يكون موجهًا إلى جمهور عريض من المتلقين.

كما ساهم التوفر السريع لأدوات حرية الإنترنت في التأثير على انتفاعهم باستخدام الإنترنت. فمع تطور الأحداث السياسية بسرعة كبيرة، فإن توقيت توفر المعلومات ومشاركتها يؤثر في فعاليتها وقدرتها على تغيير طبيعة الحراك والرأي العام. عندما يتمكن مستخدمو الإنترنت من إيصال قصصهم قبل أن يُعرض عليهم نشرها على وسائط الإعلام الخاضعة لإدارة الدولة، يتحولون إلى أطراف فاعلة تحدد

---

[3] Faris et al., 2011, p. 31.

[4] David Robinson, Harlan Yu, and Anne An, Collateral Freedom: A Snapshot of Chinese Internet Users Circumventing Censorship, OpenITP, April 2013, p. 11.

اتجاه الخطط. وهذا ما يدفع الأنظمة إلى ممارسة لعبة المتابعة، عن طريق عرض حساب بديل، ليحل محل حساب الحدث نفسه.[5]

وعلى النقيض، وفي معظم حالات الأنشطة غير الشرعية، تكون المعلومات التي تتم مشاركتها عبر الإنترنت مملوكة لصالح *club good*. يختلف المجرمون عن مستخدمي الإنترنت الراغبين في نشر المعلومات عبر النطاقات العامة، فإن المجرمين يسعون لتقييد القدرة على الوصول إلى المعلومات وحصرها بين مجموعة صغيرة من المشاركين في الشبكات الفرعية، وذلك لأنه في معظم الحالات يؤدي إلى زيادة الربح المادي من ملاحقة الأنشطة المحظورة. فعلى سبيل المثال، يستطيع مروجو المواد الإباحية للأطفال زيادة ما يحققونه من أرباح مادية عبر حظر الوصول إلى المحتويات غير الشرعية عن طريق منح حق الوصول إلى الأعضاء المستعدين لسداد مبلغ شهري (بعملة مجهولة) أو مشاركة مكتباتهم مع غيرهم من المستخدمين. كما قد يرغب تجار المخدرات في حظر الوصول إلى معلومات مواقع الشراء على مجموعة منتقاة بعناية من مستخدمي الإنترنت. ولهذا، يسعى مروجو الأنشطة غير المشروعة عبر الإنترنت إلى الوصول إلى مجموعة محدودة ومنتقاة بعناية من مستخدمي الإنترنت، بدلًا من السعي لزيادة عدد الجمهور المتلقي لرسالة معينة.[6]

علاوة على ذلك، يتحتم على مروجي المحتويات غير المشروعة عبر الإنترنت تغيير عنوان الإنترنت الخاص بمواقعهم بشكل مستمر، لتفادي اكتشافهم وملاحقتهم من قبل السلطات الحكومية، ولهذا لا يشكل بناء الشهرة أمرًا ذا أهمية بل ولا يمكن تحقيقه. ثم ينتقل بعد ذلك مروجو المحتويات غير الشرعية عبر الإنترنت إلى نقاط محورية (مثل: شبكة طريق الحرير) لزيادة احتمالية تحقق الصفقات. ويعتبر الوصول الفوري أمرًا أقل أهمية نظرًا لكون المحتوى لا يتأثر بالسياق السياسي.

وعلى النقيض من ذلك، أمن التواصل بين المجرمين يكون بجودة أضعف أمن حلقة بينهم. فإن فشل أحد أعضاء المجموعة في تشفير اتصالاته سيعرض أمن المجموعة كلها للخطر. وبالمثل، لكي تتحول إحدى شبكات الإنترنت إلى نقطة مركزية، ينبغي أن تكون مدعومة بأدوات حرية الإنترنت شائعة الاستخدام لزيادة عدد الأعضاء الجدد في المجموعة. تسهم هذه الخاصية الناجمة عن التكنولوجيا في خلق تأثير الجمود الذي يترتب عليه تحولات أحادية الجانب للانتقال من تكنولوجيا إلى أخرى غير معززة للفائدة.

---

[5] هذا مع افتراض تقديم مستخدمي الإنترنت بيانات حساب صحيحة، وهو ما قد لا ينطبق، سواء بقصد أو دونه، أو حتى نتيجة لما يتمتع به جميع المشاركين من خبرات موضوعية.

[6] وتعتبر حملات التجنيد الإرهابي عبر الإنترنت استثناء نادر الحدوث من هذا النمط.

بالنسبة لبعض الأنشطة المحظورة، قد يلزم الأمر توفر كمية كبيرة من مستخدمي التكنولوجيا للانتقال من استخدام إحدى أدوات حرية الإنترنت إلى أداة أخرى.

وبصفة عامة، فإننا نجد أن حساسية عنصر الزمن، وبناء الشهرة، والطبيعة العامة لحراك عامة مستخدمي الإنترنت هي السمات الأساسية المميزة لنشاطهم عبر الإنترنت. ومن ناحية أخرى، يعتبر نموذج النادي المغلق هو أفضل وصل لسلوك المجرمين عبر الإنترنت، وهو أقل اهتمامًا بالوقت، ويتعرض لتكاليف انتقال أعلى بكثير.

المنهجية

بعد دراسة الاختلاف بين احتياجات مستخدمي الإنترنت والمجرمين، ننتقل الآن إلى عرض المنهجية التالية، والتي صممت خصيصًا لتحقيق نتائج دفاعية يمكن تكرارها.

نبدأ بوصف مختصر لتكنولوجيا أو خدمة محددة (والمشار إليهما فيما يلي بلفظ "أداة" أو "مشروع").[1] ثم بعد ذلك، سنتناول الأغراض المستهدفة من هذا المشروع، كما أوضحها القائمون على تطبيقه. ثم نتناول بالتفاصيل مزاياه في دعم وتعزيز رسالة مكتب الديمقراطية وحقوق الإنسان والعمل لتحقيق حرية استخدام الإنترنت في جميع أنحاء العالم. ثم ننتقل بعد ذلك إلى دراسة النطاق الممكن لاستخدام تلك الأدوات في أغراض غير مشروعة.[2] ليس هدفنا هو إثبات أن هناك أداة بعينها لا يمكن مطلقًا استخدامها في أنشطة إجرامية، ولكن نهدف إلى فهم الإمكانيات المحتملة لاستخدام تلك الأدوات في أغراض إجرامية.

ولمناقشة تلك التحديات، تقدمنا بمقترح لمجموعة معايير الحد الأدنى التي يتحتم تلبيتها في أحد المشروعات ليمكن استخدامه في أغراض غير مشروعة: أولًا ، يجب أن يناقش مشكلة محددة لأحد ممارسي الأنشطة غير المشروعة؛ ثانيًا، يتحتم أن يوفر قدرات مادية أفضل من الأدوات التي سبقت وجود مكتب الديمقراطية وحقوق الإنسان والعمل، أو تم تطويرها بصفة مستقلة عن جهود المكتب؛ وثالثًا، يتحتم أن تتوفر للمجرمين بسعر معقول وأن تكون خالية من أي سبل وقائية مُحكمة. ولينخرط مكتب الديمقراطية وحقوق الإنسان والعمل في ممارسة دوره وتقديم إجابة شافية،

[1] لاحظ أنه نظرًا لقيامنا بفحص مجموعة من التقنيات والخدمات، فيحتمل وجود اختلافات فردية عبر كافة الأركان التي تشكل هذا التحليل. وفي الحالات التي تنطوي على اختلافات مادية في السلوك أو الإمكانات، فإننا نحدد الإمكانية، ولكن من دون تحديد برنامج تكنولوجي فريد من نوعه.

[2] كما تجدر ملاحظة أنه لكون التحدي الذي نواجهه هو دراسة كيفية دعم هذه المشاريع للأنشطة الإجرامية، فقد قمنا بتوصيف، وليس بتقييم ما توفره من منافع لمستخدمي الإنترنت.

فيتحتم أن تستوفي الأداة (أو المشروع أو الخدمة) المعايير الثلاثة تلك. ثم بعد ذلك ننتقل إلى دراسة كل واحد من تلك الشروط على حدة.

بالنسبة للمعيار الأول، وهو ضرورة معالجة التكنولوجيا أو الخدمة لإحدى مشكلات الاتصال الرقمي التي يواجهها المجرمون، نفترض أن توفير أحد المشروعات التي لا تقدم أي حل للمشكلة لن يلقى رواجًا أو اهتمامًا لدى المجرمين، لذا فإنه سيفشل في هذا الاختبار.[3] بعد التصنيف المبسط الذي أعده Gambetta (2011)،[4] نرى بأن المجرمين يواجهون ثلاث مشكلات شائعة. الأولى، يسعى المجرمون للتواصل في سرية تامة مع زملائهم المعروفين دون الخضوع للمراقبة، مثلما يخططون وينفذون إحدى الجرائم. وتعرف هذه المشكلة بمصطلح مشكلة الاتصال. ثانيًا، يسعى المجرمون إلى التواصل مع الغير، ممن لم يسبق لهم مقابلتهم، لتجنيد أعضاء جدد أو جمع التبرعات على سبيل المثال. وتعرف هذه المشكلة بمصطلح مشكلة التعريف. المشكلة الثالثة هي تحدي بيع سلع مسروقة أو تسويق خدمات غير قانونية. وتعرف هذه المشكلة بمصطلح مشكلة الدعاية. ولهذا، نقول تكون الأداة التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل أقرب للاستخدام في أنشطة غير مشروعة، عندما تقدم حلًا لواحدة على الأقل من مشكلات الاتصال أو التعريف أو الدعاية.

أما المعيار الثاني، والذي يشترط اجتياز الأداة التي يمولها مكتب الديمقراطية وحقوق الإنسان للاختبار الأول، فهو ضرورة توفير الأداة للمجرمين إمكانية أفضل من إمكانيات الأدوات الأخرى التي لا يمولها المكتب، أو التي قد تتوفر في غياب تمويل المكتب.[5] لذا قمنا أيضًا بدراسة ما إذا كانت الأدوات البديلة - التي لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل - صالحة للاستخدام في الغرض ذاته أم لا. فعلى سبيل المثال، قارنا تطبيقات البرمجيات التي تضمن حماية الخصوصية المطلقة إلى الأبد[6] مع دليل مختصر في حماية الرسائل الإلكترونية. تساعد قدرات الأول المجرمين في التملص من سلطات إنفاذ القانون (لذا فهو يجتاز هذا الاختبار)، بينما يمكن الحصول

---

[3] ومن هذا المنطلق، فإننا نقر بأنه ليس من العملي أو الضروري أن نهتم بدراسة كل صعوبة قد يواجهها كل نوع من المجرمين على حدة. بدلًا من ذلك، نعتقد بأن الحل العملي هو دراسة الأمور العامة التي قد يواجهها عموم المجرمين والجماعات الإجرامية أثناء ممارستهم لأنشطتهم.

[4] Diego Gambetta, Codes of the Underworld: How Criminals Communicate, Princeton, N.J.: Princeton University Press, 2011. في الحين الذي أشارت فيه دراسة Gambetta إلى أن نشر الرسائل وتبادل الأهداف بالإضافة إلى التواصل المباشر بين الأطراف، فإن هناك تطبيقات مفيدة يمكن استغلالها عند فحص وتقييم احتياجات التواصل لكل من المعنيين بحقوق الإنسان والمجرمين على حد السواء.

[5] وما افترضناه بخصوص القدرة المادية هي تلك التي تمنح تحسنًا أساسيًا أو استثنائيًا لم يكن ليتوفر من دونها.

[6] مُختارة لأغراض التوضيح فقط، نظرًا لأنه من الواضح أن هذه الملكية لا يمكن الحصول عليها بسهولة.

على الأخير من أي مكان آخر. كما اختبرنا أيضًا وجود أي أدلة على الاستخدام الفعلي في أنشطة غير مشروعة، عندما أمكن ذلك. وبناء على ذلك، ندفع بأن احتمالية استخدام الأدوات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل ترتفع عندما توفر للمجرمين قدرات مادية لا يمكنهم الحصول عليها دون توفر تمويل المكتب.

وأخيرًا، حتى ولو لم توفر الأداة حلًا لإحدى المشكلات، ولكنها تعتبر أفضل من الناحية المادية، فسيظل المجرمون قادرين على استخدامها، إما لتمتعهم فعليًا بالوصول إليها أو لندرة التدابير الوقائية التي تحول دون استخدامها. فعلى سبيل المثال، لن يستطيع المجرمون استخدام تلك الأدوات أو الخدمات التي لا يتم توفيرها إلا لمجموعة محددة من الأشخاص، لذا تفشل تلك الأدوات في هذا الاختبار. وبالمثل، توفر تلك الأدوات التي تحتوي على تدابير وقائية كافية أو غيرها من سمات التصميم التي تحول دون قدرة المجرمين على استخدامها قدرًا أقل من المنافع للمجرمين. ومن ناحية أخرى، تجتاز الأدوات المتاحة للعامة هذا الاختبار. وبناء عليه، ندفع بأنه تزداد احتمالية استخدام الأدوات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل في الأنشطة غير المشروعة في ظل غياب التدابير الوقائية التي قد تعتبر كافية لحظر المجرم عن استخدامها أو الحصول عليها.

تحليل مشاريع حرية الإنترنت لدى مكتب الديمقراطية وحقوق الإنسان والعمل

بينما خضع كل مشروع للفحص والدراسة بصفة مستقلة، إلا أن سياسة مكتب الديمقراطية وحقوق الإنسان والعمل تنص على عدم الإفصاح عن هوية المستفيد من المنحة دون الحصول على موافقة صريحة بذلك. علاوة على ذلك، طُلب من RAND تقييم تشكيلات من المشروعات، المصنفة وفقًا لما توفره من قدرات.[1] لهذا، قمنا بتقييم مشروعات مكتب الديمقراطية وحقوق الإنسان والعمل وتصنيفها إلى المجموعات التالية: الأمان الرقمي، anti-DDoS، الشبكات المتداخلة، الخوادم الوكيلة/الشبكات الافتراضية الخاصة، الاتصالات المحمولة المؤمنة، Tor، بالإضافة إلى مشروعين آخرين تم جمعهما سويًا تحت عنوان "أخرى". لاحظ أننا لم نقدم على تقديم أو تعريف تحليل شامل واستثنائي لمشروع Tor، وذلك بسبب ما يتمتع به من شهرة وقدرات متطورة.[2]

الأمان الرقمي

توجه مشروعات الأمان الرقمي إلى مجموعات البشر المعزولين والمهمشين والمستضعفين، أو لمن يعيشون في دول تفرض رقابة وحصار على وسائطها الإعلامية. حيث تعمل هذه البرامج على دعم حرية الإنترنت عن طريق تعليم وتوعية وتدريب مستخدمي الإنترنت لمخاطر الاتصال عبر الإنترنت، بالإضافة إلى توفير خدمات الترجمة (مثل: ترجمة اللغات) لأدوات المراوغة والاتصالات المؤمنة الموجودة مسبقًا.

[1] بينما تتواجد بعض الاختلافات بين الأدوات والخدمات في تلك المجموعات والتي ستتلاشى حتمًا في خضم التوصيف العام، إلا أنها لن تسفر عن تفاوت في استنتاجنا النهائي للتصنيف.

[2] ولقد حصلنا على موافقة من مشروع Tor لدراسته في هذا المشروع بصفة مستقلة.

كما توفر أشكالًا أخرى من التدريب الشخصي لجملة الناشطين في مهن تُعرّض أصحابها للخطر كالصحافيين ونشطاء التكنولوجيا والعاملين في مجال حقوق الإنسان والمدونين، وتتضمن كلًا من النقاشات الفنية والتدريب العملي بما يتعلق بسلامتهم الشخصية. وقد يتم إيصال المواد التدريبية أو التعليمية عبر عروض تقديمية، ونقاشات جماعية وتوجيه فردي وكذلك تدريب عملي. وتشمل الأمثلة تعليمات توجيهية ومهام صُممت خصيصًا لتعليم طريقة استخدام بعض أدوات الحماية والخصوصية، وعروض توضيحية لهجمات الشبكات اللاسلكية، ونصائح لتجنب الوقوع تحت الرقابة الشبكية، والحماية المناسبة للأجهزة المحمولة وأجهزة الحاسب الآلي المنزلية. ويتم تقديم التدريب نفسه في مراكز معينة،و عبر أي وسيلة متاحة للاتصال بالإنترنت.

بالإضافة إلى برامج التدريب تلك، تعمل مشروعات أخرى على تجميع الأخبار ومختلف صور المحتويات المحلية (أي المحتويات المحلية المتعلقة بمنطقة أو دولة بعينها) وتضمن توزيعها على من لا يستطيعون الوصول إليها بأي طريقة أخرى. علاوة على ذلك، ينصب تركيز العديد من المشروعات هذه على دول أو مناطق محددة تكون رازحة تحت ما تفرضه الدولة من قيود رقابية.

ونبدأ الآن في تطبيق الاختبار الثلاثي الأجزاء للاستخدام غير المشروع لأدوات الأمان الرقمي. ونظرًا لأن تركيز جهود التدريب يكون في أماكن صغيرة عادةً، أو بين شخصين، فيكون لها قدرة محدودة على تلبية احتياجات ما يواجهه المجرمون من مشكلات في الاتصال أو تعريف الهوية أو الدعاية. ولأن مشروعات التدريب تهتم في الأساس بمبادئ الخصوصية الفردية للمستخدم وبالاستخدام الآمن للإنترنت، فلن تستطيع أن تقدّم أي ميزة ملموسة للمجرمين. ثالثًا، تكون الجهات المستفيدة التي تدعم تلك المشروعات في علاقة تعاون وثيقة وحتى شخصية، مع منظمات محلية غير حكومية، بهدف بناء علاقات وثيقة والحفاظ على هذه العلاقات مع المواطنين والنشطاء المحليين في جميع أنحاء العالم. توفر استراتيجية التطبيق وسيلة حماية قوية ضد الاستخدام غير المشروع لأي من الدورات التدريبية أو التعليمية. كما تسعى الجهات المستفيدة لبناء علاقات وطيدة مع مجموعات محلية غير ربحية لضمان ممارسة أعمالها بطريقة سليمة في كل دولة.

ولهذا، خلصنا إلى أن مشروعات الأمان الرقمي تلك لا تصلح للاستخدام في الأنشطة غير المشروعة، عند مقارنتها بالحلول التي لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل، وذلك لأنها لم تستوفِ أيًا من شروط الاختبار ثلاثي الأقسام.

مضادات حجب الخدمة anti-DDOS

تساعد مشروعات anti-DDOS التي يدعمها مكتب الديمقراطية وحقوق الإنسان والعمل، كل من منظمات المجتمع المدني والمنظمات غير الربحية في الحفاظ على وجودها على الإنترنت من خلال ضمان مرونتها في مواجهة هجمات حجب الخدمة DDoS.[3] تعمل تلك الخدمات على حماية موقع العميل عن طريق استخدام القوائم السوداء على الإنترنت وأساليب الحماية الأساسية بالجدار الناري، والتي تقوم بترشيح البيانات الضارة والتخلص منها. بالإضافة إلى أنها تقوم بتوظيف عدد من الإمكانيات الفنية الأخرى، مثل موازنة التحميل وقراءة نظام أسماء النطاقات ذات العمر المحدود، وتخزين الوكيل المؤقت العكسي. يمكن الحصول على خدمات anti-DDoS هذه، عن طريق الاشتراك فيها نظير تكلفة منخفضة أو ربما مجانًا لصالح مجموعات غير ربحية قد تعتبر هدفًا للمعتدين والمستبدين بسبب نشاطها في مجال حقوق الإنسان.

ثم بعد ذلك، نطبق الاختبار الثلاثي الأجزاء لتقييم الاستخدام غير المشروع. بما يخص حل مشاكل المستخدمين الذين يلجؤون إلى طرق غير شرعية، تعتبر خدمات anti-DDoS بمثابة الحل الأمثل للتغلب على مشكلات الدعاية، وذلك لأنها تمكنهم من الوصول إلى المواقع المتاحة للعامة. ثم إن القدرات التي توفرها الخدمات هذه لا تختلف كثيرًا عمّا توفره الأدوات المتاحة تجاريًا، بل وتوفر، في بعض الحالات، مجموعة أكبر وأشمل من خدمات إدارة تدفق المعلومات والحماية من الهجمات الإلكترونية بتكلفة أعلى - ومنها على سبيل المثال: CloudFlare (www.cloudflare.com), Rackspace (www.rackspace.com), وAmazon Web Services (aws.amazon.com). ثالثًا، يتم تشغيل تلك الخدمات بواسطة مالكي المشروع أنفسهم، بدلًا من ترك تشغيلها من المستخدمين. وبناء عليه، يتحتم على المنظمات الامتثال والالتزام بمجموعة من المتطلبات الأخلاقية، للاستمتاع بالحماية ولضمان دعمهم لحقوق الإنسان ولحرية استخدام الإنترنت. ويعتبر هذا الانتقاء للعملاء المحتملين وسيلة قوية للحماية ضد الاستخدامات غير المشروعة لخدمات anti-DDoS.

لذا، لا تستوفي هذه الخدمات سوى القسم الأول من الاختبار (مشكلة الدعاية)، ولكنها تفشل في الاختبار الثاني (وذلك نظرًا لوجود خدمات بديلة متاحة بصورة أفضل للمستخدمين غير الشرعيين)، وكذلك في الاختبار الثالث (لأنه يتم إجراء تحريات شاملة للتحقق من امتثال المستفيدين من خدمات anti-DDoS لجهود ومواثيق حقوق

[3] هجمات DDoS هي الهجمات التي يسعى منفذوها لإعاقة أو حجب الوصول إلى خدمة عبر الإنترنت (كحجب أحد المواقع مثلًا) عن طريق التحميل الزائد على نظام الحاسوب من الأنشطة.

الإنسان). ونستنتج في النهاية أنه من المستبعد استخدام خدمات anti-DDoS الممولة من مكتب الديمقراطية وحقوق الإنسان والعمل في أنشطة غير مشروعة، مقارنة بالحلول الأخرى التي لا يمولها المكتب.

الشبكات المتداخلة

توفر تكنولوجيا الشبكات المتداخلة بنية تحتية للاتصالات تعمل بصفة مستقلة عن قنوات الاتصال المحمولة واللاسلكية، ولهذا تكون أكثر فائدة في المواقع التي لا تتوفر فيها إمكانية اتصال موثوقة وخاصة (مثل: الطلب المرتفع المؤقت) أو الخاضعة لرقابة شديدة، أو المفروض عليها قيود قمعية. صُممت الشبكات المتداخلة التي تستخدم الهواتف المحمولة لخدمة التجمعات المؤقتة والعشوائية من الناس، كما في حالة التظاهرات أو الأحداث التي تحرك المجتمع ككل. تعمل بعض الشبكات المتداخلة عن طريق إنشاء شبكة الند للند (P2P) بين الحواسب الشخصية أو الأجهزة المحمولة لأشخاص تفصل بينهم مئات المترات. حيث يصبح من الممكن، بعد تنظيم العدد الكافي من حلقات الربط وجمعها سويًا، تقديم خدمة الاتصال للشبكات العامة باستخدام جهاز واحد فقط. فعلى سبيل المثال، يستطيع الكثير من المستخدمين المقيمين في مجمع سكني واحد تمرير الرسائل فيما بينهم مستخدمين اتصال شخص واحد منهم فقط بالإنترنت. كما يمكن استخدام محطات أو هوائيات مركزية أكبر لتمديد النطاق الفعال للشبكات الخاصة هذه.

تعتبر الشبكات المتداخلة قيّمة في حالة التظاهرات، وعندما تعمل الحكومة القمعية على إيقاف خدمات الإنترنت العامة فجأة (كما هو واضح، على سبيل المثال، في الشكل 2.1). ففي هذه الحالات، يُنشئ المشاركون شبكة خاصة لغرض مشاركة المعلومات وتنسيق الأنشطة. كما أُضحت الشبكات المتداخلة وسيلة اتصال للبث المصاحب للبث الأصلي ذات أهمية بالغة في أوقات الكوارث الطبيعية، لتساعد في تنظيم وتوزيع الاحتياجات الإنسانية. ولقد كتب أحد الصحافيين في ذلك "توفر [الشبكات المتداخلة] وسائل تسمح للناس بتنظيم أنفسهم في جماعات، ومشاركة المصادر فيما بينهم: تُدار الشبكات المتداخلة بواسطة المجتمع ولخدمة المجتمع".[4]كما أنه "بفضل توفر الشبكات المتداخلة، يستطيع العامة تأسيس بنية تحتية شبكية متنامية لتشمل المجتمع: فهي شبكة محلية موزعة ومتداخلة، تخضع لإدارة مجموعة مختلفة من

[4] Primavera De Filippi، "آن الأوان للنظر إلى الشبكات المتداخلة بشكل جدي (وليس فقط للأسباب التي تعتقدها)" *Wired.com* 2 يناير/كانون الثاني 2014 (التوضيح في الأصل).

القيادات الشعبية بالمجتمعات. هدفها هو توفير نظام اتصال محكم ومتين مع تعزيز وضمان الوصول الديمقراطي لخدمات الإنترنت في نفس الوقت"[5]

ونبدأ الآن في تطبيق الاختبار الثلاثي الأجزاء لاستخدام الشبكات المتداخلة في أنشطة غير مشروعة. أولًا، نظرًا لكون الغرض الرئيسي من تصميم الشبكات المتداخلة هو توفير الدخول إلى الشبكة في مناطق لا تحتوي على بنية تحتية موثوقة للاتصالات (أو محجوبة أو خاضعة للرقابة)، فإنها، وبأعلى تقدير، توفر حلًا لمشكلة تواصل المجرمين الذين يسعون للاجتماع في مساحة جغرافية ضيقة للتخطيط أو لتنفيذ نشاط ما.[6] لذا لن تقدم هذه الخدمات حلًا مفيدًا لمشكلات الدعاية والإعلان، على سبيل المثال، نظرًا لأنها لا توفر دعمًا مباشرًا للإعلان عن الخدمات غير المشروعة، وخصوصًا فيما يتجاوز نطاق الشبكة المتداخلة (والذي لا يتجاوز بضعة مئات من الأمتار).

ثانيًا، لا تزال المشروعات التي تهتم بها حافظة استثمارات مكتب الديمقراطية وحقوق الإنسان والعمل في مراحل تطويرها المبكرة، لذلك فهي لا توفر إمكانات مادية جديدة للمجرمين غير موجودة في غيرها. ومن أمثلة الأدوات التي لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل أداة تُعرف باسم Edge Velosity،[7] وهي مؤسسة هادفة للربح تعمل على توفير حلول الشبكات المتداخلة لجهات الاستجابة مع الحالات الطارئة. كما تُعتبر كل من Athens Wireless Metropolitan Network, the Guifi network في إسبانيا و the Free Network Foundation في كانساس من الأمثلة الأخرى على أدوات الشبكات الشعرية التي لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل.[8] شهد تطبيق FireChat لهواتف iPhone ارتفاعًا ضخمًا في الإقبال على استخدامه في كل من العراق وهونج كونج.[9]

ثالثًا، وقع الاختيار على تقنيات الشبكات المتداخلة التي تمولها حافظة استثمارات مكتب الديمقراطية وحقوق الإنسان والعمل، نظرًا لأنها تتوفر كمصادر مفتوحة يمكن نشرها بحرية لتلبية متطلبات نشطاء حقوق الإنسان في جميع أنحاء العالم. بينما من

---

5 De Filippi, 2014.

6 من المؤكد أن الشبكات المتداخلة تساعد في حل مشاكل الاتصال وكشف الهوية بالنسبة للنشطاء الراغبين في التواصل في الفعاليات والتظاهرات، ولتحذير بعضهم بعضًا في حالة وجود أي خطر.

7 Edge Velocity Corporation, "About Us", صفحة إنترنت، مُحدثة.

8 Clive Thompson, "كيف تستطيع إبعاد وكالة الأمن القومي الأمريكية عن حاسوبك," *Mother Jones*, سبتمبر/أيلول-أكتوبر/تشرين الأول 2013.

9 Russell Brandom, "العراقيون يبحثون عن أدوات جديدة لفك حصار الإنترنت," *The Verge*, يونيو/حزيران 18, 2014; Steven Max Patterson, "الشبكات المتداخلة و FireChat: كيف يستطيع متظاهرو هونج كونج إبقاء الاتصالات بينهم حيّة", *NetworkWorld.com*, 2 أكتوبر/تشرين الأول 2014.

الممكن تصوّر استغلال الشبكات المتداخلة من قبل المجموعات الإجرامية (الإرهابيين أو الجريمة المنظمة)، إلا أن هذه المجموعات أكثر ميلًا إلى استخدام الشبكات اللاسلكية التقليدية وذلك لأن الشبكات المتداخلة أقل عملية في تشغيل شبكة اتصالات ثابتة ودائمة وواسعة النطاق. وعلى الرغم من استخدام اتصالات مشفرة بين الآلات في بعض الأحيان(مثل استخدام بروتوكول HTTPS)، إلا أن تدفق المعلومات عبر الشبكة يخضع في الغالب لرقابة المضيف. ويتسبب هذا في إحجام المستخدم عن الاتصال بالمستخدمين غير الموثوق بهم.

باختصار، استطاعت التقنيات هذه اجتياز الاختبار الأول بشكل جزئي(الاتصال)، وفشلت في اجتياز الاختبار الثاني (الميزة المادية لصالح المجرمين)، واجتازت الاختبار الثالث (التوفر العام). ونستنتج في النهاية أنه من المستبعد استخدام تقنيات الشبكات المتداخلة التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل في أنشطة غير مشروعة، مقارنة بحلول أخرى التي لا يمولها المكتب.

الوكيل / الشبكة الافتراضية الخاصة

تسهم تكنولوجيا كل من الوكيل والشبكة الافتراضية الخاصة في تفعيل قدرات التغلب على الرقابة والتهرب من الرصد، حيث تعمل كوسيط اتصال بين مستخدمي الإنترنت. وتضمن بعض الأدوات تحقيق ذلك عبر إرسال بيانات المستخدم الخاضع للرقابة إلى وكيل واحد أو إلى خادم مركزي يقع خارج نطاق النظام الذي فرض الرقابة، بينما تستغل بعض الأدوات الأخرى تقنيات أكثر تطورًا وتعقيدًا لإدارة وتوزيع القوائم التي تضم الخوادم الوكيلة والشبكات الافتراضية الخاصة التابعة لها.[10] وفي الطريقتين كلتيهما، يتم إخفاء موقع المستخدم الحقيقي عن طريق خدمات الوكيل أو الشبكة الافتراضية الخاصة. وعلى الرغم من وجود بعض التشابه بينها وبين تقنيات الشبكات المتداخلة، إلا أن أهم الفروق بينهما تكمن في أن حلول الشبكات الافتراضية الخاصية تستلزم توفر اتصال بالإنترنت لكي تعمل. تساعد الأدوات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل نشطاء حقوق الإنسان من خلال تمكينهم من الوصول إلى المحتويات المتوفرة على الإنترنت (مثل: المواقع والمعلومات) والتي تكون محجوبة أو خاضعة للرقابة.

[10] بينما يعتبر هذان بمثابة حلول "قفزة واحدة"، إلا أن الفرق بين الشبكات الافتراضية الخاصة والوكيل هو أن الشبكات الافتراضية الخاصة تحافظ على اتصال ثابت ومستمر بين المستخدم وصاحب الشبكة الافتراضية وتربط بين جميع الحواسب المتصلة عبر قنوات مشفرة. ومن الناحية الأخرى، فإن خدمات الوكيل تعمل في الغالب على تحويل تدفق بيانات المستخدم إلى الخادم الوكيل.

ونبدأ الآن في تطبيق الاختبار الثلاثي الأجزاء لاستخدام تلك الأدوات في الأنشطة غير المشروعة. أولًا، لن تقدم أدوات الوكيل والشبكات الافتراضية الخاصة التي تمولها محفظة مكتب الديمقراطية وحقوق الإنسان والعمل سوى حل جزئي لمشكلات الاتصال وتعريف الهوية والدعاية، لأنها وببساطة شبكات قائمة على الاتصال بالإنترنت، بدلًا من كونها منصات صالحة لبيع السلع غير الشرعية. فعلى سبيل المثال، لا تصلح هذه الأدوات، بالاعتماد عليها فقط، للاستخدام في حفظ أو الترويج لأي معلومات أو ملفات.

ثانيًا، في حين أن القدرة على إعادة توجيه رسائل مستخدم الإنترنت عبر قنوات مشفرة تمنح للمستخدم قدرًا كبيرة من الأمان والخصوصية، إلا أن الأدوات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل لا تقدم ميزة مادية ملموسة للمجرمين والتي تتجاوز ما هو متاح بالفعل في العديد من برامج وتطبيقات الوكيل والشبكات الافتراضية الخاصة.[11] فعلى سبيل المثال، هناك العديد من خدمات الشبكات الافتراضية الخاصة البديلة، لا يمولها مكتب الديمقراطية وحقوق الإنسان تعمل في دول أجنبية، ولا تخضع لقوانين الولايات المتحدة الأمريكية، لذا يفضل المجرمون استخدامها. ومن أمثلتها خدمتان روسيتان للشبكات الافتراضية الخاصة وهما cryptovpn.com و vpn-service.us.[12]

ثالثًا، تتوفر الأدوات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل مجانًا على الإنترنت، ويمكن للجميع تحميلها وتشغيلها وضبطها. بيد أن هناك العديد من سبل الوقاية التي تقيد قدرة المجرمين على استخدامها. فعلى سبيل المثال، وحتى لو عملت بعض الأدوات على تشفير الاتصالات بين المستخدم ومزوّد الشبكة الافتراضية الخاصة، تبقى اتصالات المستخدم عرضة للمراقبة من مشغلي هذه الخدمة. بالطبع، هذا ما يمنح المشغلين القدرة على حجب تدفقات مشكوك بأمرها، أو حتى حظر أنواع بعينها من الأنشطة غير المشروعة. حيث يقوم المشغل الواحد بالإشراف على ورصد حوالي 3% من التدفق لاكتشاف ما يعتبره محتوى غير لائق.[13] بالإضافة إلى أنه يتحتم على مزودي خدمات الوكالة والشبكات الافتراضية الخاصة الامتثال إلى طلبات المثول والتفتيش الصادرة عن جهات إنفاذ القانون، وهو ما قد يؤدي إلى كشف هويات المستخدمين أو المحتويات التي يتبادلونها.[14] علاوة على ذلك، قد تكون عناوين

---

[11] ولا يعتبر ذلك إقرارًا لأنها لا تقدم مزايا مادية ملموسة لنشطاء حقوق الإنسان.

[12] Max Goncharov, Russian Underground Revisited, Trend Micro, Cybercriminal Underground Economy Series, 2014.

[13] اعتمد هذا التقدير على مرشحات المشغّل للمحتويات غير المقبولة (والتي قد لا تكون بالضرورة غير قانونية).

[14] فعلى سبيل المثال، أقر أحد مزودي خدمات الشبكة الافتراضية الخاصة في المملكة المتحدة بامتثاله لطلب مقدم من مكتب التحقيقات الفيدرالية بالولايات المتحدة، للكشف عن هوية أحد المجرمين المزعومين. انظر "VPN HMA Hacker10.com, "FBI the to Over Handed IP After Arrested User, بتاريخ 28 سبتمبر/أيلول 2011.

بروتوكول الإنترنت IP الخاصة بخوادم الوكيل أو الشبكات الافتراضية الخاصة معلومة للعامة، لذلك تكون عرضة للرقابة. ذلك بالإضافة إلى تميز عدد من الأدوات الممولة تحت هذا التصنيف بقدرتها على تفادي الرقابة عبر تمرير الرسائل من خلال أحد الأصدقاء أو الزملاء المعروفين. بالنظر إلى أن عددًا قليلًا من المدافعين عن حقوق الإنسان لا يُسهّلون النشاط الإجرامي عن دراية، إلا أن ميزة التصميم هذه تشير إلى أن هذه الأدوات ستكون ذات منفعة عملية كبيرة لنشطاء حقوق الإنسان أكثر منها للمجرمين. وعلى الرغم من تدابير الوقاية هذه وغيرها المتاحة في خادم الوكيل وبرمجيات الشبكة الافتراضية الخاصة، إلا أنه لا يمكن استبعاد استخدامها في الأنشطة الإجرامية.

بإيجاز، استطاعت تقنيات الوكيل والشبكة الافتراضية الخاصة اجتياز الاختبار الأول (الاتصال) بشكل جزئي، وفشلت في اجتياز الاختبار الثاني (الميزة المادية لصالح المجرمين)، واجتازت الاختبار الثالث (التوفر العام). ونستنتج في النهاية أنه من المستبعد استخدام تقنيات الشبكات المتداخلة التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل في أنشطة غير مشروعة، مقارنة بالحلول البديلة (التي لا يمولها المكتب وغير المخصصة للاستخدام في الولايات المتحدة).

الاتصالات المحمولة الآمنة

تزوّد تقنيات الاتصالات الآمنة في الهواتف المحمولة الممولة بواسطة محفظة مكتب الديمقراطية وحقوق الإنسان والعمل تشفيرًا لكل من الرسائل والاتصالات المصورة والصوتية والنصية عبر الأجهزة المحمولة (iOS and Android). وتستخدم إما لتحل محل الخدمات غير المشفرة أو لزيادتها، مثل Skype و Google Talk و Jabber و Facebook. توفر بعض التقنيات أيضًا مخزنًا آمنًا للرسائل النصية والصوتية. بالإضافة إلى وجود تقنيات أخرى توفّر مراسلات آمنة تُستخدم بأنظمة PC و Mac و Linux. تقوم تقنيات أخرى ممولة من حافظة استثمارات مكتب الديمقراطية وحقوق الإنسان والعمل في الهواتف المحمولة بتسهيل التسامح مع تأخير الشبكات، وهو أمر ضروري عندما لا يمكن الاعتماد على خدمات الإنترنت الرئيسية أو عندما تظل غير متاحة لساعات أو لأيام. فعلى سبيل المثال، تخيل عندما يقوم الأفراد بتسجيل الفعاليات المحيطة بهم في مظاهرة، ولكن عليهم الانتظار لعدة أيام قبل أن يتمكنوا من إيصالها إلى الغير. وهنا يأتي دور تلك التطبيقات على الهواتف المحمولة والتي تساعد في ضمان نقل الرسائل الصوتية والنصية والإلكترونية والمصورة وبثها بطريقة موثوقة وآمنة.

لذا تعتبر تقنيات الهواتف المحمولة هذه ركنًا هامًا ورئيسيًا لنشاطات حقوق الإنسان. يستطيع النشطاء، بفضل استخدام ما تحويه تلك الأجهزة من ميكروفونات

وكاميرات، توثيق ونشر الممارسات المشينة التي يمارسها المسؤولون وضباط الجيش والشرطة الفاسدون، وعصابات ترويج المخدرات، وغيرهم من مرتكبي جرائم العنف. كما توفر تقنيات الهواتف المحمولة الآمنة وسائل للحفظ الآمن لهذه الصور والرسائل فور التقاطها، وبث الصور فور توفر الاتصال، وحتى تحذير الحلفاء حال وقوع خطب ما، وذلك أثناء حمايتها للمستخدم والجهاز من الانتقام.[15]

ونبدأ الآن في تطبيق الاختبار الثلاثي الأجزاء لاستخدام تلك الأدوات في الأنشطة غير المشروعة. أولًا، تستطيع هذه المشروعات إيجاد حل لمشكلات الاتصال التي يواجهها المجرمون. وفي الأساس، تعمل هذه التكنولوجيا على توفير سبل آمنة لتبادل الرسائل بين طرفين يعرف كل منهما الآخر (على عكس بث رسائل جماعية إلى مجموعة غير معلومة من الناس، أو تسويق خدمات غير مشروعة).

ثانيًا، بعد تقييم كل أداة بالتفصيل، خلصنا إلى أنها لا توفر أي مزايا مادية للمجرمين تتخطى ما يمكنهم الحصول عليها دون توفر تمويل مكتب الديمقراطية وحقوق الإنسان والعمل. هناك عدد كبير من التقنيات الأخرى، لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل، توفر قدرات مشابهة لتشفير الرسائل الصوتية والنصية على الأجهزة المحمولة. ومنها على سبيل المثال، شركة Silent Circle (وهي شركة ربحية) فهي تبيع هاتفًا فريدًا يعمل بأنظمة تشغيل مصممة لأغراض خاصة، بهدف توفير خدمات تشفير قوية للاتصالات الصوتية والمصورة والنصية وكذلك الاتصال بالشبكة.[16] توفر بعض التطبيقات على الهواتف المحمولة مثل Wikr[17] أيضًا خدمة الرسائل الآمنة، ومن المعروف أيضًا أن المنظمات الإجرامية تعمل في بعض الحالات على تطوير واستخدام تقنية المراسلة الفورية الخاصة بها.[18]

ثالثًا، تتوفر تلك الأدوات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل مجانًا دون تكلفة، ويتوفر الكثير منها إما كتطبيق للهاتف المحمول أو كشفرة المصدر. بيد أن هناك العديد من سبل الوقاية التي تحظر بعض الاستخدامات غير المشروعة. وعلى الرغم من السرية التي يوفرها تشفير الاتصالات النصية أو الصوتية، إلا أنه يمكن

---

15 Tanya O'Carroll, "تقنيات الهواتف المحمولة تساعد النشطاء والمدافعين عن حقوق الإنسان," *Ethical Consumer*, غير محددة التاريخ.

16 Blackphone, الصفحة الرئيسية, محدثة.

17 Wickr, "كيفية عمل Wickr," محدثة.

18 Jeremy Kirk, "طوّر القراصنة برامج محادثة فورية خاصة، لتبقيهم بعيدًا عن قبضة القانون," *ComputerWorld.com*, بتاريخ 28 مارس/آذار 2007.

استخدام البيانات الوصفية للكشف عن مصدر ووجهة الرسائل المرسلة من الأجهزة[19]، ولهذا تسهم في تيسير عمل جهات إنفاذ القانون وأنشطة التحقيق. علاوة على ذلك، تشكل الميكروفونات والكاميرات الموجودة بشكل واسع في تلك الأجهزة المحمولة تهديدًا شديدًا للمجرمين، إن أمكن تفعيلها عن بعد بواسطة سلطات تنفيذ القانوني لتسجيل وتوثيق الأنشطة الإجرامية.

بإيجاز، استطاعت تلك التقنيات اجتياز الاختبار الأول (الاتصال) بشكل جزئي، وفشلت في اجتياز الاختبار الثاني (لا توفر أي ميزة مادية لصالح المجرمين)، واجتازت الاختبار الثالث (التوفر العام). ونستنتج في النهاية أنه من المستبعد استغلال التقنيات التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل في أنشطة غير مشروعة، مقارنة بالحلول الأخرى التي لا يمولها المكتب.

Tor (التوجيه البصلي)

يوفر مكتب الديمقراطية وحقوق الإنسان والعمل تمويلًا مباشرًا وغير مباشر لعدد من المشروعات الفرعية المحددة والتي تعمل مجتمعة على تحسين تكنولوجيا Tor، والقدرة على استخدامه والتوثيق ودعم العملاء.[20] ويتميز تطبيق Tor بصفة إجمالية بقدرته على توفير السرية والأمان للاتصالات الجارية عبر الإنترنت عبر استخدام هندسة توزيع وبروتوكولات خاصة مفتوحة المصدر لتغليف وإخفاء نقل البيانات عبر الإنترنت. حيث تمر بيانات الشبكة للمستخدم عبر خوادم تبديل مستقلة (قد توجد في أي مكان بالعالم) ضمن شبكة Tor، مع إضافة طبقة من التشفير الجديدة لكل اتصال، بحيث لا يستطيع كل خادم تبديل تابع لشبكة Tor سوى مراقبة مصدر ووجهة نقل البيانات لخوادم Tor التي يتصل بها هو مباشرة. فعلى سبيل المثال، في الدائرة ثلاثية التوزيع، لا يستطيع الخادم الأوسط رصد عنوان بروتوكول الإنترنت للمستخدم الذي قام بالطلب الأساسي، ولا عنوان الوجهة النهائية للطلب. وبهذا يوفر هذا البروتوكول وسيلة دفاع قوية ضد تحليل نقل البيانات والرقابة وانتهاك الخصوصية. ويضمن هذا المشروع أن يظل المستخدم مجهولًا تمامًا ودائمًا، بشرط ألا يسرب المستخدم بنفسه أي معلومات شخصية عن نفسه، ولا يقتصر ذلك على جلسة واحدة فقط (أي أن الموقع لن يتمكن من التعرف على عنوان بروتوكول الإنترنت للمستخدم)، بل ويمتد أيضًا بين الجلسات المتعددة

[19] سواء عبر عنوان بروتوكول الإنترنت أو عبر الرقم الفريد لتعريف الجهاز.

[20] ولنكن واضحين، فإن مشروع Tor أيضًا يحصل على تمويل من أشخاص ومنظمات، بما فيها 4300 عملية تبرع شخصي، بالإضافة إلى الهيئات الحكومية الاتحادية والمؤسسات التجارية. انظر مشروع Tor: صفحة "رعاة Tor"، غير محدد بتاريخ.

(أي أنه لن يتمكن موقعان إلكترونيان من تحديد مستخدم بعينه في جلستين مختلفتين).[21] وقد ساهمت تلك الخصائص في جعل Tor مرغوبًا بشدة لدى كل من يبحث عن مستوى عالٍ من الخصوصية والاتصالات المشفرة بالإضافة إلى التخفّي المحكم (عدم القدرة على الربط) بين المستخدم والموقع المنشود.

تتيح الحماية الرقمية التي يقدّمها Tor العديد من المزايا لمستخدمي الإنترنت ولناشطي حقوق الإنسان على حد سواء. فعلى سبيل المثال، يستخدم الصحافيون Tor للتواصل مع المتمردين والمخبرين. كما يستخدم أعضاء من الأقليات وجماعة المحرومين Tor في التواصل فيما بينهم ومع من يعانون من التهديدات ذاتها أو يقعون تحت وطأة الجرائم نفسها. فلقد كتب أحد المعلقين قائلًا:

> على الرغم من أنني مقيم في دولة شمالية، إلا أنني استخدم Tor في كتابة المدونات على الإنترنت. فآرائي لا تلقى رواجًا بين زملائي، وقد يتسبب هذا في فقداني لوظيفتي بكل سهولة. فحرية التعبير غير مكفولة تمامًا حتى في الأنظمة الديمقراطية. وهو أمر علينا العمل يوميًا لتحقيقه. ولقد ساعدنا Tor في ضمان فرصة للإفصاح عن أفكارنا دونما خوف.[22]

وكتب معلق آخر قائلًا:

> بصفتي ناشط مدافع عن حقوق المتحولين جنسيًا، فلقد تواصل معي الكثير من المتحولين من جميع أنحاء العالم. ولسبب ما، أصبح اسمي معروفًا بين أوساط المتحولين جنسيًا في منطقة الشرق الأوسط وجنوب آسيا. ودائمًا ما كنت أنصح من أتواصل معهم باستخدام Tor لحماية أنفسهم.[23]

كما تلجأ سلطات تنفيذ القانون والوكالات الاستخباراتية إلى استخدام Tor لمطاردة واعتقال المجرمين ومكافحة تهديدات الأمن الوطني.[24] يحتاج ضباط الشرطة المتخفين إلى القدر الكافي من السرية والخصوصية والتي لا يمكن توفيرها إلا من خلال تقنيات مثل Tor. فعلى سبيل المثال، أشار ضابط شرطة أنه كان يستخدم Tor عند عمله على بعض القضايا ذات الصلة بجرائم الإنترنت ضد الأطفال. فكان يستخدم Tor

---

[21] وبالطبع تكون تلك المزايا مصحوبة بحجب القدرة على التتبع من طرف المستخدم عبر ملفات تعريف الارتباط Cookies أو غيرها من الآليات.

[22] تعليق مجهول المصدر على مدونة مشروع Tor (مشروع Tor، "شاركونا بقصصكم الجيدة مع Tor" بتاريخ 17 أغسطس/آب 2011).

[23] تعليق مجهول المصدر على مدونة مشروع Tor (مشروع Tor 2011).

[24] انظر مشروع Tor، "أسئلة مكررة حول إساءة الاستخدام"، صفحة إنترنت، غير مؤرخة.

للدخول إلى مواقع التواصل الاجتماعي لمساعدته في الحفاظ على هويته الخفية عند تواصله مع المشاركين في أنشطة استغلال الأطفال. وبالمثل، كان يستخدم Tor عندما يتواصل بالرسائل الفورية مع مروجي المخدرات. علاوة على ذلك، تستخدم سلطات تنفيذ القانون مزايا التخفي التي يوفرها Tor للتواصل مع المخبرين وغيرهم من مصادر المعلومات وجهات الاتصال الهامة والحساسة. بالإضافة إلى أن إخفاء موقع الحاسب الآلي أمر غاية في الأهمية عند التحقيق في مواقع إلكترونية لمجرم مشتبه به، سواء كانت داخل الولايات المتحدة الأمريكية أو خارجها.

ثم بعد ذلك، نطبق الاختبار الثلاثي الأجزاء لتقييم الاستخدام غير المشروع لمشروع Tor. وفيما يتعلق بحل المشكلة التي ذكرها Gambetta[25] فقد نجح Tor في حل مشكلة الاتصال بالنسبة للمشغلين والمستخدمين في كل من الشبكات الخفية، وطريق الحرير، عبر السماح لهم بإدارة التواصل عبر خادم شبكة يُيسر ممارسة الأنشطة غير القانونية.[26] ذلك بالإضافة إلى كون Tor غير مخصص لمواجهة تحديات التعرف على الأشخاص من ذوي الاهتمامات المشتركة، سواء كانت إجرامية أو غير ذلك. بيد أن ما يوفره Tor من حفظ للتخفي والسرية عبر بنيته التحتية للتواصل قد خلق منصة اتصال يشعر من خلالها كل من مستخدمي الإنترنت والمجرمين بالمزيد من الأمان لمناقشة الشؤون والقضايا التي ستشكل لهم الكثير من المشكلات إن تم الكشف عن هوياتهم. أما بخصوص مشكلة الدعاية، فإن Tor غير مصمم تحديدًا لحل تلك المشكلة ، ولكن ما يوفره من حماية للسرية أتاح فرصة ترويج سلع وخدمات يخشى المستخدمون أن تكون محظورة وقد تضعهم قيد التحقيق إذا تم الكشف عن هوياتهم. (سنناقش الخدمات المخفية في Tor لاحقا في هذا الفصل).

ثانيًا، في حين يوفر Tor العديد من مزايا السرية والخصوصية المتطورة، حتى عند مقارنتها بأدوات لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل، فإن هناك أيضًا عدد من التقنيات الأخرى التي توفر إمكانات مشابهة لما يوفره Tor وليست ممولة من قبل مكتب الديمقراطية وحقوق الإنسان والعمل. ومن الأمثلة على ذلك، ما اقترحه العديد من التوجهات الحديثة والتي تفيد باستخدام منصات التواصل الاجتماعية الشبكية الجديدة (مثل Instagram و Kik) بشكل كبير في ممارسة أنشطة مماثلة لما يمكن إنجازه عبر شبكة Tor، بل وتتميز بكونها أكثر جاذبية من Tor نظرًا لارتفاع عدد المشترين المحتملين في السوق السري (مثل: طريق الحرير). وعلى سبيل المثال، ساهم نشر صور أسلحة أو مخدرات عبر Instagram تحت اسم مستخدم مثل "ihavedrugs4sale"

---

[25] Gambetta, 2011.

[26] "The Amazons of the Dark Net," *The Economist*, November 1, 2014.

أو استخدام بعض الوسوم مثل "#ar15" في حل مشكلة التسويق للسلع وسرّع اكتشافها ممن لديهم اهتمام بها.[27]

ذلك بالإضافة إلى خدمة FreeNet (والتي توفر خدمة حفظ واسترداد ملفات مشفرة وموزعة) والتي صممت لحماية هوية المستخدم الذي يطلب المحتوى والموقع المادي للمحتوى، والتي تعتبر ملاذًا لحل مشكلة المجرمين من مستخدمي Tor عند رغبتهم في الإعلان عن السلع المسروقة.[28] وهناك أيضًا ما يعرف باسم I2P وهو شبيه Tor، إنه يوفر اتصالات شبكية مشفرة يمكن استخدامها في الوصول إلى خدمات الإنترنت العامة والخاصة دون الكشف عن الهوية.[29] وبعد عرض ما سبق، يتضح بأن السوق السوداء التي تستغل ما توفره شبكة Tor تنعم بازدهار كما أكدت التقارير.[30]

ونظرًا لأن Tor سبق في تواجده تدخل مكتب الديمقراطية وحقوق الإنسان والعمل بعقد من الزمان، يمكن القول بأن قدراته ومزاياه الجوهرية كانت متوفرة سواء مع دعم المكتب أو بدونه.[31] ومن المؤكد أن التكنولوجيا الأساسية التي يعمل بها Tor كانت في الأصل من تطوير ورعاية مختبر أبحاث البحرية الأمريكية في منتصف التسعينيات، فهو سابق لأي تمويل من قبل مكتب الديمقراطية وحقوق الإنسان والعمل. ذلك بالإضافة إلى كون مشروع Tor من مشروعات تطوير البرمجيات الضخمة وهو مؤلّف من عدة مكونات منفصلة ولكنها ذات صلة ببعضها البعض، والتي لم يساهم مكتب الديمقراطية وحقوق الإنسان والعمل إلا بتمويل بعضًا منها فقط. ومن المؤكد أن العناصر المحددة التي ساهم مكتب الديمقراطية وحقوق الإنسان والعمل بتمويلها كانت ذات صلة بتدويل وتعميم استخدام تطبيقات Tor، بدلًا من تمويل المكونات الرئيسية التي قد تساعد في ممارسة الأنشطة الإجرامية.

ثالثًا، يتميز برنامج Tor وخدماته بأنه متاح مجانًا على الإنترنت. بيد أن هناك العديد من سبل الوقاية التي تحظر بعض الاستخدامات غير المشروعة. فعلى سبيل المثال، يواجه المجرمون بعض التحديات بصفتهم مستخدمون لخدمات الوكيل/الشبكة الافتراضية الخاصة

---

[27] Fletcher Babb, "Lean on Me: Emoji Death Threats and Instagram's Codeine Kingpin," *Vice.com*, October 24, 2013.

[28] راجع https://freenetproject.org/.

[29] راجع https://geti2p.net/en/.

[30] "The Amazons of the Dark Net," 2014.

[31] وفقًا لما أقره مشروع Tor، والذي أفاد بأن تمويل مكتب الديمقراطية وحقوق الإنسان والعمل قد بدأ في 2013، بينما بدأ تطوير مشروع Tor في منتصف التسعينيات، وتم إصدار Tor لأول مرة في 2002. للمزيد من المعلومات حول تمويل Tor، أنظر صفحة مشروع Tor، غير مؤرخة. للمزيد من المعلومات عن الإصدار الأول، أنظر Roger Dingledine, "Pre-Alpha: شغل وكيل Onion الآن!" رسالة إلكترونية بتاريخ 20 سبتمبر/أيلول 2002.

- وهو احتمال معرفة عنوان بروتوكول الإنترنت لأحد نقاط التحويل في شبكة Tor، الأمر الذي يمكن الحكومات، وسلطات إنفاذ القانون، وحتى المواقع الربحية (مثل: Google) من تتبع وحجب الطلبات.[32] علاوة على ذلك، لا تزال هناك احتمالية لاكتشاف ما يمارسه المستخدمون من أنشطة إجرامية عبر شبكة Tor نتيجة للخطأ البشري والأساليب التي تتبعها سلطات إنفاذ القانون. ومثالًا على ذلك، نذكر أنه تم اعتقال طالب في جامعة هارفارد بعد إرساله رسالة إلكترونية للتهديد بوجود قنبلة، وعلى الرغم من استخدامه Tor إلا أن الشرطة تمكنت من القبض عليه سريعًا عن طريق إعداد قائمة محدودة بمن كانوا يستخدمون Tor داخل الجامعة وقت إرسال الرسالة الإلكترونية.[33] تمكن مكتب المباحث الفدرالية من السيطرة على سوق الإجرام الإلكتروني المعروف باسم طريق الحرير (وكذلك خليفته طريق الحرير الإصدار 2)، حتى مع تشغيله من خلال شبكة Tor، وهو ما تم تحقيقه بواسطة أساليب تقليدية لإنفاذ القانون.[34] وأخيرًا، توفرت أدلة أيضًا تفيد بأن أنظمة Tor شأنها شأن غيرها من جميع التطبيقات والبرمجيات، تعاني من هجمات وثغرات. حيث ورد في أحد التقارير الإخبارية تعرض أحد منافذ خدمات Tor قد تعرض لإصابة بملفات خبيثة تقوم بتعديل الملفات الأصلية لخدمات Tor عند تحميلها وتزرع بها برامج ضارة مع احتمالية التعرف على ما يمارسه المستخدمون من أنشطة (سواء كانت مشروعة أو غير مشروعة).[35] كما أن هناك مؤشرات أيضًا ذكرها الباحثون أنه يحتمل أن يتعرض مستخدمو Tor لمستويات متفاوتة من الاكتشاف، وذلك وفقًا لما يتوفر من معلومات ومصادر كافية للمعتدي.[36]

ولقد شارك قادة مشروع Tor في العديد من أنشطة الوقاية المصممة خصيصًا لتعزيز الاستخدام المناسب والشرعي لتكنولوجيتهم. فعلى سبيل المثال، تم بذل جهود مضنية

---

[32] تساعدك المزايا الجديدة نسبيًا في Tor Bridges على تفادي تلك المخاطر.

[33] Runa A. Sandvik, "حصل طالب في جامعة هارفارد على رمز F نتيجة لفضل Tor عندما أرسل تهديدًا مجهول المصدر بوجود قنبلة" *Forbes* بتاريخ 18 ديسمبر/كانون الأول 2013.

[34] Kim Zetter, "كيف استطاعت المباحث الفدرالية إسقاط أرض العجائب للمخدرات المعروفة بطريق الحرير." *Wired.com*, بتاريخ 18 نوفمبر/تشرين الثاني 2013. بخصوص الإصدار 2 من طريق الحرير، يمكنك الاطلاع على تحقيقات المباحث الفدرالية، المكتب الميداني في نيويورك "الحكم بالسجن على مشغل موقع طريق الحرير 2 أمام المحكمة الاتحادية في مانهاتن" تقرير صحفي، بتاريخ 6 نوفمبر/تشرين الثاني 2014.

[35] Darren Pauli, "تنشر إحدى نقاط الخروج من شبكة Tor البرامج الضارة في التنزيلات" *The Register*, بتاريخ 27 أكتوبر/تشرين الأول 2014.

[36] Sambuddho Chakravarty, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis, "On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records," in Michalis Faloutsos and Aleksander Kuzmanovic, eds., *Passive and Active Measurement: Proceedings of 15th International Conference, PAM 2014*, Los Angeles, Calif.: Springer, March 10–11, 2014.

لمناقشة مزايا استخدامه وتوطينه مما ساعد نشطاء حقوق الإنسان الذين يقيمون في أماكن نائية على تأمين الوصول لأدوات الخصوصية. علاوة على ذلك، فقد بذلوا الكثير من المجهودات في سبيل توفير استخدام البيانات ومستوى الأداء للعامة لأغراض الأبحاث والشفافية. فعلى سبيل المثال، كان من بين البيانات التي قدموها الأدلة التي أفادت الطفرة التي شهدها استخدام المشروع إبان اندلاع ثورات الشرق الأوسط. وكانت تلك البيانات أيضًا هي ما مكنت المشغلين من ملاحظة تغيير مفاجئ في الاستخدام، ويُعتقد أن يكون بفعل الهجمات الضارة (botnet).[37] وساهم توفر تلك البيانات وجهود حماية الخصوصية في رصد ومقاومة أي تدفقات ضارة للبيانات. وأخيرًا، فإن قادة مشروع Tor يمارسون دورًا نشطًا في مجالي الحماية والخصوصية ، بما في ذلك مجموعات حرية الإنترنت ليس في الولايات المتحدة وحدها بل في جميع أنحاء العالم. فقد كانوا واضحين في الترويج لمشروع Tor على أنه أداة لحماية الخصوصية والأمان، يمكن للصحافيين ومستخدمي الإنترنت وسلطات تنفيذ القانون والقوات المسلحة الأمريكية وغيرهم استخدامها.[38] كما شارك ممثلو Tor في العديد من مؤتمرات المباحث الفدرالية وتنفيذ القانون الدولي لإطلاع المسؤولين على قدرات Tor بالإضافة إلى ما يقدمه من مزايا لعملائهم أثناء إجراء التحقيقات.[39] كما تلقوا دعوات منتظمة لحضور وإلقاء كلمات في العديد من سلطات تنفيذ القانون سواء المحلية أو الدولية للتوعية وتدريب المستخدمين على مزايا ومنافع استخدام سبل الاتصال السرية والآمنة.

ثم قمنا بعد ذلك، وخصوصًا في حالة Tor، بدراسة استخدام البيانات في العالم الواقعي وجمعها من مصادر مختلفة. وعلى الرغم من احتمالية وجود مشكلة إن كان القدر الأكبر من البيانات المنقولة عبر شبكات Tor هو لممارسة أنشطة غير شرعية، إلا أن هذا ما لم تؤكده البيانات المتاحة. فعلى سبيل المثال، أجرى Chaabane وزملائه (2010) فحصًا لحوالي 373 جيجا بايت من البيانات المنقولة عبر شبكة Tor والتي تم جمعها من ستة نقاط خروج، وموزعة عبر مختلف أنحاء العالم، لمدة استمرت 23 يومًا أواخر عام 2009 وفي مطلع 2010.[40] وما توصلوا إليه هو أن حوالي 52 بالمائة من حجم البيانات المتدفقة كان لمشاركة الملفات من نظير إلى نظير P2P (مثل BitTorrent)، كان نصفها غير مشفر. وبلغت

---

[37] مشروع Tor, "كيفية إدارة الملايين من الوكلاء الجدد في شبكة Tor," منشور في مدونة بتاريخ 5 سبتمبر/أيلول 2013.

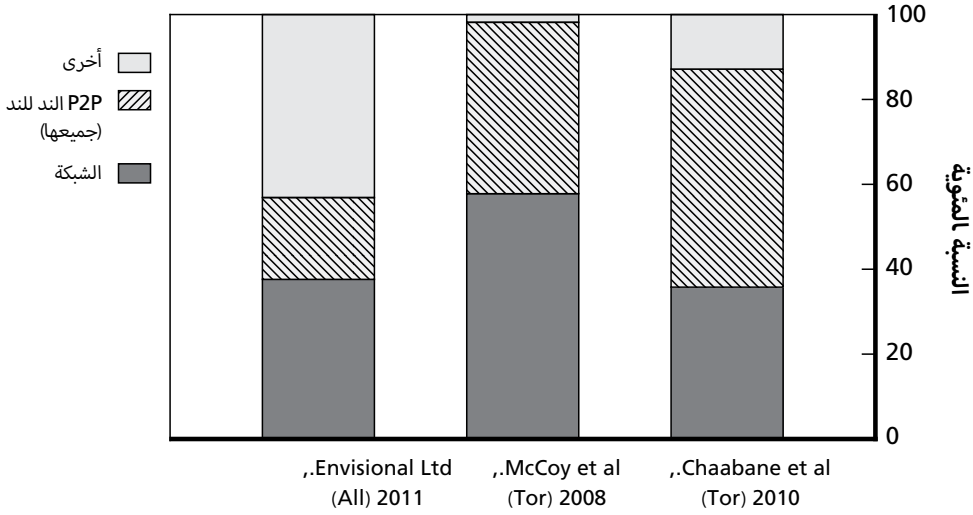
[38] للتعرف على الوصف الكامل لتفاصيل مستخدمي Tor، أنظر مشروع Tor "الإصدار"، صفحة إنترنت، غير مؤرخة.

[39] مشروع Tor "تقرير عن رحلة Tor، التدريب المقدم للشرطة الهولندية والبلجيكية" منشور في مدونة، بتاريخ 5 فبراير/شباط 2013؛ مشروع Tor "تقرير حول مؤتمر المباحث الفدرالية المنعقد في أكتوبر/تشرين الأول"، منشور في مدونة، بتاريخ 16 ديسمبر/كانون الأول 2012.

[40] Abdelberi Chaabane, Pere Manils, and Mohamed Ali Kaafar, "Digging into Anonymous Traffic: A Deep Analysis of the Tor Anonymizing Network," in Proceedings of the 2010 Fourth International Conference on Network and System Security, September 2010، سبتمبر/أيلول 2010.

نسبة تدفق بيانات غير مشفرة عبر الشبكة 36 بالمائة، و 5 بالمائة كانت تدفق لبيانات مشفرة، و 25.0 بالمائة للمراسلة الفورية، والبقية كانت لاتصالات متنوعة وبروتوكولات نصية فقط. وبالمثل، لم يثبت أن تدفق البيانات غير المشفرة لم يستخدم في أغراض غير مشروعة؛ ولا يمكن الجزم بما إذا كانت نسبة المراسلة الفورية غير مشروعة أم لا - وبغض النظر عن ذلك، فستكون النسبة الإجمالية النهائية ضئيلة للغاية. وقد أثبت بحث آخر ما يدعم تلك النسب المرتفعة لتدفق الاتصالات النصية فقط (58 بالمائة) نقل بيانات عبر برنامج BitTorrent (40 بالمائة) من 709 جيجا بايت من تدفق البيانات عبر شبكات Tor.[41] وبالمقارنة بين التقديرات لعام 2011، نجد أن إجمالي تدفق البيانات عبر الشبكة يمثل 38 بالمائة من إجمالي نطاق الإنترنت في الولايات المتحدة، بينما تشكل مشاركة البيانات عبر الند للند P2P حوالي 19 بالمائة من إجمالي نطاق الاتصال.[42] يوضح الشكل رقم 7.1 ملخصًا بتلك النتائج.

الشكل 7.1
مقارنة بين تدفق البيانات عبر Tor والإنترنت (من حيث الحجم)



41 Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker, "Shining Light in Dark Places: Understanding the Tor Network," in *Proceedings of the 8th International Symposium on Privacy Enhancing Technologies*, Leuven, Belgium, July 2008.

42 Envisional, Ltd., *Technical Report: An Estimate of Infringing Use of the Internet*, Cambridge, UK, January 2011, p. 49.

وبما أن القسم الأكبر من تدفق البيانات عبر Tor هو لمشاركة الملفات عبر P2P، فساعد ذلك على فحص نوعية الملفات التي تتم مشاركتها. وقد ورد في تقرير لفحص عينة تضم 100,000 ملف من ملفات BitTorrent، أن حوالي 85 بالمائة منها كانت ملفات فيديو، انقسمت إلى مقاطع إباحية (36 بالمائة) و أفلام (35 بالمائة) وبرامج تلفزيونية (13 بالمائة). بينما شكلت البرامج والملفات الموسيقية وألعاب الكمبيوتر مجتمعة حوالي 14 بالمائة من إجمالي تدفق البيانات عبر BitTorrent. علاوة على ذلك، أوضح التقرير أن حوالي 64 بالمائة من إجمالي الملفات كانت مواد محمية بحقوق النشر، مما يعني أن أغلب المواد الإباحية غير محمية بحقوق النشر. ولم يتمكن معدو التقرير من تحديد نسبة محتويات المواد الإباحية غير المشروعة أو المحمية بحقوق النشر.[43]

وعند فحص أنواع المواقع التي يتصفحها مستخدمو Tor، اكتشف Chaabane وزملائه (2010) النتائج التي أعيد نشرها في الجدول 7.1.

الجدول 7.1.
أنواع المواقع الإلكترونية الأكثر زيارة من قبل مستخدمي متصفح Tor

التصنيف	الفئة	النسبة المئوية
1	محركات بحث/بوابات	14.45
2	المواد الإباحية	11.50
3	حواسب/الإنترنت	11.45
4	شبكات التواصل الاجتماعي	9.52
11	المدونات / التجارة عبر الإنترنت	2.26
13	وسائط البث/ Mp3	1.82
14	تنزيل البرمجيات	1.66
36	القرصنة	0.30
40	السياسية	0.18
42	غير قانونية / محل شك	0.15
52	غير قانونية / المخدرات	0.06

المصدر: Chaabane et al., 2010.

[43] Envisional, Ltd., 2011, p. 10.

تشير النتائج إلى أنه من بين كافة الأنشطة التي خضعت للفحص في شبكة Tor، لم يكن سوى 11.5 بالمائة منها لتصفح ما تم اعتباره مواد إباحية (وهو ما يعتبره البعض نشاطًا غير قانوني) و 0.21 بالمائة فقط كانت أنشطة غير قانونية صراحة (وفقًا لأحكام قانون الولايات المتحدة).

بعد ذلك، عملنا على دراسة التوزيع العالمي لمستخدمي Tor. إذا كان ما يشغل بال الزعماء السياسيين في النهاية هو الأنشطة غير المشروعة التي يمارسها الأمريكيون، فسيكون من المقلق أن نكتشف أن الغالبية العظمى من مستخدمي Tor هم من مواطني الولايات المتحدة الأمريكية. يوضح الجدول 7.2 توزّع أعلى خمس عملاء من ثلاثة أبحاث مستقلة.

كما يوضح الجدول 7.2 أعداد ونسب عملاء Tor (التي تم إحصاؤها باستخدام عنوان بروتوكول الإنترنت الفريد) المتصلين بأحد نقاط الدخول إلى شبكة Tor التي يستخدمها الباحثون، ومصنفة حسب الدولة. يوضح القسم الأيمن 7,571 طلب عميل تم جمعه خلال 2007-2008، بينما يوضح القسم الأيسر 7,575 طلب تم جمعها خلال 2009-2010، والجانب الأيسر يوضح 932,5 طلب تم جمعها خلال 2010. توضح هذه البيانات أن غالبية الطلب على شبكة Tor تأتي دائمًا من ألمانيا، ويليها الولايات المتحدة ثم الصين ثم إيطاليا، وقد بلغ تدفق البيانات من الولايات المتحدة حوالي 13 بالمائة من إجمالي مستخدمي Tor. وقد أكدت هذه النتائج أيضًا البيانات التي قدمها مشروع Tor نفسه.[44]

وفي بحث آخر، قام Huber and colleagues (2010) بدراسة طلبات HTTP فقط، واكتشف أن غالبية الطلبات المنقولة عبر الشبكة هي لشبكات التواصل الاجتماعي ومحركات البحث ومواقع مشاركة الملفات.[45]

وقد أظهر فحص تلك البيانات (تدفق البيانات عبر Tor على حسب الخدمة ودولة العميل) أنه في حين كون غالبية تدفق البيانات غير مشفرة إما بتصفح الشبكة أو بمشاركة الملفات عبر تقنيات P2P، إلا أن نسبة محدودة للغاية (حوالي 13 بالمائة) هي لمستخدمين من داخل الولايات المتحدة الأمريكية.

ثم عملنا على تقييم بعض المزايا التي يتمتع بها Tor والتي تُموّل من قبل مكتب الديمقراطية وحقوق الإنسان والعمل. وعلى هذا الأساس، نقول إن الهدف الأساسي لم يكن دراسة وظيفة بعض الخدمات المخفية في Tor، بصفتها عنصر هام وضروري في تطبيق

---

44 مشروع Tor, "أهم 10 دول من حيث المستخدمين المتصلين مباشرة," قاعدة البيانات، غير مؤرخ.

45 Markus Huber, Martin Mulazzani, and Edgar Weippl, "Tor HTTP Usage and Information Leakage," in *Proceedings of the 11th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security*, Linz, Austria, May 2010.

الجدول 7.2
توزيع مواقع عملاء متصفح Tor

Chaabane et al. (2008–2007)			McCoy et al. (2010–2009)			Li et al. (2010)		
الدولة	العدد	%	الدولة	العدد	%	الدولة	العدد	%
ألمانيا	304,2	30	ألمانيا	114,1	15	ألمانيا	076,1	18
الصين	988	13	**الولايات المتحدة الأمريكية**	**970**	**13**	**الولايات المتحدة الأمريكية**	**734**	**12**
الولايات المتحدة الأمريكية	**864**	**11**	بولندا	839	11	إيطاليا	657	11
إيطاليا	254	3	رومانيا	583	8	الصين	469	8
تركيا	221	3	روسيا	553	7	فرنسا	356	6
أخرى	940,2	61	أخرى	516,3	46	أخرى	640,2	45
الإجمالي	571,7	100	الإجمالي	575,7	100	الإجمالي	932,5	100

المصادر: Chaabane et al., 2010, p. 19; McCoy et al., p. 72; and Bingdong Li, Esra Erdin, Mehmet Hadi Güneş, George Bebis, and Todd Shipley, "تحليل لاستخدام تقنيات إخفاء الهوية," in *Proceedings of the Third International Conference on Traffic Monitoring and Analysis*, Vienna, Austria, April 2011.
ملحوظة: تم إضافة تأكيدات.

Tor ككل. تزوّد خدمات Tor الخفية الأفراد بآلية تمكّنهم من استضافة تطبيقات الإنترنت (مثل المواقع) واستخدامها بسرية ضمن شبكة Tor الكبيرة المخفية عن أعين العامة وسلطات إنفاذ القانون.[46] ورد في الكثير من التقارير أن الخدمات المخفية تُستخدم في الأنشطة الإجرامية، مثل مواقع تجارة التهريب الإلكترونية (مثل طريق الحرير) ومواد استغلال الأطفال.[47] وعندما أضيف لها العملات المجهولة التي تستخدم للدفع، أثبت مزيج التقنيات هذا صعوبة على قوات تطبيق القانون باحتوائها ومتابعتها. وعلى الرغم من كون خدمات Tor المخفية خارج نطاق هذا التحليل، إلا أنها تعتبر عنصرًا هامًا يتطلب اهتمامًا أكبر لأنها تشكل تحديًا صعبًا أمام سلطات تنفيذ القانون، ولذلك فهي تستحق الاعتراف بها.

وتلخيصًا لما سبق، خلصنا إلى أن Tor قد اجتاز المرحلة الأولى (الاتصال، والدعاية) من اختبار المراحل الثلاث، بغض النظر عن تدابير الوقاية المتعددة ذات الصلة بكل من تطبيق Tor واستخدامه العملي. بيد أنه قد فشل في اجتياز المرحلة الثانية لأنه لا يوفر إمكانات مادية لا يمكن أن تكون موجودة بدونتمويل مكتب الديمقراطية وحقوق الإنسان والعمل. واجتاز الاختبار الثالث، فعلى الرغم من توفر عدد محدود من تدابير الوقاية، إلا أنه يتوفر بدون أي مقابل مادي. بالرغم من ذلك، وبغض النظر عن شعبية Tor وإمكاناته المذهلة، فقد خلصنا إلى أن تمويل مكتب الديمقراطية وحقوق الإنسان والعمل لم يجعل من استخدام هذه الأداة في أغراض غير مشروعة.

مشروعان آخران

يوفر أحد هذين المشروعين خدمات تطبيقات لشبكة الإنترنت وللحواسب الشخصية والهواتف المحمولة، والتي صممت خصيصًا لمساعدة نشطاء حقوق الإنسان والصحافيين وغيرهم من الأطراف المعنية على جمع وتوثيق ومشاركة قضايا ومشكلات وانتهاكات حقوق الإنسان بطريقة آمنة.

وبتطبيق الاختبار الثلاثي الأجزاء لاكتشاف الاستخدام غير الشرعي، لاحظنا أنه لكون هذا المشروع في الأساس عبارة عن تطبيق يسمح بالحفظ الآمن، فإنه قد يصلح جزئيًا لحل مشكلة الاتصال التي يواجهها المجرمون، حيث يمكن للعديد من المجرمين إنشاء حساب مشترك عبر هذا التطبيق وتبادل المحتويات من خلاله. وبهذا يساعد في تبادل المحتويات بين المستخدمين المعلومين.

---

46 I.e., the so-called "dark web".

47 Alex Biryukov, Ivan Pustogarov, Fabrice Thill, Ralf-Philipp Weinmann, "Content and Popularity Analysis of Tor Hidden Services," 2013.

ثانيًا، تعتبر إمكانية الحفظ الآمن للملفات (أي تشفيرها) من المزايا التي تتوفر بسهولة للمجرمين من خلال الكثير من التطبيقات والبرمجيات المتاحة الأخرى. وحتما هناك الكثير من البدائل التي لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل، توفر خدمة التخزين الآمن للملفات نفسها، وتكون على الأغلب أيسر للاستخدامات غير المشروعة. وتشتهر تلك الأدوات باسم cyberlockers ومنها MegaUpload و RapidShare و HotFile.

ثالثًا، في حين يتوفر هذا التطبيق مجانًا، فإن هناك عدة تدابير وقائية قد تحد من استخدامه في أنشطة غير مشروعة. تُشفّر الملفات المخزنة على تطبيقات العميل أو المرفوعة على خدمات الإنترنت، مما يمنع مشغّلي الخدمات هذه من الإطلاع عليها. لكن يستطيع المشغلون مراقبة بيانات التعريف ذات الصلة باستخدام الحساب والدخول إلى الموقع (مثل تواجد الملفات، عناوين بروتوكول الإنترنت المستخدمة في تسجيل الدخول إلى الحساب) والتي قد تصبح بعد ذلك متاحة لسلطات إنفاذ القانون. وهذا ما سيؤدي إلى إحجام المجرمين عن استخدام هذه الأداة، لأنها لا تمنحهم قدرًا من السرية يرنون إليه لإخفاء أنشطتهم أو مواقعهم.

بإيجاز، استطاع هذا المشروع اجتياز الاختبار الأول (الاتصال) بشكل جزئي، وفشل في اجتياز الاختبار الثاني (الميزة المادية لصالح المجرمين)، واجتاز الاختبار الثالث (التوفر العام). وبناء على ذلك نخلص في النهاية إلى أنه من المستبعد استخدام المشروع المموّل من قبل مكتب الديمقراطية وحقوق الإنسان في أغراض غير مشروعة، مقارنة بالحلول التي لا يمولها المكتب.

أما المشروع الثاني فيوفر بيئة تشغيل يمكن أن تقلع باستخدام قرص تخزين USB، مع ضبط مسبق لإعدادات برامج حماية الخصوصية لتمكين المستخدم من تصفح الإنترنت بسرية تامة وبأمان. ويسهل الحصول على اتصال غير مراقب بالإنترنت، عبر استخدام منصة تشغيل آمنة تحول دون وصول البرامج الضارة التي قد تتسبب في كشف هوية المستخدم. كما يمكن ضبط إعدادات هذه الأداة باستخدام ملف نظام مشفر أو للقراءة فقط، بحيث يحول دون حفظ غير مقصود لملفات قد تكشف معلومات شخصية أو تضر بالخصوصية.

أدركنا عند تنفيذ الاختبار الثلاثي الأجزاء للاستخدام غير المشروع، ونظرًا لكون هذا المشروع مصمم خصيصًا ليوفر منصة آمنة من الاتصالات السرية المجهولة، فإنه لا يسهم بشكل مباشر أو بطريقة محددة في حل أي من مشكلات الاتصال أو تحديد الهوية أو الدعاية.

ثانيًا، نظرًا لما يوفره المشروع ككل من مزايا قد تسهل الاستخدامات غير المشروعة، فإنه يحوي العديد من المكونات المستقلة التي تكون متاحة بالفعل للمجرمين

من خلال برامج لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل. فعلى سبيل المثال، تُعرف TAILS بأنها بيئة تشغيل توفر نظام تشغيل قابل للإقلاع مُعد مسبقًا لاتصال آمن ومجهول بالإنترنت.[48]علاوة على ذلك، هناك العديد من أنظمة Linux للتشغيل توفر إمكانية التوزيع المباشرة والتشغيل من أقراص CD/DVD ولهذا تكون محمية من الرقابة أو التعرض لتهديدات البرامج الضارة.

ثالثًا، يقتصر توزيع هذه الأداة على أفراد خضعوا لتدريب شخصي في استخدامها، وتم انتقاؤهم من قبل مطوّري هذا المشروع. ومن الواضح أن هذا يوفر تدابير قوية للوقاية من الاستخدامات غير المشروعة.

لذلك، ولأن هذا المشروع فشل في اجتياز الاختبارات الثلاث نخلص في النهاية إلى أنه من المستبعد استخدام هذا المشروع الذي يموله مكتب الديمقراطية وحقوق الإنسان في أغراض غير مشروعة، مقارنة بالحلول التي لا يمولها المكتب.

الملخص

تُلخص Table 7.3 النتائج التي توصلنا إليها من هذا التحليل. تم إدراج كل مشروع يموله مكتب الديمقراطية وحقوق الإنسان في سطور، أما الأعمدة 3 - 1 فتضم النتائج لكل قسم من أقسام الاختبار الثلاثي الأجزاء. يلخص العمود 4 النتائج التي خلصنا إليها من دراسة ما إذا كان تمويل مكتب الديمقراطية وحقوق الإنسان والعمل يسهم في رفع احتمالية استخدام الأداة في أغراض غير شرعية. كما أسلفنا، لكي يقدّم تدخل مكتب الديمقراطية وحقوق الإنسان والعمل إجابة شافية، فيتحتم على الأداة أو المشروع أو الخدمة اجتياز الاختبارات الثلاث كل على حدة. واستنادًا لتحليلنا، خلصنا إلى أن تدخل مكتب الديمقراطية وحقوق الإنسان والعمل في تمويل تلك البرامج لم يسهم في زيادة احتمالية استخدامها في أنشطة غير مشروعة. بينما يوضح العمود 2 أنه ما من أدوات وفرت ميزة مادية للمجرمين تتخطى ما توفره التقنيات البديلة، وتحققت هذه النتيجة بفعل عدة أسباب مختلفة، سبق أن شرحناها ولخّصناها في العمود 5.[49]وعلى وجه الخصوص، اكتشفنا أنه نظرًا لتوفير برمجيات الأمان الرقمي و anti-DDoS بصفة

[48] للمزيد من المعلومات, تفضل بزيارة https://tails.boum.org/.

[49] كما سبق وذكرنا، أن القواعد التي صيغت لإتمام الاختبار الثلاثي الأجزاء قد صيغت بهدف تحديد الحد الأدنى من مجموعة الشروط التي قد تؤدي حين توفرها إلى زيادة في الاستخدامات غير المشروعة. بينما كانت جميع الإجابات على القسم الثاني من الاختبار (هل توفر الأداة أو المشروع أو الخدمة إمكانية مادية لا تتوفر بغياب تمويل المكتب؟) سلبية، هذا لا يقلل من قيمة السؤال، لأن تلك الإجابات لم تكن معلومة قبل ذلك.

الجدول 7.3
ملخص التقييمات

	هل توفر حلًا لمشكلة اتصال المجرمين؟ (1)	هل تمنح للمجرمين ميزة مادية؟ (2)	هل يستطيع المجرمون الوصول إلى الأداة بسهولة ويسر؟ (3)	هل ساهمت مشاركة مكتب الديمقراطية وحقوق الإنسان والعمل في زيادة احتمالية الاستخدام في أنشطة غير مشروعة؟ (4)	تفسير النتائج (5)
الأمان الرقمي	لا	لا	لا	لا	يقدم التدريب بصفة شخصية، ولا يزود المجرمين بإمكانات مادية.
مضادات حجب الخدمة Anti-DDoS	نعم	لا	لا	لا	يتحتم أن يكون العملاء المنتقون من المزودين داعمين لأنشطة حقوق الإنسان
الشبكات المتداخلة	نعم	لا	نعم	لا	قد تلبي عدة أدوات بديلة لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل احتياجات مستخدمين في أنشطة غير شرعية بشكل أفضل.
الوكيل / الشبكة الافتراضية الخاصة	نعم	لا	نعم	لا	قد تلبي عدة أدوات بديلة لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل احتياجات مستخدمين في أنشطة غير شرعية بشكل أفضل.
الاتصالات الآمنة	نعم	لا	نعم	لا	عدة أدوات بديلة غير مدعومة من قِبل مكتب الديمقراطية وحقوق الإنسان والعمل وتزوّد إمكانات مشابهة، قد تلبي احتياجات مستخدمين في أنشطتهم غير الشرعية بشكل أفضل.
Tor	نعم	لا	نعم	لا	قدرات متطورة ومعقدة، وقاعدة مستخدمين ضخمة؛ Tor قبل أي تدخل من قبل مكتب الديمقراطية وحقوق الإنسان والعمل.
أخرى / المشروع أ	لا	لا	نعم	لا	أدوات بديلة غير مدعومة من قبل مكتب الديمقراطية وحقوق الإنسان والعمل وتزوّد إمكانات مشابهة، قد تلبي احتياجات مستخدمين في أنشطتهم غير الشرعية بشكل أفضل.
أخرى / المشروع ب	لا	لا	لا	لا	ينتقي مالكو المشروع المستخدمين بعناية.

ملحوظة: يحوي هذا الجدول نتائج التحليل المُلخصة والمشروحة في هذا التقرير. وعلى وجه الخصوص، يلخص هذا الجدول نطاق الزيادة في احتمالية استخدام البرامج التي يمولها مكتب الديمقراطية وحقوق الإنسان والعمل في أنشطة غير مشروعة بواسطة المجرمين.

شخصية أو للعملاء ممن يدعمون أنشطة حقوق الإنسان بعد منحهم حق استخدامها من قبل المشغلين، فإنها لا تسهم في ارتفاع احتمال استخدامها لأغراض غير مشروعة. أما بخصوص تقنيات الشبكات المتداخلة، وأدوات الوكالة / الشبكات الافتراضية الخاصة، وأدوات الاتصالات الآمنة، فهناك عدة أدوات بديلة متاحة لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل، وتقدم قدرات مشابهة وربما تكون أكثر ملائمة للأنشطة الإجرامية، لأنها، على سبيل المثال، تعتبر بمثابة خدمات تُدار في دول أجنبية ولا تمتثل بالضرورة إلى مطالبات سلطات إنفاذ القانون في الولايات المتحدة. ثم بعد ذلك، على الرغم من توفير شبكة Tor لخدمات تشفير وسرية قوية، فإن مزاياه الجوهرية سبقت أي بديل آخر موله مكتب الديمقراطية وحقوق الإنسان والعمل. وفي الختام، وجدنا أن كلًا من المشروعين الإضافيين اللذين قمنا بتقييمهما لا يسهمان في زيادة الأنشطة الإجرامية إما لتوفر الكثير من الأدوات البديلة والمتاحة للمجرمين أو بسبب فحص مشغلي البرنامج للمستخدمين المحتملين.

وتلخيصًا لما سبق، واستنادًا إلى فرضياتنا ومنهجيتنا، فقد خلصنا في النهاية إلى أن مشاركة مكتب الديمقراطية وحقوق الإنسان والعمل في تمويل أدوات الخصوصية والسرية هذه لم يؤدّ إلى زيادة احتمالية استخدامها لأغراض غير مشروعة.

لاحظ أنه عند استخدامنا للمنهجية وإطار العمل المعد خصيصًا لتقييم تلك المشروعات بعينها، أدركنا أنها صالحة للتعميم، ويمكن استخدامها في تقييم مشروعات مستقبلية.

تدابير احترازية إضافية للحد من المخاطر

نظرًا للتنوع في استخدام تقنيات وخدمات الخصوصية والأمان الخاضعة للتقييم ضمن هذا التقرير، فإن التحديات التي تواجهها الحكومات التي تسعى إلى تمويل أدوات حرية الإنترنت تنقسم إلى شقين. أولًا، قد تزعم الحكومات بأن الفوائد المترتبة على تعزيز الحرية (لمستخدمي الانترنت على سبيل المثال) تفوق التكاليف المتكبدة جراء إعطاء الحرية للمجرمين بما يمكنهم من الإفلات من الملاحقة القضائية. ثانيًا، يمكنها القول بأن مشاريعها قد تكون، وربما هي بالفعل، مُصممة خصيصًا بهدف إمالة واجتذاب الفوائد تجاه إنماء حقوق الإنسان وضد أي نشاط غير مشروع. في واقع الأمر، يختبر التحدي الأول الفوائد المتأتية من دعم تلك الأدوات مقارنةً بتكلفتها، في حين يشير الثاني إلى أن هناك طرقًا يمكن اتباعها لتحسين هذه البرامج بهدف تقليل أي تبعات غير مقصودة.

ومع ذلك، فإن التحدي الثاني يقوم على ثلاثة مقترحات هي: أولًا، أن الطرق التي تستخدمها هذه الأدوات في دعم ممارسة حقوق الإنسان تختلف عن تلك المستخدمة في دعم نشاط غير مشروع؛ وثانيًا، أن المعايير التي تُهيّئ نشطاء حقوق الإنسان لاستخدام أدوات مكتب الديمقراطية وحقوق الإنسان والعمل تختلف عن تلك التي تُهيّئ المجرمين لاستخدام أدوات مماثلة متوفرة في السوق مسبقًا؛ وثالثًا، أنه يمكن وضع تدابير احترازية من شأنها ردع أي استخدام غير مشروع. ونحن نناقش المسألة الثالثة بمزيد من التفصيل في هذا الفصل؛ ألا وهي إمكانية وضع تدابير احترازية إضافية لتقييد أو منع الاستخدام الإجرامي.

أثناء تقييمنا للمشاريع الممولة في إطار حافظة مكتب الديمقراطية وحقوق الإنسان والعمل، قمنا بتحديد عدد من التدابير الاحترازية والتصميمات التي من شأنها تقليل وتقييد استخدامها من قبل المجرمين. في بعض الحالات، لا تتاح المشاريع سوى لمجموعة محدودة من الأفراد المعروفين الذين خضعوا للفحص والتدقيق من قبل أصحاب المشروع والمُشَغِّلين. في حين أن القدرة على إجراء تحقيق قانوني يوفر رادعًا

قويًا ضد الاستخدام الإجرامي في حالات أخرى. وعلاوةً على ذلك، فلقد تبين في حالة استخدام [Tor] أنه حتى الأدوات الأكثر تطورًا لا تزال عرضة للخطأ البشري وتحقيق سلطات إنفاذ القانون.

ثمة طريقة لتهدئة المخاوف بشأن الاستخدام غير المشروع للأدوات الممولة بواسطة مكتب الديمقراطية وحقوق الإنسان والعمل ألا وهي التشجيع على التوضّع الأوسع نطاقًا والتدريب على السلامة الرقمية ونشر التوعية بواسطة مستفيدين أكثر من التمويل في مزيد من البلدان حول العالم. ويمكن للمكتب أيضًا مطالبة المستفيدين من تمويله بتوثيق التدابير الاحترازية والتصميمات والافتراضات وغيرها من العوامل التي من شأنها تقليل أو تقييد أو ردع استخدام تقنياته من قبل مجرمين. إضافةً إلى ذلك، يمكن للمكتب أيضًا مطالبة كل جهة حاصلة على تمويل برصد ومراقبة أي دليل على استخدام غير مشروع لأدواته وتوثيق هذا الدليل (بطريقة مناسبة).

وقد يفضي الوضوح في النقاش حول أدوات المراوغة والتحايل إلى مزيد من الشفافية من قبل المكلفين بإنفاذ القانون (وربما مجتمع الاستخبارات) فيما يتعلق بالإبلاغ عن عدد المرات التي أحبطت فيها جهودهم أثناء التحقيقات بسبب تقنيات تعزيز الخصوصية. وهذا الإفصاح العلني يصف استخدام جهات إنفاذ القانون لعمليات التنصت على المكالمات الهاتفية، على الأقل فيما يخص قانون التنصت والذي يُلزم الحكومة بنشر الإحصاءات المتعلقة باستخدامها.[1] فعلى سبيل المثال، أفاد المكتب الإداري للمحاكم الأمريكية أنه قد تم استخدام التشفير في 41 حالة من إجمالي 3576 حالة للتنصت على المكالمات الهاتفية الصادرة في عام 2013، وقد أعاق التشفير جهات إنفاذ القانون من حل التشفير في تسع حالات فقط.[2] وعلاوةً على ذلك، اشتملت نسبة 87% من عمليات التنصت على جرائم مخدرات، بينما اشتملت نسبة 97% من كافة عمليات التنصت منذ عام 2013 على أجهزة محمولة. غير أن هذا لا يوفر سوى رؤية محدودة للصعوبات التي تواجهها جهات إنفاذ القانون، إذ أن قانون التنصت لا يُنظِّم سوى المعلومات التي جُمِعَت وقت الإرسال فحسب. ومن ناحية أخرى، فإن قانون تسجيل الأرقام الهاتفية المطلوبة[3] يُنَظِّم بيانات التعريف، والتي قد تكون أكثر فائدةً

[1] المادة 18، الفصل 119 من قانون الولايات المتحدة، اعتراض وسائل الاتصالات السلكية والإلكترونية والشفهية (2522–2510 §§).

[2] وهذا يتعلق بالاتصالات الشفهية والإلكترونية والسلكية. راجع محاكم الولايات المتحدة تقرير التنصت، 31 ديسمبر 2013. غير أنه يتعين ملاحظة أنه من المحتمل أن تُقلل هذه البيانات من الاستخدام الحقيقي للتشفير بمقدار غير معلوم.

[3] المادة 18، الفصل 206 من قانون الولايات المتحدة، أجهزة تسجيل الأرقام الهاتفية المطلوبة والرصد والتتبع (3127–3121 §§).

نظرًا لأن معظم الرسائل تُرسل عبر الأجهزة المحمولة والإلكترونية. غير أن قانون تسجيل الأرقام الهاتفية المطلوبة (حتى بصيغته المعدلة بموجب قانون مكافحة الإرهاب "باتريوت" لعام 2001) لا يستلزم الإفصاح العلني عن أي إحصاءات مُجمعة. ولهذا، فمن المحتمل أن تساعد البيانات الإضافية على تحديد المدى الذي تسهل به الأدوات المضادة للرصد والرقابة وقوع نشاط إجرامي.

وعلاوةً على ذلك، بينما حددنا مسبقًا بعض الاختلاف والتباين بين مستخدمي الانترنت وبين تفضيلات المجرمين لتلك المشاريع، إلا أنه يمكن إجراء بحث إضافي لفهم التفضيلات المتمايزة هذه بشكل أشمل (أي المراوغة والتحايل والتشفير والوصول وقابلية الاستخدام والتعليم). وهذا من شأنه مساعدة مكتب الديمقراطية وحقوق الإنسان والعمل على منح جوائزه للجهات التي تعمل على تطوير وإنماء القدرات التي تزيد اهتمام مستخدمي الانترنت العاديين بها وتنقص اهتمام المجرمين بها. وإضافةً إلى ذلك، قد يساعد بحث مخصص لفهم أوضح لهذه التفضيلات بكشف مزيج من التدابير الاحترازية ليتم تطبيقها عبر محفظة الجهات الحاصلة على المنح والتمويل.

وأخيرًا، لا يُعرف في الوقت الراهن سوى القليل بشأن مدى اختراق وتجاوز أنواع مختلفة من حركة البيانات على الإنترنت (قانونية وغير مشروعة) لأدوات الخصوصية والأمن بشكلٍ عام، والأدوات التي خضعت للتقييم ضمن محفظة مكتب الديمقراطية وحقوق الإنسان والعمل بشكل خاص. ولعل للبحث الذي يدرس سلوكيات الشبكة هذه ويحدد مقدارها بطريقة قانونية[4] تراعي الخصوصية فائدة عظيمة في مناقشة هذه السياسة الحاسمة بشأن الاستخدام غير المشروع لأدوات حرية استخدام الإنترنت.[5]

---

[4] على سبيل المثال، في حين أن التحليل واسع النطاق لحركة الشبكة الظاهرية الخاصة والشبكة Tor يعد أمرًا ممكنًا من الناحية التجريبية، إلا أنه يلزم توخي الحذر كي لا يتم انتهاك قوانين التنصت الأمريكية، مثل قانون خصوصية الاتصالات الإلكترونية (18 U.S.C. §§2511-2522).

[5] لمناقشة البحث الأخلاقي لأحد المعلقين في هذا المجال، راجع [كريستوفر سفيان]، "المعايير المجتمعية المُطبقة على الأبحاث بشأن مُستخدمي الشبكة المجهولية"إيضاحات بشأن علوم الحاسب، المجلد 7126، 2012.

الخـاتمة

تناول هذا التقرير النطاق المحتمل لاستخدام مشروعات حرية استخدام الإنترنت التي تمولها وزارة الخارجية الأمريكية في أغراض غير مشروعة. واستهل تناوله بالمزايا التي تنطوي عليها تلك المشروعات في دعم مكتب الديمقراطية وحقوق الإنسان والعمل في رسالته لتعزيز وتأمين حرية استخدام الإنترنت في جميع أنحاء العالم لأغراض حماية حقوق الإنسان. وتابع بدراسة إمكانية استغلال تلك المشروعات في أغراض غير مشروعة، من خلال تطبيقه لهذا الاختبار المقسم إلى ثلاثة أجزاء: هل توفر حلًا لمشكلة التواصل التي يواجهها المجرمون؟ هل تمنح المجرمين ميزة مادية؟ هل يستطيع المجرمون الوصول إليها بسهولة؟

وعلى الرغم من إبداء الكونجرس لمخاوفه بشأن استغلال حرية استخدام الإنترنت في أغراض غير مشروعة، إلا أن تمويل البرنامج يسري على قدم وساق منذ عدة سنوات، وهو ما يؤكد على اجتماع الآراء على اعتباره عنصرًا هامًا ومفيدًا لسياسات الولايات المتحدة الخارجية. فعلى سبيل المثال، ازداد تمويل الكونجرس لمكتب الديمقراطية وحقوق الإنسان والعمل خلال السنوات المالية المنصرمة، بغض النظر عن قيود الميزانية المفروضة بموجب قانون الرقابة على الميزانية لسنة 2011، والاستقطاعات الضخمة للعديد من برامج الدعم الأجنبي. وفي الواقع، تجاوزت الاعتمادات التي قدمها الكونجرس المبلغ المطلوب في ميزانية الرئيس في السنوات المالية المنصرمة، وهو ما يشير إلى الدعم الشديد لمهمة مكتب الديمقراطية وحقوق الإنسان والعمل، بإجمالي اعتمادات تشغيلية بلغت 8.18 مليون دولار خلال العام المالي 2009 لترتفع إلى 32.3 مليون دولار للعام المالي 2015.[1] وينعكس هذا

[1] وزارة الخارجية الأمريكية، تقرير مجلس الشيوخ لتبرير ميزانية العام المالي *2011*، الإصدار *1*: عمليات وزارة الخارجية، 1 فبراير (شباط) 2010، الصفحة 351؛ "بيان إيضاحي قدمه السيد/ روجرز من ولاية كنتاكي، بصفته رئيس لجنة الاعتمادات بمجلس النواب، بخصوص تعديلات مجلس النواب على تعديل مجلس الشيوخ لقانون حقوق الإنسان رقم 83، من قانون الاعتمادات الموحدة والمستمرة لعام 2015"، سجل الكونجرس الإصدار 160، رقم 151، بتاريخ 11 ديسمبر (كانون الأول) 2014، H9948.p.

الدعم أيضًا من خلال ما شهده إجمالي عدد الموظفين بدوام كامل في مكتب الديمقراطية وحقوق الإنسان والعمل، والذي ارتفع من 118 موظف خلال العام المالي 2009 ليصل إلى 161 في العام المالي 2015.[2] شهد صندوق دعم حقوق الإنسان والديمقراطية، والذي تطلق عليه وزارة الخارجية اسم "البرنامج الرئيسي لمكتب الديمقراطية وحقوق الإنسان والعمل"[3] نموًا مستقرًا في مستويات التمويل خلال السنوات المالية المنصرمة.

وإلى جانب التحليل سالف الذكر والوارد في هذا التقرير، أوردنا أيضًا دراسة متعمقة إضافية لمشكلة الاستخدام غير المشروع لتقنيات الأمن والخصوصية والتي تعتبر مشكلة معقدة. في البداية، وكما أسلفنا الذكر، نؤكد على عدم إمكانية تقييد استخدامات التكنولوجيا. فسواء استخدم فرد سيارة أو قلمًا أو هاتفًا أو برنامجًا للولوج إلى الإنترنت العام، هناك فرصة ضئيلة لتفعيل الاستخدام الشرعي لها مع حظر الاستخدامات غير الشرعية في الوقت نفسه. صرح أحد مطوري البرمجيات، أثناء تعليقه على احتمالية الاستخدام المزدوج، قائلًا: "لم يكن هذا أبدًا هو الغرض المستهدف، ولكن ما من طريقة ممكنة لحظر استخدام بعينه لتلك الأدوات دون التضحية بمميزاتها كافة".[4] وكان ما يرمي إليه هذا المطور هو مشكلة ترشيح المحتويات غير الشرعية (أو أي نوع من المواد المشكوك بأمرها) ومنع استخدامها في أحد برامج الاتصال، الأمر الذي يستلزم توفر قدرة فحص وتدقيق كل رسالة تمر عبره. فعلى الرغم من سمو الهدف من خاصية الفحص والتدقيق هذه، إلا أنها تعتبر انتهاكًا فاضحًا للخصوصية وهذا ما صُمم البرنامج للوقاية منه.

ومن المفيد أيضًا الانتباه إلى احتمالية استخدام التشكيلات الإجرامية للعديد من التقنيات المختلفة، غير الممولة من قبل حافظة استثمارات مكتب الديمقراطية وحقوق الإنسان والعمل، لتتمكن من التواصل عبر الإنترنت، وفي أحيان كثيرة، هذه هي التقنيات التي يستخدمها الأمريكيون يوميًا. فعلى سبيل المثال، ذُكر في مقال صدر مؤخرًا "هناك الكثير من التقنيات الرئيسية التي يستطيع المجرمون استخدامها لإخفاء أنشطتهم، مثل: هواتف الأقمار الصناعية، رقم التعريف الشخصي [PIN] الرسائل عبر هواتف

---

[2] وزارة الخارجية الأمريكية،تقرير الكونجرس لتبرير ميزانية العام المالي *2010*، 12 مايو/أيّار 2009، الصفحة 367؛ وزارة الخارجية الأمريكية، تقرير الكونجرس لتبرير ميزانية العام المالي *2016*، الملحق *1:* المشاركة الدبلوماسية لوزارة الخارجية الأمريكية،2 فبراير/شباط 2015، الصفحة 237.

[3] وزارة الخارجية الأمريكية، مكتب الديمقراطية وحقوق الإنسان والعمل، "برامج المكتب"، صفحة إنترنت مُحدثة.

[4] "لقاء مع Brend Kreuss من شركة "TorChat منظمة Free Software، بتاريخ 26 أغسطس/آب 2013.

BlackBerry وحتى خدمة Apple iMessage"[5] وخلصت المحادثات التي جرت بين الخبراء الأمنيين وخبراء حرية استخدام الإنترنت إلى استخدام المجرمين لخدمات Skype، والرسائل الفورية، والدردشة المنقولة عبر الإنترنت، [6] وكل من Reddit و Facebook والرسائل الإلكترونية المشفرة بالإضافة إلى الهواتف الخلوية المسروقة. كما شرح تقرير صدر مؤخرًا تقنيات السوق السوداء والتي تتضمن كافة الخدمات بداية من منتديات المحادثة الفورية وتوصيل الرسائل الإلكترونية (شاملة الإرسال السري لمسودات الرسائل الإلكترونية)، والمنتديات الشبكية وحتى الحسابات الخاصة على Twitter.[7] ووفقًا لتقرير آخر، أشار إلى استخدام المجرمين أيضًا لخدمات مشاركة الصور والفيديو على الإنترنت (Instagram) لشراء وبيع المخدرات عبر الإنترنت،[8] وموقع السؤال والجواب fm.ask الذي يخفي الهويات، والذي يُستخدم في الحث من جهة، والإجابة من جهة أخرى،على الاهتمامات اليومية المتعلقة بحياة الراغبين في أن يصبحوا متطرفين دينيًا.[9]

كما أن هناك أدلة تؤكد ارتياب دول أجنبية وجماعات دينية متطرفة (مثل: الجهاديين) من استخدام أي برنامج كتبه أو دعمه مطورون غربيون (والأمريكيون على وجه الخصوص).[10] ويسري هذا أيضًا سواء كان البرنامج مفتوح أو مغلق المصدر، وحتى لو كان يساعد في حماية هوياتهم أو إخفاء استخدامهم للإنترنت بشكل أفضل. وسيؤدي هذا الارتياب إلى إحجام الكثير من الإرهابيين (أو غيرهم من الأطراف الأجنبية) عن استخدام أي من الأدوات التي مولتها حافظة استثمارات مكتب الديمقراطية وحقوق الإنسان والعمل. تناول العديد من المقالات الصحفية المزيد من الأدلة على ذلك، حيث صنفت عدد من أدوات التشفير عمل على تطويرها خصيصًا مجموعات متطرفة لتضمن

---

[5] Lev Grossman و Jay Newton-Small, "الشبكة السرية: أين توجد حياة المخدرات والإباحية والجريمة في الإنترنت"، *Time* بتاريخ 11 نوفمبر/تشرين الثاني 2013.

[6] برنامج Norton من شركة Symantec "السوق السوداء لجرائم الإنترنت" صفحة إنترنت مُحدثة.

[7] Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, أسواق أدوات الإجرام الإلكتروني والبيانات المسروقة: *Hackers' Bazaar*, Santa Monica, Calif.: RAND Corporation, RR-610-JNI, 2014.

[8] Fletcher Babb, "كيف لا يتم كشف صفقات المخدرات في موقع Instagram", *VentureBeat.com*, 11 سبتمبر/أيلول 2014.

[9] John Hall، "لا تحتاج إلى الكثير، فستحصل على راتبك من هنا، بالإضافة إلى الطعام والمسكن: دليل السفر الإرشادي الذي يستخدمه مقاتلو الدولة الإسلامية في العراق والشام من البريطانيين في إغراء المواطنين البريطانيين للالتحاق بصفوف الجهاديين في العراق" *Daily Mail*، 18 يونيو/حزيران 2014.

[10] Rodrigo Bijou، "استعراض لبرامج التشفير التي يستخدمها الجهاديون"، منشور عبر مدونته بتاريخ 31 أكتوبر/تشرين الأول 2013.

لهم إمكانيات المراسلة النصية مجهّلة المصدر عبر شبكات الحواسب الشخصية والمحمولة.[11] فعلى سبيل المثال، أكدت تقارير متكررة قيام كل من وكالة الفجر والجبهة الإعلامية الإسلامية العالمية (ذراعين للقاعدة) بتطوير برامج تشفير خاصة بهما على نظام تشغيل Android.[12] كما أكد العديد من التقارير قيام المنظمات الإجرامية بتطوير برامج المراسلة الفورية الخاصة بها لتبادل المعلومات المالية التي تقوم بسرقتها.[13]

وللمزيد من التحقق ممّا إذا كانت حافظة استثمارات مكتب الديمقراطية وحقوق الإنسان والعمل تحتضن الأنشطة الإجرامية، تمت دراسة في عالمين: عالم حالي يتضمن المكتب وتمويله، وعالم افتراضي لم تؤسس فيه حافظة استثمارات مكتب الديمقراطية وحقوق الإنسان والعمل مطلقًا. والعديد من المشاريع هذه تتواجد في كلا العالمين. بيد أن التحسينات التي مولها برنامج مكتب الديمقراطية وحقوق الإنسان والعمل تتواجد فقط في العالم الأول. فعلى سبيل المثال، بدأ تنفيذ مشروع Tor في منتصف التسعينيات بالتعاون مع مختبر الأبحاث البحرية الأمريكية، ولكنه يتلقى تمويله حاليًا من قبل كيانات عدة خاصة وعامة. وخلال عام 2012، لم يتجاوز التمويل الاتحادي المخصص له سوى 28 بالمائة مقدمة من وزارة الخارجية.[14] وفي حين أنه من الشرعي طرح تساؤلات حول ما إذا كان تنفيذ هذه التحسينات أدى إلى رفع احتمالية استخدام الأداة في أغراض إجرامية، إلا أننا نؤكد عدم مشروعية، بموجب هذا التحليل، محاسبة مكتب الديمقراطية وحقوق الإنسان والعمل على الاستخدامات الإجرامية لهذه الأدوات على اعتبار أنها كانت لتتواجد بغياب تمويل المكتب.

علاوة على ذلك، فإن مكتب الديمقراطية وحقوق الإنسان والعمل كان واضحًا ومحددًا للغاية عند اختياره لما سيموله من جهود، حيث أكد على تخصيص جهوده لدعم أنشطة التدريب والتكنولوجيا الداعمة لحقوق الإنسان وحرية استخدام الإنترنت في جميع أنحاء العالم:

> بُذلت جهود جبارة لتجنب دعم من يدافعون عن ارتكاب العنف أو أنشطة أخرى تنتهك حريات الآخرين أو تعيق استمتاعهم بها.... وقد صممت تقنيات حرية استخدام الإنترنت الذي يموله الوكالة الأمريكية للتنمية الدولية [USAID]

---

[11] Recorded Future, 2014a, و Bijou, 2013, على الترتيب.

[12] David Kravets, تبني الإرهابيين لتطبيق التشفير الجديد وذلك بعد ما تبع تسريبات سنودون Android Crypto", *Ars Technica*, بتاريخ 1 أغسطس/آب 2014.

[13] Kirk, 2007.

[14] Moody, Famiglietti, و Andronico, LLP, مشروع *Tor, Inc*. والشركات التابعة: البيانات والتقارير المالية المجمعة واللازمة لعمليات التدقيق بموجب متطلبات المعايير القياسية لتدقيق الحكومة ونشرة مكتب شؤون الميزانية والتنظيم رقم *A-133* بتاريخ *31* ديسيمبر/كانون الأول *2013*، توكسبري، ماساتشوستس، في 11 يوليو/تموز 2014ـ الصفحة 12.

> بهدف نشره في البيئات القمعية، وصممت على أساس ما وصل إليها من تعليقات النشطاء والمدونين وغيرهم ممن يعملون في تلك البيئات بهدف تلبية احتياجاتهم. وتعبر أساليب التوزيع وشبكات تقنيات حرية استخدام الإنترنت عن ذلك، وينصب تركيزها على مساعدة الأفراد في ظل البيئات التي تقمع استخدام الإنترنت. في بعض الدول الحساسة، يخضع المشاركون في البرامج إلى تدقيق مُحكم لضمان عدم تمويل الإرهابيين أو المشاركين في الأعمال الاستخباراتية.[15]

كما أورد أيضًا مكتب الديمقراطية وحقوق الإنسان والعمل في تقريره السنوي قائلًا: "دعم البرامج التي تلتزم بمبادئ الديمقراطية، ودعم ومساندة المؤسسات الديمقراطية، وتعزيز ورعاية حقوق الإنسان، وبناء المجتمع المدني في جميع أنحاء العالم، بالإضافة إلى

> عدم التفات مكتب الديمقراطية وحقوق الإنسان والعمل إلى المشروعات التي ترتبط بأي حال بدعم أي عضو أو تابع أو ممثل لها على علاقة بأي منظمة إرهابية، سواء كانوا أعضاء منتخبون في الحكومة أو لم يكونوا كذلك. قد يُطلب من المنظمات التي تتلقى دعوة بتقديم مقترحاتها ومن ثم اعتمادها لتنفيذ المقترح، تقديم المزيد من المعلومات حول المنظمة وأفرادها الرئيسيين ليتم إخضاعهم للفحص والتدقيق.[16]

وفي النهاية، وكما أسلفنا الإيضاح في هذا التقرير، بينما لا تنطوي المشروعات التي يتم دعمها بواسطة حافظة استثمارات مكتب الديمقراطية وحقوق الإنسان والعمل على أي قدرات مادية تخدم المجرمين، إلا أن هذا لا يعني بالضرورة أنها لا توفر خدمات حرجة وربما خطيرة لجمهورها المستهدف من نشطاء حقوق الإنسان والأقليات المعرضة للمخاطر في جميع أنحاء العالم. وإنه من المؤكد، على وجه الخصوص، أن تخفيض أو حظر تمويل تلك المشروعات سيكون له تأثير ضار وسلبي للغاية على نشطاء حقوق الإنسان، والسبب البسيط في ذلك هو ما يتاح أمام المجرمين من فرصة أكبر لاختيار أدوات الأمن والخصوصية التي تمكنهم من ممارسة أنشطتهم غير الشرعية. فيمكنهم استخدام أي من الأدوات الواردة في هذا التقرير، أو غيرها من المنتجات سواء التجارية أو المجانية، ذلك بالإضافة إلى الأدوات المُعدة لأغراض خاصة أو غير الشرعية. وعلى الجانب الآخر نجد أن نشطاء حقوق الإنسان، وهم أقل تمويلًا، يعانون

---

[15] رسالة إلكترونية إلى المحررين من فريق العمل بمكتب الديمقراطية وحقوق الإنسان والعمل، بتاريخ 18 نوفمبر 2013.

[16] وزارة الخارجية الأمريكية، "بيان مكتب الديمقراطية وحقوق الإنسان والعمل السنوي بخصوص تكنولوجيا حرية استخدام الإنترنت"، صفحة إنترنت، بتاريخ 3 إبريل 2013.

من قصور حاد في الخيارات المتاحة لهم من التكنولوجيا التي تضمن لهم حفظ أمنهم وخصوصيتهم. وبالتالي سيؤدي القضاء على التقنيات الشرعية هذه إلى تركهم دون توفير وسائل أو سبل اتصال آمنة وتضعهم في مهب المخاطر التي قد تلحق بهم شخصيًا.[17]

[17] وكان مجتمع Tor هو أول من أثار هذه القضية أمام المحررين.

المراجع

Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Santa Monica, Calif.: RAND Corporation, RR-610-JNI, 2014. As of June 9, 2015: http://www.rand.org/pubs/research_reports/RR610.html

"The Amazons of the Dark Net," *The Economist*, November 1, 2014. As of June 9, 2015: http://www.economist.com/news/international/21629417-business-thriving-anonymous-internet-despite-efforts-law-enforcers

Babb, Fletcher, "Lean on Me: Emoji Death Threats and Instagram's Codeine Kingpin," *Vice.com*, October 24, 2013. As of June 9, 2015: http://noisey.vice.com/blog/lean-on-me

———, "How Instagram's Drug Deals Go Undetected," *VentureBeat.com*, September 11, 2014. As of June 9, 2015: http://venturebeat.com/2014/09/11/how-instagrams-drug-deals-go-undetected/

Bijou, Rodrigo, "An Overview of Jihadist Encryption Programs," blog post, October 31, 2013. As of June 9, 2015: http://www.rbijou.com/2013/03/18/an-overview-of-jihadist-encryption-programs/

Biryukov, Alex, Ivan Pustogarov, Fabrice Thill, Ralf-Philipp Weinmann, "Content and Popularity Analysis of Tor Hidden Services," 2013. As of June 16, 2015: http://arxiv.org/abs/1308.6768

Blackphone, homepage, undated. As of June 30, 2014: https://www.blackphone.ch/

Brandom, Russell, "Iraqis Seek Out New Tools to Blast Through Internet Blockade," *The Verge*, June 18, 2014. As of June 30, 2014: http://www.theverge.com/2014/6/18/5820694/iraqis-seek-out-new-tools-to-blast-through-internet-blockade

Chaabane, Abdelberi, Pere Manils, and Mohamed Ali Kaafar, "Digging into Anonymous Traffic: A Deep Analysis of the Tor Anonymizing Network," in *Proceedings of the 2010 Fourth International Conference on Network and System Security*, September 2010, pp. 167–174.

Chakravarty, Sambuddho, Marco V. Barbera, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis, "On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records," in Michalis Faloutsos and Aleksander Kuzmanovic, eds., *Passive and Active Measurement: Proceedings of 15th International Conference, PAM 2014*, Los Angeles, Calif.: Springer, March 10–11, 2014, pp. 247–257.

De Filippi, Primavera, "It's Time to Take Mesh Networks Seriously (and Not Just for the Reasons You Think)," *Wired.com*, January 2, 2014. As of July 14, 2014: http://www.wired.com/2014/01/its-time-to-take-mesh-networks-seriously-and-not-just-for-the-reasons-you-think/

Dingledine, Roger, "Pre-Alpha: Run an Onion Proxy Now!" email dated September 20, 2002. As of June 12, 2015: http://archives.seul.org/or/dev/Sep-2002/msg00019.html

Edge Velocity Corporation, "About Us," web page, undated. As of June 30, 2014: http://www.edgevelocity.com/about_us.html

Envisional, Ltd., *Technical Report: An Estimate of Infringing Use of the Internet*, Cambridge, UK, January 2011. As of June 9, 2015: http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf

"Explanatory Statement Submitted by Mr. Rogers of Kentucky, Chairman of the House Committee on Appropriations, Regarding the House Amendment to the Senate Amendment on H.R. 83, Consolidated and Further Continuing Appropriations Act, 2015," *Congressional Record*, Vol. 160, No. 151, December 11, 2014.

Faris, Robert, John Palfrey, Ethan Zuckerman, Hal Roberts, and Jillian York, *International Bloggers and Internet Control: Full Survey Results*, Cambridge, Mass.: Harvard University Berkman Center for Internet and Society, August 18, 2011. As of January 23, 2015: https://cyber.law.harvard.edu/publications/2011/International_Bloggers_Internet_Control_Full_Survey_Results

Federal Bureau of Investigation, New York Field Office, "Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court," press release, November 6, 2014. As of June 9, 2015: http://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court

Forde, Patrick, and Andrew Patterson, "Paedophile Internet Activity," *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*, Vol. 97, November 1998. As of January 25, 2015: http://pandora.nla.gov.au/pan/10850/20110125-1520/%7B8DC57715-E250-43B1-91BD-D04752499CA8%7Dti97.pdf

Gambetta, Diego, *Codes of the Underworld: How Criminals Communicate*, Princeton, N.J.: Princeton University Press, 2011.

Goncharov, Max, *Russian Underground Revisited*, Trend Micro, Cybercriminal Underground Economy Series, 2014. As of June 30, 2014: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf

Gorman, Siobhan, "Iran-Based Cyberspies Targeting U.S. Officials, Report Alleges," *Wall Street Journal*, May 29, 2014. As of July 2, 2014: http://online.wsj.com/articles/iran-based-cyberspies-targeting-u-s-officials-report-alleges-1401335072

Grossman, Lev, and Jay Newton-Small, "The Secret Web: Where Drugs, Porn, and Murder Live Online," *Time*, November 11, 2013.

Hall, John, "'U dnt need much, u get wages here, u get food provided and place to stay': The Rough Travel Guide British ISIS Fighters Are Using to Lure Fellow Britons in to Waging Jihad in Iraq," *Daily Mail*, June 18, 2014. As of June 9, 2015: http://www.dailymail.co.uk/news/article-2661177/Travel-light-leave-Islamic-books-home-dont-arouse-suspicion-Isis-militants-offer-travel-advice-jihadists-arriving-Syria-Iraq-Britain.html

Harris, Shane, "Exclusive: Inside the FBI's Fight Against Chinese Cyber-Espionage," *Foreign Policy*, May 27, 2014. As of July 2, 2014: http://www.foreignpolicy.com/articles/2014/05/27/exclusive_inside_the_fbi_s_fight_against_chinese_cyber_espionage

Henry, Ryan, Stacie L. Pettyjohn, and Erin York, *Portfolio Assessment of Department of State Internet Freedom Program: An Annotated Briefing*, Santa Monica, Calif.: RAND Corporation, WR-1035-DOS, 2014. As of June 4, 2015: http://www.rand.org/pubs/working_papers/WR1035.html

"HMA VPN User Arrested After IP Handed Over to the FBI," Hacker10.com, September 28, 2011. As of July 16, 2014: http://www.hacker10.com/internet-anonymity/hma-vpn-user-arrested-after-ip-handed-over-to-the-fbi/

Huber, Markus, Martin Mulazzani, and Edgar Weippl, "Tor HTTP Usage and Information Leakage," in *Proceedings of the 11th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security*, Linz, Austria, May 2010.

"Interview with Bernd Kreuss of TorChat," Free Software Foundation, August 26, 2013. As of June 9, 2015:
https://www.fsf.org/blogs/licensing/interview-with-bernd-kreuss-of-torchat

Joof, Modou S., "'Internet Is Being Used as a Platform for Nefarious and Satanic Purposes,'" Front Page International, July 28, 2013. As of July 16, 2014:
http://frontpageinternational.wordpress.com/2013/07/28/internet-is-being-used-as-platform-for-nefarious-and-satanic-activities/

Kelly, Sanja, Mai Truong, Madeline Earp, Laura Reed, Adrian Shahbaz, and Ashley Greco-Stoner, eds., *Freedom on the Net 2013: A Global Assessment of Internet and Digital Media*, Freedom House, October 3, 2013. As of June 8, 2015:
https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf

Kirk, Jeremy, "Hackers Build Private IM to Keep Out the Law," *ComputerWorld.com*, March 28, 2007. As of July 15, 2014:
http://www.computerworld.com/s/article/9014675/Hackers_build_private_IM_to_keep_out_the_law

Kravets, David, "Terrorists Embracing New Android Crypto in Wake of Snowden Revelations," *Ars Technica*, August 1, 2014. As of August 2, 2014:
http://arstechnica.com/tech-policy/2014/08/terrorists-embracing-new-android-crypto-in-wake-of-snowden-revelations/

Li, Bingdong, Esra Erdin, Mehmet Hadi Güneş, George Bebis, and Todd Shipley, "An Analysis of Anonymity Technology Usage," in *Proceedings of the Third International Conference on Traffic Monitoring and Analysis*, Vienna, Austria, April 2011.

"Libyan Uprising One-Year Anniversary: Timeline," *The Telegraph*, February 17, 2012. As of June 5, 2015:
http://www.telegraph.co.uk/news/worldnews/africaandindianocean/libya/9087969/Libyan-uprising-one-year-anniversary-timeline.html

McCoy, Damon, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker, "Shining Light in Dark Places: Understanding the Tor Network," in *Proceedings of the 8th International Symposium on Privacy Enhancing Technologies*, Leuven, Belgium, July 2008, pp. 63–76.

Moody, Famiglietti, and Andronico, LLP, *The Tor Project, Inc. and Affiliate: Consolidated Financial Statements and Reports Required for Audits in Accordance with Government Auditing Standards and OMB Circular A-133—December 31, 2013*, Tewksbury, Mass., July 11, 2014. As of June 12, 2015:
https://www.torproject.org/about/findoc/2013-TorProject-FinancialStatements.pdf

Norton by Symantec, "The Cybercrime Blackmarket," web page, undated. As of June 30, 2014: http://us.norton.com/cybercrime-blackmarket

O'Carroll, Tanya, "Mobile Technologies Helping Activists and Human Rights Defenders," *Ethical Consumer*, undated. As of June 9, 2015: http://www.ethicalconsumer.org/ethicalreports/mobilesreport/activism.aspx

Patterson, Steven Max, "Mesh Networks and FireChat: How Hong Kong Protestors Are Keeping Communications Alive," *NetworkWorld.com*, October 2, 2014. As of June 8, 2015: http://www.networkworld.com/article/2691105/opensource-subnet/mesh-networks-and-firechat-how-hong-kong-protestors-are-keeping-communications-alive.html

Pauli, Darren, "Tor Exit Node Mashes Malware into Downloads," *The Register*, October 27, 2014. As of June 9, 2015: http://www.theregister.co.uk/2014/10/27/tor_exit_node_mashes_malware_into_downloads/

Protalinski, Emil, "Osama bin Laden Didn't Use Encryption: 17 Documents Released," blog post at *ZDNet.com* website, May 3, 2012. As of January 25, 2015: http://www.zdnet.com/article/osama-bin-laden-didnt-use-encryption-17-documents-released/

Recorded Future, "How Al-Qaeda Uses Encryption Post-Snowden (Part 1)," May 8, 2014a. As of June 5, 2015: https://www.recordedfuture.com/al-qaeda-encryption-technology-part-1/

———, "How Al-Qaeda Uses Encryption Post-Snowden (Part 2)—New Analysis in Collaboration with ReversingLabs," August 1, 2014b. As of June 5, 2015: https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2/

Robinson, David, Harlan Yu, and Anne An, *Collateral Freedom: A Snapshot of Chinese Internet Users Circumventing Censorship*, OpenITP, April 2013. As of June 8, 2015: https://www.teamupturn.com/static/files/CollateralFreedom.pdf

Sandvik, Runa A., "Harvard Student Receives F for Tor Failure While Sending 'Anonymous' Bomb Threat," *Forbes*, December 18, 2013. As of June 30, 2014: http://www.forbes.com/sites/runasandvik/2013/12/18/harvard-student-receives-f-for-tor-failure-while-sending-anonymous-bomb-threat/

Soghoian, Christopher, "Enforced Community Standards for Research on Users of the Tor Anonymity Network," *Financial Cryptography and Data Security, Lecture Notes in Computer Science*, Vol. 7126, 2012, pp. 146–153.

Thompson, Clive, "How to Keep the NSA Out of Your Computer," *Mother Jones*, September–October 2013. As of June 30, 2014: http://www.motherjones.com/politics/2013/08/mesh-internet-privacy-nsa-isp

"Timeline: Egypt's Revolution," *Al Jazeera*, February 14, 2011. As of June 5, 2015: http://www.aljazeera.com/news/middleeast/2011/01/201112515334871490.html

The Tor Project, "Abuse FAQ," web page, undated a. As of June 9, 2015: https://www.torproject.org/docs/faq-abuse.html.en

———, "Tor: Sponsors," web page, undated b. As of June 9, 2015: http://www.torproject.org/about/sponsors.html.en

———, "Inception," web page, undated c. As of June 30, 2014: https://www.torproject.org/about/torusers.html.en

———, "Top-10 Countries by Directly Connecting Users," database, undated d. As of June 30, 2014: https://metrics.torproject.org/users.html

———, "We Need Your Good Tor Stories," blog post, August 17, 2011. As of June 9, 2015: https://blog.torproject.org/blog/we-need-your-good-tor-stories

———, "Trip Report, October FBI Conference," blog post, December 16, 2012. As of July 16, 2014: https://blog.torproject.org/blog/trip-report-october-fbi-conference

———, "Trip Report, Tor Trainings for the Dutch and Belgian Police," blog post, February 5, 2013a. As of July 16, 2014: https://blog.torproject.org/blog/trip-report-tor-trainings-dutch-and-belgian-police

———, "How to Handle Millions of New Tor Clients," blog post, September 5, 2013b. As of June 30, 2014: https://blog.torproject.org/blog/how-to-handle-millions-new-tor-clients

———, "Metrics," database, dated June 30, 2014. As of June 5, 2015: https://metrics.torproject.org

United States Code, Title 18, Chapter 119, Wire and Electronic Communications Interception and Interception of Oral Communications (§§ 2510–2522).

United States Code Title 18, Chapter 206, Pen Registers and Trap and Trace Devices (§§ 3121–3127).

United States Courts, *Wiretap Report 2013*, December 31, 2013. As of March 24, 2015: http://www.uscourts.gov/statistics-reports/wiretap-report-2013

U.S. Department of State, *Congressional Budget Justification for Fiscal Year 2010*, May 12, 2009.

———, *Congressional Budget Justification for Fiscal Year 2011, Volume 1: Department of State Operations*, February 1, 2010.

———, "DRL Internet Freedom Annual Program Statement for Internet Freedom Technology," web page, April 3, 2013. As of June 12, 2015: http://www.state.gov/j/drl/p/207061.htm

———, "Bureau of Democracy, Human Rights and Labor Internet Freedom Annual Program Statement," web page, June 2, 2014. As of June 4, 2015: http://www.state.gov/j/drl/p/227048.htm

———, *Congressional Budget Justification for Fiscal Year 2016, Appendix 1: Department of State Diplomatic Engagement*, February 2, 2015.

U.S. Department of State, Bureau of Democracy, Human Rights, and Labor, "DRL Programs," web page, undated. As of June 9, 2015: http://www.state.gov/j/drl/p/

U.S. House of Representatives, *House Report 112-331—Military Construction and Veterans Affairs and Related Agencies Appropriations Act, 2012*, 2012.

U.S. Senate, *Senate Report 113-81—Department of State, Foreign Operations, and Related Programs Appropriations Bill, 2014*, 2014.

Wickr, "How Wickr Works," undated. As of July 2, 2014: https://www.mywickr.com/how-wickr-works/

Zetter, Kim, "How the Feds Took Down the Silk Road Drug Wonderland," *Wired.com*, November 18, 2013. As of June 30, 2014: http://www.wired.com/2013/11/silk-road/

أشاد مكتب الديمقراطية وحقوق الإنسان والعمل، التابع لوزارة الخارجية الأمريكية، كجزء ضمن جهوده الحثيثة لحماية وضمان الحريات السياسية والاقتصادية وغيرها من حقوق الإنسان، بما ورد في إستراتيجية الولايات المتحدة للفضاء الإلكتروني بهدف مناصرة الحق الأساسي في حرية التعبير والترابط عبر الإنترنت والفضاء الإلكتروني؛ وتمكين الأطراف المؤثرة في المجتمع المدني، ونشطاء حقوق الإنسان، والصحافيين من استخدام الوسائط الرقمية بحرية؛ وتشجيع الحكومات للحد من القيود التي تفرضها إما على حرية التعبير أو حرية نقل وتبادل المعلومات.

ولهذا قام مكتب الديمقراطية وحقوق الإنسان والعمل بتمويل العديد من مشروعات تطوير برامج وتطبيقات الأمن والخصوصية على الإنترنت. إلا أن هناك قدر من المفاضلة يصحب هذا النوع من الاستثمارات. فمن ناحية، يمكن لأدوات حفظ الأمان والخصوصية توفير خدمات آمنة وموثوقة تحفظ سرية وخصوصية مستخدمي الإنترنت، ممن قد يخضعون لولا توفرها للاستهداف أو التصنيف أو يقعون تحت طائلة العقاب نتيجة لأنشطتهم الإلكترونية. ومن ناحية أخرى، يمكن استخدام هذه الأدوات أيضًا لإخفاء أو ارتكاب أنشطة إجرامية. وقد عُني هذا التقرير بدراسة وفحص مجموعة من الأدوات التي مولها مكتب الديمقراطية وحقوق الإنسان والعمل بهدف دعم حرية استخدام الإنترنت وتقييم آثار هذه الأدوات في تعزيز مصالح الولايات المتحدة.

وفي البداية، سنتناول مزايا هذه الأدوات في دعم رسالة مكتب الديمقراطية وحقوق الإنسان والعمل بشأن ضمان حرية استخدام الإنترنت في جميع أنحاء العالم. ثانيًا، سندرس ما تنطوي عليه من إمكانيات واحتمالية استخدامها في أنشطة إجرامية وطرح بعض النماذج على ذلك. ثالثًا، دراسة القدرة على استخدام الأدوات المناظرة، التي لا يمولها مكتب الديمقراطية وحقوق الإنسان والعمل، في تلك الأغراض. ورابعًا، نقوم بفحص واختبار سبل الوقاية والتصميم ونماذج الخدمات التي يمكن تطبيقها للحد من أو حظر استخدام التكنولوجيا في أغراض إجرامية. ويخلص التقرير في خاتمته إلى تأكيد أن دعم مكتب الديمقراطية وحقوق الإنسان والعمل لتوفير أدوات حرية استخدام الإنترنت لم يجعل منها صالحة للاستخدام في أغراض إجرامية، بالمقارنة مع التقنيات البديلة التي لم يمولها المكتب.

NATIONAL SECURITY RESEARCH DIVISION RAND

www.rand.org

$15.00

ISBN7-9110-8330-0 10-
ISBN9-9110-8330-0-978 13-

9 780833 091109 51500

Arabic translation
[Internet Freedom Software and Illicit Activity:
Supporting Human Rights Without Enabling Criminals]
RR-1151/1-DOS