منظور تحليلي

رؤى الخبراء بشأن قضايا السياسات الآنية

RAND CORPORATION

استخبارات الإشارات (SIGINT) للجميع

التوفر المتنامي لاستخبارات الإشارات في المجال العام

كورتني واينباوم (Cortney Weinbaum)، ستيفن برنر (Steven Berner)، بروس ماكلينتوك (Bruce McClintock)

استخبارات الإشارات التي تُعَرَّف بالاختصار (SIGINT)، هي المعلومات الاستخبارية التي يتم جمعها من الاتصالات، أو الإلكترونيات، أو الأجهزة الأجنبية المُصدِرَة للإشارات،[1] وقد اعتُبِرَت تقليدياً وظيفةً حكوميةً متأصلة. وتاريخياً، وحدها الحكومة كانت تملك الوسائل المالية والسلطة القانونية لإجراء أنشطة استخبارات الإشارات، ومن خلال خبراتنا، نجد أن الكثير من أعضاء الحكومة الأمريكية ما زالوا يتبنون هذا الرأي حتى اليوم. لقد اختبرنا وجهة النظر هذه عن طريق إجراء مسحٍ للسوق من أجل البحث عن أمثلةٍ لكيفية تحدي التكنولوجيات الجديدة، والابتكارات، والسلوكيات، لمنظومة التفرد الحكوميّ القائمة. لقد قمنا بدراسة اتساع نطاق التكنولوجيات المتوفرة اليوم، والتي أفادت التقارير أنه سوف يتم نشرها في المستقبل القريب، من أجل فهم القدرات التي توفرها كلٌّ منها، والجمهور والسوق اللذان تخدمهما، وما التبعات التي قد تكون لكلٍّ منها بالنسبة للسياسات والممارسات الحكومية.

لقد كان هذا الأمر جهداً استكشافياً، أكثر من كونه مسعى بحثياً شاملاً. وقد اعتمدنا على موادَّ غير سرّيةٍ ومتاحةٍ للعامة من أجل العثور على أمثلةٍ عن القدرات التي تتحدى منظومة التفرّد الحكوميّ. عَرَّفنا طرقاً قد تؤثّر هذه القدرات والاتجاهات بحسبها على الحكومة الأمريكية من جهة التهديدات الناشئة، والتبعات في السياسات، والتداعيات في مجال التكنولوجيا، والاعتبارات المتعلقة برأس المال البشريّ، والآثار المالية. أخيراً، عَرَّفنا بمجالاتٍ للدراسة المستقبلية يستطيع القادة الأمريكيون وقادة الحكومات المتحالفة الاستجابة بموجبها لهذه التغييرات.

خلال مسحنا للسوق، عثرنا على أمثلةٍ لقدرات استخبارات الإشارات خارج الحكومة، وهي متوفرةٌ للجميع. القدرات التي عثرنا عليها لها تطبيقاتٌ في التوعية بأحوال المجال البحري؛ والمسح المحيطيّ لطيف الترددات الراديوية (radio frequency [RF] spectrum mapping)؛ والتنصّت، والتشويش، والاستيلاء على اتصالات الأقمار الاصطناعية، ومراقبة الفضاء الإلكترونيّ. معظم هذه القدرات متوفرٌ تجارياً، والعديد منها مجانيّ، وبعضها غير قانونيّ. ومن وجهة نظرنا، فإنّ وجود الأسواق القانونية وغير القانونية على حدٍّ سواء، ووجود القدرات تنتج عنه بيئةٌ أصبحت فيها استخبارات الإشارات ذات طابع ديمقراطي، أي أنها أصبحت متوفرة للجميع.

لقد كان للقدرات التي وجدناها تداعياتٌ بالنسبة للحكومة الأمريكية وحلفائها. إنها تعزز بيئة التهديد عن طريق تزويد الخصوم بقدراتٍ ما كان لها أن تكون متوفرةً بشكلٍ آخر، وهي تنطوي على قدرة تهديد الممارسات الحالية

للحكومة الأمريكية في ما يتعلق بشؤون ممارسات جمع المعلومات وتحليلها.

تملك الحكومة الأمريكية فرصةً للاستجابة لهذه البيئة عن طريق تطوير إطار عملٍ قانونيٍّ يتناول السياسات ويكون مُنَظِّماً لاستخبارات الإشارات التجارية؛ كما تملك الحكومة فرصةً للنظر بإحداث تغييراتٍ في استراتيجيتها الاستثمارية؛ وتطوير قوى عاملةٍ تستخدم هذه القدرات بشكلٍ مناسب.

في منظورنا يوفر استخدام الاستخبارات الجغرافية المكانية (geospatial intelligence [GEOINT]) للأغراض التجارية دراسة حالةٍ توضيحيةٍ لكيفية تطور قدرةٍ اتصفت تاريخياً بأنها حكومية، إلى مشروعٍ تجاريٍّ إلى حدٍّ كبير. لقد حوّل استخدام الاستخبارات الجغرافية المكانية للأغراض التجارية كيفية جمع الحكومات للصور المُلتقَطة بواسطة الأقمار الاصطناعية وتحليلها.[2] لقد أثّر على كمية القدرات التي تبنيها وتشغّلها الحكومة الأمريكية وأنواعها في ما يتعلق بالتقاط الصور في الجو الرأسيّ.[3] أدى هذا الأمر إلى وفوراتٍ في التكلفة عندما يمكن استخدام أنظمةٍ بديعةٍ تتفرد بها الحكومة بشكلٍ أكثر فعاليةً بأن توكل الوظائف التي لا تستلزم القدرة الكاملة التي لدى الأنظمة الحكومية، إلى الأنظمة التجارية ذات القدرة الأدنى. وبينما تُعَدّ التطورات في استخبارات الإشارات التي لا تملكها الحكومة محدودة النطاق، إلا إنها قد تُمَكّن من تغييراتٍ مماثلة.

إضفاء الطابع الديموقراطيّ أم الاستخدام للأغراض التجارية؟

لقد استهللنا هذا الجهد بنيّة دراسة استخدام استخبارات الإشارات (SIGINT) للأغراض التجارية، لكننا وجدنا بسرعةٍ أن **الاستخدام للأغراض التجارية** لم يكن مصطلحاً مناسباً لوصف التغييرات التي نجدها في قطاع التكنولوجيا. سوف يؤدي اقتصار بحثنا على القدرات التي يكون لها سوقٌ تجارية، إلى استبعاد القدرات التي ما زالت غير قانونيةٍ في الولايات المتحدة، ولكنها مع ذلك متوفرةٌ لكل مَن هو مستعدٌ لدفع ثمنها. من الصحيح أنّ السوق التجارية لاستخبارات الإشارات تستحق الدراسة — وإننا نقوم بذلك — إلا إنه من غير الكافي أن نُجريَ توصيفاً لكامل التغييرات في التكنولوجيات المتصلة باستخبارات الإشارات والتي هي الآن متوفرةٌ لكل مَن هو راغبٌ ومستعدٌ لأن يدفع ثمنها. وعلى امتداد هذا التقرير، نناقش ما إذا كانت كل قدرةٍ على حدة، قانونيةً أم غير قانونية، وكيف لهذا التمييز أن يؤثّر على الحكومة الأمريكية.

يصف مصطلح **إضفاء الطابع الديموقراطيّ** الحالة التي يكون فيها الشيء متوفراً لكل مَن يرغب به. لقد وجدنا أنّ إضفاء الطابع الديموقراطيّ يناسب بيئة استخبارات الإشارات بشكلٍ أكبر، ويبيّن الشكل رقم 1 التمييز بين القدرات التي تتفرد بها الحكومة، والاستخدام للأغراض التجارية، وإضفاء الطابع الديموقراطيّ.

لقد اكتشفنا، عبر التكنولوجيات التي تم فحصها، أنّ القدرات غير الحكومية في الفضاء الخارجيّ — حتى الوقت الحاضر — تجاريةٌ على الدوام. وفي هذه الأثناء، فإن القدرات التي لا تتعلق بمجال الفضاء، مثل أنظمة الفضاء الإلكترونيّ والأنظمة الأرضية، قد تكون تجاريةً أو غير مشروعةٍ أو مُصَمَّمَةً للهواة (do-it-yourself [DIY]). تشمل القدرات المُصمّمَة للهواة أجهزةً يمكن بناؤها بحدٍّ أدنى من الخبرة التقنية وباستخدام مكوّناتٍ منخفضة التكلفة.

قدرات استخبارات الإشارات (SIGINT) التي أُضفِيَ عليها الطابع الديموقراطيّ

لقد اعتمدنا المعلومات المتاحة للعامة وذات المصدر المفتوح من أجل بحثنا، ويصف هذا القسم أنواع القدرات التي اكتشفناها. لم نهدف إلى التعريف بكل التكنولوجيات المتوفرة؛ قد توجد تكنولوجياتٌ إضافيةٌ في برامج الأبحاث والتطوير التي لم تصبح عامةً بعد، وقد تكون هناك بعض التكنولوجيات

الشكل رقم 1. التعريفات

قدرةٌ تتصف بالتفرد الحكوميّ	الحكومة (الحكومات) هي التي تبني القدرة وتشغلها، أو أنّ القدرة تبنيها وتُشَغّلها جهةٌ مزودةٌ تجارية، ولكنْ يمكن الوصول إليها من قِبَل الحكومة (الحكومات) فقط
قدرةٌ يمكن استخدامها للأغراض التجارية	القدرة متوفرةٌ للشراء في الأسواق القانونية
قدرةٌ أُضفِيَ عليها الطابع الديموقراطيّ	القدرة متوفرة، بشكلٍ قانونيٍّ أو غير قانونيّ، للشراء أو مجاناً لمَن يرغب بها، ويشمل ذلك توفرها على هيئة ما هو مُصَمّمٌ للهواة (DIY)

المتوفرة مما لم يتمكن بحثنا من العثور عليه. بعض القدرات التي اكتشفناها أنشئت في بلدانٍ أجنبية، وهي تشمل قدراتٍ ما زالت قيد التطوير في روسيا وإسرائيل. في هذا القسم، نناقش أولاً القدرات التجارية المفهومة بشكلٍ جيّدٍ والمُعتَمَدَة على نطاقٍ واسع، ويلي ذلك القدرات الناشئة (وتشمل ما هو متوفرٌ في الأسواق الرمادية [الموازية] أو المشكوك في قانونيتها)، وننتهي بالقدرات غير المشروعة الموجودة خارج الأسواق القانونية.

بعض مجالات التكنولوجيا التي عرّفنا بها ليست جديدة، ولكننا وجدنا أنها أكثر تطوراً بشكلٍ ملحوظٍ من القدرات التي توفرت سابقاً للمستهلكين غير الحكوميين. مثلاً، بينما يُجرى بشكلٍ روتينيّ، مَسحٌ محيطيٌّ لطيف الترددات الراديوية (RF spectrum mapping) بهدف تحليل تغطية الهواتف الخلوية، وبينما قد توفرت التكنولوجيا الأساسية للهواة المُزَوَّدين بالهوائيات المحمولة وأجهزة تحليل الطيف، فإنها لم تتوفر تجارياً في ما يتعلق بالأقمار الاصطناعية التي توفر تغطيةً عالمية. ذلك الوضع على وشك أن يتغير.

يميز الممارسون، ضمن مجتمع استخبارات الإشارات (SIGINT) بين المكونات الخارجية للإشارات (signal externals) والمكونات الداخلية للإشارات (signal internals). توفر **المكونات الخارجية للإشارات** معلوماتٍ من نوع قوة، وتردد، وتعديل الإشارة، ويمكن استخدامها لتحليل التدفقات المرورية، والأنماط المرورية، والنشاط الشبكيّ. إنّ معلوماتٍ كهذه يمكن على سبيل المثال استخدامها لتحسين إدارة الشبكة. في المقابل، تكشف **المكونات الداخلية للإشارات** عن المحتوى المُرسَل الذي يتم نقله، وقد تستلزم فكاً للتشفير أو ترجمةً للغة. لقد وجدنا أنّ كِلا النوعَين من القدرات متوفرٌ وأنّ العملاء المختلفين يطلبون أنواعاً مختلفةً من استخبارات الإشارات.

التوعية بأحوال المجال البحريّ

التوعية بأحوال المجال البحريّ هي الأكثر نضجاً من بين التطبيقات التجارية لاستخبارات الإشارات (SIGINT) التي عثرنا عليها. إنّ **التوعية بأحوال المجال البحريّ** هي الفهم الفعال لأيٍّ من السفن أو الأجسام في المجال البحريّ التي من شأنها التأثير على الأمن، أو السلامة، أو الاقتصاد، أو البيئة.[4] في أوائل التسعينات، تم تطوير نظام تحديد الهوية الآليّ (Automatic Identification System [AIS]) ليكون نظام تتبّعٍ آليٍّ محمولٍ بواسطة السفن، يساعد

تعد مجالات التكنولوجيا التي عَرَّفنا بها أكثر تطوراً بشكلٍ ملحوظٍ من القدرات التي توفرت سابقاً للمستهلكين غير الحكوميين.

على تفادي حدوث الاصطدام في المناطق الساحلية التي تكثف فيها حركة الملاحة. فرضت المنظمة البحرية الدولية (International Maritime Organization) منذ عام 2002 استخدام نظام تحديد الهوية الآليّ على سفنٍ مختارة، ووسعت عدد السفن التي تتطلب هذا النظام مع الوقت. حالياً، أصبح نظام تحديد الهوية الآليّ إلزامياً على متن كل السفن الدولية التي تَزِن أكثر من 300 طن، وعلى كل سفن الركاب. في الأصل، كانت المحطات الأرضية الواقعة على طول الشواطئ تتلقى إرسالات نظام تحديد الهوية الآليّ التي تبثها السفن. إنّ البدء باستخدام النمط التجاريّ من الكشف بواسطة نظام تحديد الهوية الآليّ عن طريق الأقمار الاصطناعية وسّع التغطية لتشمل أعالي المحيطات.

في عام 2005، بدأ عددٌ من الكيانات الحكومية والتجارية بتجريب استخدام أجهزة استقبال بث الأقمار الاصطناعية من أجل كشف الإرسالات التي يبثها نظام تحديد الهوية الآليّ. ومنذ عام 2008، نشرت عدة شركاتٍ تجاريةٍ مثل إكزاكت إرث (exactEarth)، وأوربكوم (ORBCOMM)، وسباير (Spire)، كوكباتٍ من الأقمار الاصطناعية مزودةً بأجهزة استقبال بث أنظمة تحديد الهوية الآليّة. توفر هذه الشركات منتَجاتِ التوعية بأحوال المجال البحريّ التي تستند إلى بيانات الأقمار الاصطناعية المزودة بأجهزة استقبال بث أنظمة تحديد الهوية الآلية لديها (satellite AIS)، والتي ترافقها في كثيرٍ من الأحيان مصادرُ أخرى للبيانات. إنها توفر أيضاً بيانات تغذيةٍ صادرةٍ عن الأقمار الاصطناعية المزودة بأجهزة استقبال بث أنظمة تحديد الهوية الآلية للمُستخدِمين والموزِّعين الذين قد يمزجون بيانات أنظمة تحديد الهوية الآلية مع مصادرَ أخرى لتوليد منتجاتهم الخاصة.

هذه التطورات مهمةٌ لعددٍ من الأسباب. لقد صُمِّمَت الأقمار الاصطناعية المزودة بأجهزة استقبال بث أنظمة تحديد الهوية الآلية في الأصل من أجل تتبّع السفن المُمتَثِلَة في المياه المزدحمة، ولكنها تسمح الآن بإمكانية دمج

بيانات نظام تحديد الهوية الآليّ مع الصور المُلتَقَطَة بواسطة التصوير البصريّ ونظام الكشف وتحديد المدى الراديويّ (الرادار) ومصادر أخرى للبيانات. يمكن للبيانات المُدمَجَة، لاسيما إذا كانت هذه البيانات تستخدم أدواتٍ عالية الدقة لتحديد الموقع الجغرافيّ، أن تدمج معلوماتٍ من أجهزة استشعارٍ مختلفةٍ وجهاتٍ مزوِّدَةٍ مختلفةٍ من أجل تتبّع السفن المُمتَثِلة والسفن "المظلمة" — وهي السفن التي تختار ألا تبث إشارات نظام تحديد الهوية الآليّ لديها، أو تلك التي تبث إشارةً مزيفة (منحولة) من نظام تحديد الهوية الآليّ لديها. عندما تُضَمُّ معلوماتٌ استخباراتيةٌ أخرى مستمَدةٌ من مصادرَ مفتوحة (open source intelligence [OSINT])، يمكن الكشف عن رؤى إضافية. إن العديد من الأقمار الاصطناعية التجارية الحالية أو المُخَطَّط لها، والمُعَدَّة لالتقاط الصور تشتمل على حمولةٍ من نظام تحديد الهوية الآليّ، وإنّ كوكبةً واحدةً على الأقل من الأقمار الاصطناعية المُعَدَّة للاتصالات والتي تتحرك في مدارٍ منخفضٍ حول الأرض (low Earth orbit [LEO]) سوف يكون فيها حمولةٌ من نظام تحديد الهوية الآليّ.

تستخدم شركةٌ إسرائيليةٌ هي ويندوورد (Windward ["في اتجاه الريح"]) هذا التحليل المُدمَج المتعدد المصادر. توفر ويندوورد استخباراتٍ بحريةً للعملاء عن طريق دمج معلومات أنظمة تحديد الهوية الآلية مع الصور وغيرها من مصادر البيانات الحالية والتاريخية، وتطبيق خوارزميات الذكاء الاصطناعيّ من أجل تحديد أنماط الحياة وتوفير الإنذارات بشأن الأنماط السلوكية الشاذة.[5] تُستَخدَم هذه التحليلات في التوعية بأحوال المجال البحريّ ومن أجل استخدامٍ أكثر فعاليةً لمنصات المراقبة الأخرى ومنصات الاعتراض. تطور ويندوورد كذلك تطبيقاتٍ للاستخدام في الأسواق المالية.[6]

المسح المحيطيّ لطيف الترددات الراديوية (RF Spectrum Mapping)

ولقد وجدنا أمثلةً تجاريةً على رصد إشارات الترددات الراديوية (RF signal monitoring) خارج مجال التوعية بأحوال المجال البحريّ. ففي عام 2013، أطلقت غوغل (Google) قاعدة البيانات المسماة سبكتروم داتابيس (Spectrum Database) مجاناً للعالم، مما يسمح لأيٍّ شخص أن يدّعيَ حقاً في الطيف غير المُستَخدَم من الترددات الراديوية (الذي يُسمى أيضاً بالفضاء الأبيض). يسمح هذا العرض المجانيّ لمُستخدِمٍ ما بتحديد ما إذا كان الطيف المُستَخدَم في منطقةٍ جغرافيةٍ معيّنةٍ مُسَجَّلاً في قاعدة البيانات (ويكون بالتالي قد سُمِحَ به بواسطة أحد تنظيمات حكومة الولايات المتحدة)[7] أو غير مسجَّل (مما يمكن أن يشير إلى وجود استخدامٍ خفيّ). هذه القدرة مفيدةٌ داخل الولايات المتحدة فقط. بالنسبة للمسح المحيطيّ لطيف الترددات الراديوية الذي يستطيع الوصول إلى أماكن أبعد، تستدعي الحاجة قدراتٍ فضائية.

أُنشِئت شركةٌ أمريكيةٌ اسمها هوك آي 360 (HawkEye360 ["عين الصقر 360"]) (أو HE360) عام 2015 لمحاولة إطلاق "أول كوكبةٍ من الأقمار الاصطناعية الصغيرة في العالم، المُمَوَّلَة عن طريق القطاع الخاص، والتي ستُدفَعُ للتحليق في تشكيلٍ سوف يكون قادراً على جمع البيانات وتوليد التقارير حول الإشارات اللاسلكية التي تم تحديد موقعها الجغرافيّ".[8] تخطط هوك آي 360 لنشر كوكبةٍ تجريبيةٍ مؤلفةٍ من ثلاثة أقمارٍ اصطناعيةٍ لأغراض تطبيقات استخبارات الإشارات (SIGINT) في أواخر عام 2017. سوف تتلقى أقمار هوك آي 360 الاصطناعية إشارات نظام تحديد الهوية الآليّ (AIS)، وتزعم هوك آي 360 أيضاً أنّ كوكبتها "سوف تجمع معلوماتٍ تتعلق بإشاراتٍ راديويةٍ محددةٍ حول العالم من أجل توفير مسحٍ محيطيٍّ عالي الدقة لطيف الترددات الراديوية، وتوفير تحليلاتٍ يمكننا موائمتها لتناسب حاجات عملائنا".[9] بحسب ما جاءت به شركة هوك آي 360، فإنّ الإشارات التي تخطط لجمعها وتحليلها ليست متوفرةً حالياً في القطاع التجاريّ. إنْ كانت ناجحةً في الجمع، والمسح المحيطيّ، والتحليل التنبؤيّ، فإنّ شركة هوك آي 360 سوف توفر عرضاً استخباراتياً غير مسبوقٍ للعملاء من القطاع التجاريّ والعملاء المتمثلين بالحكومات الأجنبية على حدٍّ سواء.[10]

القدرة التجارية المعروضة لرصد إشارات التردد الراديوي مهمةٌ لأسبابٍ عدة. فمن شأنها السماح للجهات الفاعلة التجارية بكشف الإشارات وتبيين خصائصها وتحديد موقعها الجغرافيّ، مما يدعم التطبيقات المُعَدَّة للتعرف إلى أنماط النقل في ممرات الملاحة التي تشهد ازدحاماً مرورياً، أو عن طريق إنشاء خرائطَ لمناطق التداخل الطيفيّ.[11] يمكن أيضاً استخدام تحديد الموقع الجغرافيّ بواسطة باعث الإشارات من أجل تحديد موقع مصادر التداخل، ويشمل ذلك المشوِّشين المُتَعَمِّدين.

لقد كان التنصت عن طريق الأقمار الاصطناعية في السابق مجال الحكومات وبعض الهواة من المتخصصين، لكننا وجدنا أمثلةً عامةً عديدةً لأدواتٍ إما متوفرةٌ تجارياً أو يمكن الوصول إليها من قِبَل المُستخدِمين، بحيث يتمكنون من بنائها بأنفسهم بأقل قدرٍ من التكلفة والخبرة التقنية.

يملك المسح المحيطيّ لطيف الترددات الراديوية تطبيقات أمانٍ إضافية. تملك وكالة مشاريع الأبحاث الدفاعية المتطورة (The Defense Advanced Research Projects Agency)، التي تُعَرَّف بالاختصار (DARPA) برنامجاً هو راديوماب (RadioMap)، مهمته توفير التوعية بأحوال استخدام الطيف في الزمن الحقيقيّ في منطقةٍ محليةٍ ما.[12] تصف وكالة مشاريع الأبحاث الدفاعية المتطورة تطبيقاتٍ للمسح المحيطيّ للترددات الراديوية تشمل خرائطَ للاستخدام في الزمن الحقيقيّ من أجل الوصول النشط إلى الطيف، والتوعية بالأوضاع السائدة بالنسبة للوحدات التكتيكية الصغيرة، ودعم أنظمة الحرب الإلكترونية. سوف يوسّع المسح المحيطيّ للترددات الراديوية الذي يستعين بالأقمار الاصطناعية، من النوع الذي تخطط له شركة هوك آي 360 التغطية من المحلية إلى العالمية.

التنصت، والتشويش، والاستيلاء على أنظمة الأقمار الاصطناعية

لقد صُممت الأقمار الاصطناعية في الأساس دون اعتبارٍ جديٍّ للآليات الدفاعية. إنّ العديد من الأنظمة الموروثة أو الأنظمة التجارية الجديدة عُرضَةٌ للضعف أمام نوعٍ واسعٍ من التداخل الذي يطال الإشارات، إما لأنّ الدفاعات لم تكن متوفرةً في زمان الإطلاق، أو لأنه تم النظر إلى ارتفاع التكاليف استناداً إلى التهديد المُتَصَوَّر. لقد استغلت الحكومات والجهات الفاعلة غير الحكومية هيكلية اتصالات أنظمة الأقمار الاصطناعية لسنوات. وجد بحثنا أنّ القدرات التجارية تنتشر بسرعةٍ بحيث تستغل إشارات الأقمار الاصطناعية.

إنّ الشكل الأقل تهديداً والأكثر انتشاراً من أشكال استغلال الإشارات هو التنصت، الذي يوفر أيضاً القدرة الوحيدة التي تُعَدّ بوضوحٍ من ضمن استخبارات الإشارات (SIGINT)، أكثر من كونها من قدرات الحرب الإلكترونية.

يسمح التنصت لمُستخدِمٍ ما بالوصول إلى بياناتٍ مُرسَلَةٍ بواسطة الأقمار الاصطناعية أو غيرها من الوسائل. لقد كان التنصت عن طريق الأقمار الاصطناعية في السابق مجال الحكومات وبعض الهواة من المتخصصين، لكننا وجدنا أمثلةً عامةً عديدةً لأدواتٍ متوفرةٌ تجارياً أو يمكن الوصول إليها من قِبَل المُستخدِمين، بحيث يتمكنون من بنائها بأنفسهم بحدٍّ أدنى من التكلفة والخبرة التقنية.

أحد الأمثلة على التنصت عن طريق الأقمار الاصطناعية كان استخدام البرنامج الروسيّ المسمى سكاي غرابر (SkyGrabber "[القابض على السماء]")، الذي كانت كلفته 26 دولار أمريكيّ، من قِبَل المخربين (القراصنة) الإلكترونيين في العراق من أجل التقاط تغذيات الفيديو في الطائرة بدون طيارٍ المسماة بريداتور (Predator drone) (Predator "الحيوان المفترس") التي يستخدمها الجيش الأمريكيّ عام 2009. تَنَصَّتَ المتمردون على التغذية غير المشفرة للفيديو التي سُحِبَت من طائرات بريداتور بدون طيار عبر الأقمار الاصطناعية التجارية المُعِدَّة للاتصالات.[13] المفاجئ أنّ نقاط ضعفٍ في التشفير كهذه ما تزال موجودةً بالنسبة لبعض أنظمة الأقمار الاصطناعية التجارية. تعالج الحكومة هذا القصور عن طريق إلزام إجراء التشفير في الاتصالات العسكرية التي تعتمد على الأنظمة التجارية، لكنّ ما سوى ذلك من حركة مرورٍ غير حكوميةٍ عبر تلك الأنظمة قد يظل عُرضةً للضعف.

يعد التنصت شكلاً سلبياً من استغلال الإشارات، لكنّ أشكالاً أخرى أكثر نشاطاً من التداخل تؤثر أيضاً على الجهات المزوِّدة التجارية. لقد أصبح التشويش السبب الأوليّ لإضعاف خدمات الأقمار الاصطناعية والحط منها. يحدث **التشويش** عندما يُغرِقُ المهاجم أو يتغلب على إشارة، أو جهاز إرسال، أو جهاز استقبال، عن طريق التداخل مع الإرسالات الشرعية.[14] قد يكون هدف المُشوِّش القمر الاصطناعيّ، أو محطةً أرضية، أو طبقاً أرضياً

لاستقبال بث الأقمار الاصطناعية. لقد كانت الأقمار الاصطناعية التجارية ضحيةً للتشويش المُتَعَمَّد لأكثر من ثلاثة عقود. في أحد الأمثلة الأقدم، عام 1986، استخدم رجلٌ أجهزةً متوفرةً تجارياً لاعتراض، وتشويش، واستبدال بث القمر الاصطناعي التابع لهوم بوكس أوفيس (Home Box Office [HBO]) برسالته الخاصة.[15]

خلال القسم الأكبر من الأعوام الثلاثين الماضية، تفادت الجهات المزوِّدة التجارية تعديل أقمارها الاصطناعية بحيث تتعامل مع التشويش المُتَعَمَّد (في مقابل التداخل غير المُتَعَمَّد)، بحجة التكاليف المرتفعة، أو لأنها كانت تأمل ببساطةٍ أن تتراجع حوادث التشويش. لكنّ التشويش في الواقع أصبح الآن يحدث بوتيرةٍ أعلى، لاسيما في منطقة الشرق الأوسط على أثر الربيع العربيّ (Arab Spring)، والاضطرابات السياسيّة في إيران. اليوم، تقول شركتان هما عربسات (Arabsat) ونايلسات (Nilesat) أنّ التداخل المرتبط بالربيع العربيّ وصل إلى نقطةٍ أصبح يؤثّر فيها مادياً على إيراداتهما. وقد أعلن مُشَغِّل أسطول الأقمار الاصطناعية التجارية يوتِلسات (Eutelsat) عام 2013 أنه بدأ بوضع قدرةٍ تجريبيةٍ لمكافحة التشويش في أحد أقماره الاصطناعية القادمة التي يُعتَزَم إطلاقها لتستقر فوق منطقة الشرق الأوسط، وهو قرارٌ دفع إليه التداخل المُتَعَمَّد المتزايد في المنطقة.[16]

يتمثل أكثر أشكال التخريب (القرصنة) الإلكتروني إثارةً للقلق الذي يتعلق بالأقمار الاصطناعية في الاستيلاء على رابط القياس عن بُعد والتتبُّع والقيادة (TT&C) في محاولةٍ للسيطرة على القمر الاصطناعيّ نفسه. في عام 2009، اكتُشِفَت ثغراتٌ أمنيةٌ في تكنولوجيات الاتصالات بواسطة الأقمار الاصطناعية، كانت قد سمحت للمخربين (القراصنة) الإلكترونيين بإغلاق أنظمة القيادة والتحكم، ومكنتهم من سرقة البيانات. يُعتَقَدُ أنّ هذه الثغرات كان قد بدأ استغلالها منذ أوائل عام 2007 من قِبَل مخربين (قراصنة) إلكترونيين من الروس ربما كانت ترعاهم الحكومة.[17]

في عام 2015، أثبت باحثٌ في شؤون الأمن أنه، بمبلغٍ قدره 1,000 دولار أمريكيّ، يمكن لأحدٍ ما أن يبنيَ جهازاً لإرسال بياناتٍ منحولةٍ للقمر الاصطناعيّ غلوبال ستار (GlobalStar). يُستَخدَم نظام غلوبال ستار "لرصد البنية التحتية الصناعية المهمة مثل خطوط الأنابيب، أو لتتبع المتنزهين سيراً على الأقدام وغيرهم من المغامرين الذين يستخدمون جهاز التتبع المتاح للمستهلِكين الذي يوفره غلوبال ستار."[18] قال الباحث أنه يستطيع، باستخدام جهازه، رصد أيّ جسمٍ يجري تتبُّعُه على شبكة غلوبال ستار "لعدة أميال" في محيط موقعه.[19]

إنّ إضفاء الطابع الديموقراطيّ على استخبارات الإشارات (SIGINT) ظاهرٌ بوضوحٍ على امتداد جميع مجالات أنظمة الأقمار الاصطناعية — التنصت، والتخريب (القرصنة) الإلكترونيّ، والتشويش.

مراقبة الفضاء الإلكترونيّ

لقد كانت مراقبة الفضاء الإلكترونيّ موضوعاً للدراسة الموسعة. استكشف العديد من زملائنا في مؤسسة RAND ما سَمَّوه "الأسواق السوداء والرمادية (الموازية) لأدوات التخريب (القرصنة) الإلكترونيّ [و] خدمات التخريب (القرصنة) الإلكترونيّ" في تقريرهم عام 2014، وعنوانه "أسواقٌ لأدوات جرائم الفضاء الإلكترونيّ والبيانات المسروقة: بازار المخربين (القراصنة) الإلكترونيين"[20] (*Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*). كتبوا:

> إنّ سوق المخربين (القراصنة) الإلكترونيين — التي كانت يوماً مشهداً متنوعاً لشبكاتٍ ظرفيةٍ متكتمةٍ من الأفراد الذين لم يكن يدفعهم في الأساس إلا ما هو أكثر بقليلٍ من الغرور وحب الشهرة — برزت لتصبح ملعباً لمجموعاتٍ لها دوافعُ مالية، وهي عالية التنظيم، ومتطورة. من بعض الجهات، يمكن للسوق السوداء أن تكون مُربِحَةً أكثر من الاتجار غير القانونيّ بالمخدرات؛ الروابط المؤدية إلى المُستخدِمين النهائيين مباشِرةٌ بشكلٍ أكبر، ولأنّ التوزيع حول العالم يتم بالواسطة الإلكترونية، تكون المستلزمات مما لا يُعتَدّ به.[21]

اليوم، يتم تسويق أدوات التخريب (القرصنة) الإلكترونيّ بين المستهلكين بشكلٍ مفتوح، مما يطرح مشاكلَ مرهِقةً أمام الاستخبارات ووكالات إنفاذ القانون. في وقتٍ سابقٍ من هذا العام، نقلت مجلة **بلومبرغ بزنس ويك** (*Bloomberg Businessweek*) أنه بعد تسريبات إدوارد سنودن (Edward Snowden)، "أصبح كل بلدٍ تقريباً على وجه الأرض راغباً في تطوير وكالة أمنٍ قوميٍّ (NSA) مصغرةٍ خاصةٍ به."[22] هناك شركةٌ اسمها هاكينغ تيم (Hacking Team "فريق التخريب [القرصنة] الإلكترونيّ") تقدم تراخيصَ سنويةً قيمتها 200,000 دولار أمريكيّ لنظامٍ لديها اسمه نظام السيطرة عن بُعد (Remote Control System [RCS])، وهو عبارةٌ عن أداةٍ "يمكنها التنصت على كل شيء [على حاسوب هدفٍ ما أو هاتفه] بشكلٍ لا يمكن ملاحظته". بحسب ما أفادت بعض التقارير، كان من بين عملائهم وكالاتٌ حكوميةٌ أمريكية، ووكالة الاستخبارات الروسية (FSB)، وحكومات البحرَين، ومصر، وأثيوبيا، والمغرب، وتركيا، والمملكة العربية السعودية.[23]

زعم بعض المخربين (القراصنة) الإلكترونيين أنهم وجدوا نقاط ضعف، تسمى **ثغرات**، يمكنها السيطرة على أيّ هاتفٍ بدون عِلم المُستَخدِم، أو بدون أن يكون المُستَخدِم مضطراً للنقر على أيّ رابط. هذه الثغرات، التي تُباع أحياناً لقاء ما يزيد على مليون دولار أمريكيّ لكلٍّ منها، تزعم أنها قادرةٌ على التسلل إلى العملية الصامتة التي تجري بواسطة خدمة الرسائل القصيرة (SMS) التي كانت الهواتف المحمولة تستخدمها لتحميل التحديثات وأداء المهمات الإدارية في الخلفية من غير عِلم المُستخدِمين.[24]

الأفراد والمجموعات من الذين يملكون مالاً أقل للإنفاق مُرَحَّبٌ بهم أيضاً في السوق التجارية للمراقبة الإلكترونية. تُبيِّن وثائقُ مسروقةٌ من شركتَين للبرمجيات التجسسية، هما فليكسي سباي (FlexiSpy)، وريتينا–أكس (Retina–X)، أنّ عشرات الآلاف من العملاء، "أناسٌ عاديون — محامون، ومدرسون، وعمال بناء، وأهالي، وعشاقٌ غيارى — قد اشترَوا برمجياتٍ خبيثةً من أجل رصد هواتفَ محمولةٍ أو حواسيب" و"ربما يكونون قد دفعوا ما يتراوح بين 50 دولار أمريكيّ و200 دولار أمريكيّ فحسب، لقاء اشتراكٍ شهريٍّ أو سنويٍّ في البرمجيات التجسسية."[25] بعبارةٍ أخرى يستطيع أيّ شخص، بتكلفةٍ متدنية، أن يرصد اتصالات شخصٍ آخر دون مسوغ قانوني أو سلطةٍ قانونيةٍ لفِعلِ ذلك.

إن القدرات التي كانت يوماً متوفرةً حصراً للدول القومية الخصمة الندة أصبحت الآن متوفرةً لأيّ خصمٍ يرغب في استخدامها.

تبيّن التطورات الأخيرة أنّ العوائق التقنية أمام إجراء مراقبةٍ أوسع نطاقاً للفضاء الإلكترونيّ، والتي تسمى **الجمع بالجملة**، قد تكون في انخفاض. في عام 2016، قام باحثٌ اسمه نيكولاس ويفر (Nicholas Weaver) في المعهد الدوليّ لعِلم الحواسيب التابع لجامعة كاليفورنيا–بيركلي (International Computer Science Institute at the University of California–Berkeley)، بتصميم وبناء نظام مُصَغَّرٍ لمراقبة الفضاء الإلكترونيّ بتكلفةٍ تَقِلّ عن 900 دولار أمريكيّ خلال أسبوعٍ واحد. اتّسم نظام ويفر بقدراتٍ تشمل جمع البيانات بالجملة، وقابلية إجراء وظائف البحث، وتتبع ملفات تعريف الارتباط، والتعرف إلى المُستَخدِمين المجهولي الهوية، والقدرة على حقن برمجياتٍ خبيثةٍ في حواسيبَ مُستَهدَفة. بحسب ما قاله ويفر، فإنّ التكنولوجيات المُستَخدَمة لبناء أنظمة المراقبة "عاديةٌ جداً وأساسيةٌ جداً، إنها من التكنولوجيا المفهومة بشكلٍ جيّدٍ جداً". قال، "علينا أن نتصرف على أساس أنّ كل شبكةٍ لاسلكيةٍ مفتوحةٍ أو فندقٍ في منطقة واشنطن (العاصمة) يُحتَمَل أن تكون مُخترَقَة. ونظراً للتكلفة المتدنية لتجهيزٍ كهذا، فلا حاجة في الأصل لأن يبقى في مجال خدمات الاستخبارات الخارجية."[26]

يوفر قطاع استخبارات الإشارات (SIGINT) المتعلق بالفضاء الإلكترونيّ للعملاء قدراتٍ صلبةً بأسعارٍ متنوعةٍ أو تكنولوجياتٍ مُصمَّمَةٍ للهواة (DIY technologies)، وحتى الآن، يظهر أنّ البائعين وعملاءهم غير متهيّبين من أن يكون استخدام هذه الحلول ضد أهدافٍ غافلةٍ عن هذا الأمر، في الولايات المتحدة، ما زال غير قانونيّ.

التداعيات بالنسبة للحكومة الأمريكية

إنّ إضفاء الطابع الديموقراطيّ على استخبارات الإشارات (SIGINT) له

تداعياتٌ بالنسبة للحكومة الأمريكية. لم نجد أمثلةً لأنظمةٍ يمكن لها أن تحل محل القدرات الحكومية القائمة، لكنّ الأنظمة الحالية غير الحكومية بوسعها توفير مصادرَ غير سريةٍ من أجل نَظم قائمةٍ بجامعي المعلومات ومحلليها، وتسهيل تبادل المعلومات مع الشركاء الأجانب. يمكن استخدام الأنظمة غير الحكومية مثلاً، من قِبَل وزارة الدفاع الأمريكية (U.S. Department of Defense)، ووزارة الأمن الداخليّ الأمريكية (U.S. Department of Homeland Security) من أجل تحسين التوعية بأحوال المجال البحريّ. بالإضافة إلى ذلك، يمكن استخدام القدرات التي وجدناها — وفي بعض الحالات، التي كانت قد استُخدِمَت من قبل بالفعل — ضد الحكومة الأمريكية والحلفاء.

تشمل البيئة العملياتية اليوم عدداً أكبر من الجهات الفاعلة على امتداد السوق، مِمَّن يملكون القدرة على الوصول إلى قدراتٍ أكثر تقدماً في استخبارات الإشارات مما كان متوفراً في السوق من قبل. إن القدرات التي كانت يوماً متوفرةً حصراً للدول القومية الخصمة الندة أصبحت الآن متوفرةً لأيّ خصمٍ يرغب في استخدامها. هذا الأمر يزيد من المخاطر بالنسبة للأنظمة الحكومية، كما إنه يثير مخاوفَ جدّيةً بالنسبة للخصوصية. ينبغي على الحكومة أن تنظر في كيفية احتمال استغلال أدوات استخبارات الإشارات غير الحكومية من قِبَل الخصوم، وما هي المخاطر بالنسبة لأمن العمليات لدى الحكومة (operational security [OPSEC])، والخصوصية الفردية، وما هي التدابير التي يتعين على الحكومة والحلفاء اتخاذها من أجل التخفيف من هذه المخاطر.

تميّز الحكومة الأمريكية بين قدرات الجمع السلبية وأجهزة الإرسال النشطة، لأنّ الوكالات والمكونات العسكرية المختلفة تملك سلطاتٍ محددةً بالنسبة لمجموعةٍ واحدةٍ من المهمات أو لأخرى. خارج الحكومة، وجدنا أنّ هذه الفروق تُهِمُّ المُستخدِمين بدرجةٍ أقل، فهم يركزون بدلاً من ذلك على النتيجة التي يرغبون في تحقيقها. بالتالي، يشمل بحثنا قدراتٍ قد تعتبرها الحكومة حرباً إلكترونيةً أو عملياتٍ في الفضاء الإلكترونيّ، لا استخبارات إشارات.

إننا نُعرف عدة مجالاتٍ تدعو الحاجة فيها لبحثٍ ونقاشٍ إضافيَّين من أجل إنشاء حلولٍ قانونية، وتنظيمية، وحلولٍ في السياسات والعمليات ورأس المال البشري، لتحديات قدرات استخبارات الإشارات التي أُضفِيَ عليها الطابع الديموقراطيّ. إنّ مجالاتٍ كهذه تُنتِج الأسئلة البحثية التالية:

- كيف سيتم تطبيق عمليات حظر رصد الأشخاص الأمريكيين عند استخدام أنظمة استخبارات الإشارات (SIGINT)، والبيانات التي لا تسيطر عليها الحكومة؟
- ما هي القيود التي سوف تُطَبَّق على أنواع المعلومات المُتَبادلَة مع الحكومات الأجنبية، وشركات الأعمال، والمنظمات غير الحكومية وجودة هذه المعلومات؟
- كيف يمكن للقدرات الناشئة التجارية والتي أُضفِيَ عليها الطابع الديموقراطيّ أن تتدخل في العمليات العسكرية، والاستخباراتية، وعمليات إنفاذ القانون، وما هي المقاربات التخفيفية التي يجب تنفيذها؟
- ما هي المعايير التي ينبغي على الحكومة استخدامها، من خلال سلطات وزارة التجارة الأمريكية (U.S. Department of Commerce)، لتنظيم أيّ قدرات استخبارات الإشارات (SIGINT) تحصل على تراخيص إطلاقٍ فضائيّ وأيها لا تحصل عليها؟ هل ينبغي على الحكومة أن تنظّم بشكلٍ مشابهٍ قدرات استخبارات الإشارات غير الفضائية، وإن كان كذلك، فكيف يتم الأمر؟
- ما هي الآليات الدفاعية (ويشمل ذلك السياسات والإجراءات) التي ينبغي على مجموعة الاستخبارات (Intelligence Community) تنفيذها من أجل حماية ضباط الاستخبارات من استخدام الخصوم لهذه القدرات؟

إنّ إضفاء الطابع الديموقراطيّ على استخبارات الإشارات جارٍ بالفعل، لكنّ هذه التغييرات لم تُقَر أو تُفهَم على نطاقٍ واسعٍ من قِبَل الحكومة الأمريكية. إن تطوير استخباراتٍ جغرافيةٍ مكانية (geospatial intelligence [GEOINT]) تجاريةٍ يوضح أنّ المصادر التجارية يمكن لها أن تكمل القدرات الحكومية. بوسع استخبارات الإشارات التجارية أن تكمل استخبارات الإشارات الحكومية بشكلٍ مشابه، وإن كانت ستفعل ذلك بطرقٍ مختلفةٍ على الأرجح. إنّ تطوير قدراتٍ في استخبارات الإشارات خارج الحكومة يوفر، على حدٍّ سواء، مخاطرَ على الأمن الأمريكيّ وفرصاً للوكالات الأمريكية المستعدة للتحرك.

الملاحظات

[1] المنشور المشترك رقم 1-02، قاموس وزارة الدفاع للمصطلحات العسكرية والمرتبطة بها (Department of Defense Dictionary of Military and Associated Terms)، واشنطن العاصمة: وزارة الدفاع الأمريكية (U.S. Department of Defense)، 8 نوفمبر/تشرين الثاني، 2010 (بحسب التعديل الساري حتى 15 شباط/فبراير، 2016)، ص. 217.

[2] روبرت كارديلو (Robert Cardillo)، بيانٌ بغرض التدوين في المحضر أمام لجنة الاستخبارات المختارة في مجلس الشيوخ الأمريكيّ، (Statement for the Record Before the U.S. Senate Select Committee on Intelligence)، الوكالة الوطنية للاستخبارات الجغرافية المكانية (National Geospatial-Intelligence Agency)، 27 سبتمبر/أيلول، 2016. أطلع عليه بتاريخ 24 فبراير/شباط، 2017، https//:www.nga.mil/MediaRoom/SpeechesRemarks/Pages/Director-Cardillo-Senate-Select-Committee-on-Intelligence-open-hearing.aspx

[3] الوكالة الوطنية للاستخبارات الجغرافية المكانية (National Geospatial-Intelligence Agency)، "النشاط المشترك الذي نفذته الوكالة الوطنية للاستخبارات الجغرافية المكانية ومكتب الاستطلاع الوطنيّ معاً، من أجل دمج قدراتٍ تجاريةٍ جديدةٍ مُعَدَّةٍ لمجموعة الاستخبارات، في مجال الاستخبارات الجغرافية المكانية" (Joint NGO/NRO Activity to Integrate New Commercial Geospatial Intelligence Capabilities for the Intelligence Community)، بيانٌ صحفيّ، 15 يوليو/تموز، 2016. اطلع عليه بتاريخ 24 فبراير/شباط، 2017، https://www.nga.mil/MediaRoom/PressReleases/Pages/Joint-NGANRO-activity-to-integrate-new-commercial-geospatial-intelligence-capabilities-for-the-Intelligence-Community.aspx

[4] وزارة الأمن الداخليّ الأمريكية (U.S. Department of Homeland Security)، "الخطة الوطنية لتحقيق التوعية بأحوال المجال البحريّ" (National Plan to Achieve Maritime Domain Awareness)، واشنطن العاصمة، أكتوبر/تشرين الأول، 2005، ص. 2. اطلع عليه بتاريخ 6 أكتوبر/تشرين الأول، 2017، https://www.dhs.gov/sites/default/files/publications/HSPD_MDAPlan_0.pdf

[5] "التفوق لدى شركة ويندوورد" (The Windward Edge)، Windward.eu، غير مُؤَرَّخ. اطلع عليه بتاريخ 9 مارس/آذار، 2017، http://www.windward.eu/es/#/solutions/WindwardEdge؛ "ويندوورد تعتزم إطلاق حل مارينت للاستخبارات البحرية" (Windward to Launch Marint Maritime Intelligence Solution)، Ship-Technology.com، 21 مايو/أيار، 2015. اطلع عليه بتاريخ 22 مارس/آذار، 2017، http://www.ship-technology.com/news/newswindward-to-launch-marint-maritime-intelligence-solution-4582423

[6] كاثارين لوسون (Catharine Lawson)، "وايرد ماني: شركة ويندوورد تقدم التحليلات في الزمن الحقيقيّ إلى البيانات البحرية" (WIRED Money: Windward Brings Real Time Analytics to Maritime Data)، 6 يوليو/تموز، 2015. اطلع عليه بتاريخ 10 مايو/أيار، 2017، http://wired.co.uk/article/wired-money-windward

[7] كيفين فيتشارد (Kevin Fitchard)، "هل من أحدٍ يرغب بشيءٍ من الطيف غير المشغول (الفضاء الأبيض)؟ غوغل تفتح قاعدة بياناتها المسماة سبكتروم داتابيس أمام المطوِّرين" (White Spaces Anyone? Google Opens its Spectrum Database to Developers)، جيغاووم *(Gigaom)*، 14 نوفمبر/تشرين الثاني، 2013. اطلع عليه بتاريخ 6 يونيو/حزيران، 2017، https://gigaom.com/2013/11/14/white-spaces-anyone- google-opens-its-spectrum-database-to-developers/

[8] هوك آي 360 (Hawk Eye 360 ["عين الصقر 360"])، "شركة هوك آي 360 التابعة لشركة ألايد مايندز تجمع 11 مليون دولار أمريكيّ من التمويل بعنوان السلسلة A" (Allied Minds' Subsidiary HawkEye 360 Raises $11 Million in Series A Financing)، صفحة إنترنت، 23 نوفمبر/تشرين الثاني، 2016. اطلع عليه بتاريخ 30 يناير/كانون الثاني، 2017، http://www.he360.com/allied-minds-subsidiary-hawkeye-360-raises-11-million-series-financing/

[9] هوك آي 360 (HawkEye360)، الصفحة الرئيسية، غير مُؤَرَّخ. اطلع عليه بتاريخ 22 مارس/آذار، 2017، http://www.he360.com/

[10] ساندرا جونتز (Sandra Jontz)، "قطاع الصناعة يُحضِرُ المسح المحيطيّ الفضائيّ لطيف الترددات الراديوية والتحليلات الفضائية إلى القطاع التجاريّ" (Industry Bringing Space-Based RF Mapping and Analytics to Commercial Sector)، سيغنال ماغازين *(Signal Magazine)*، 28 يوليو/تموز، 2016.

[11] جونتز (Jontz)، 2016.

[12] جوزيف ب. إيفانز (Joseph B. Evans)، "المسح المحيطيّ المتقدم للترددات الراديوية (الخريطة الراديوية)" (Advanced RF Mapping [Radio Map])، وكالة مشاريع الأبحاث الدفاعية المتطورة (DARPA)، غير مُؤَرَّخ. اطلع عليه بتاريخ 9 مايو/أيار، 2017، http://www.darpa.mil/program/advance-rf-mapping

[13] تشارلز آرثر (Charles Arthur)، "سكاي غرابر: البرمجيات التي كانت كلفتها 26 دولار أمريكيّ والتي استخدمها المتمردون للقرصنة على الطائرات الأمريكية بدون طيار" (SkyGrabber: The $26 Software Used by Insurgents to Hack into U.S. Drones)، ذا غارديان (*The Guardian*)، 17 ديسمبر/كانون الأول، 2009. اطلع عليه بتاريخ 24 فبراير/شباط، 2017، https//:www.theguardian.com/technology/2009/dec/17/skygrabber-software-drones-hacked

[14] بييرلويجي باغانيني (Pierluigi Paganini)، "اقتحام الأقمار الاصطناعية بالتخريب (القرصنة) الإلكترونيّ ... أنظُر إلى السماء" (Hacking Satellites … Look Up to the Sky)، معهد إنفوسك (InfoSec Institute)، صفحة إنترنت، 18 سبتمبر/أيلول، 2013. اطلع عليه بتاريخ 24 فبراير/شباط، 2017، http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/#gref

[15] بول ماكنامارا (Paul McNamara)، "كابتن ميدنايت [الكابتن منتصف الليل]: 'لست نادماً' بشأن التشويش على أتش بي أو عام ستةٍ وثمانين" (Captain Midnight: 'No Regrets' About Jamming HBO Back in '86)، نتوورك وورلد (*Network World*)، 26 أبريل/نيسان، 2011. اطلع عليه بتاريخ 24 فبراير/شباط2017، http//:www.networkworld.com/article/2229101/security/captain-midnight-no-regrets-about-jamming-hbo-back-in-86.html

[16] بيتر ب. دو سلدينغ (Peter B. de Selding)، "يوتِلسات تعتزم إجراء تجربةٍ ميدانيةٍ لقدرةٍ جديدةٍ في مكافحة التشويش" (Eutelsat to Field Test New Anti-Jamming Capability)، سبيس نيوز (*Space News*)، 28 يناير/كانون الثاني، 2013. اطلع عليه بتاريخ 3 مارس/آذار، 2017،
http://spacenews.com/33333eutelsat-to-field-test-new-anti-jamming-capability/#sthash.6mww3eyv.dpuf

[17] كيم زِتّر (Kim Zetter)، "عصابة تجسسٍ روسيةٍ تستولي على روابطَ للأقمار الاصطناعية بهدف سرقة البيانات" (Russian Spy Gang Hijacks Satellite Links to Steal Data)، وايرد (*Wired*)، 9 سبتمبر/مارس/آذار، 3 . اطلع عليه بتاريخ2015أيلول 2017،
https://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/

[18] لورنزو فرانشسكي-بيكييراي (Lorenzo Franceschi-Bicchierai)، "هذا الجهاز الذي يكلف 1,000 دولار أمريكيّ يسمح للمخربين (القراصنة) الإلكترونيين بالاستيلاء على اتصالات الأقمار الاصطناعية" (This $1,000 Device Lets Hackers Hijack Satellite Communications)، مذربورد (*Motherboard*)، 31 يوليو/تموز، 2015. اطلع عليه بتاريخ 3 مارس/آذار، 2017،
https://motherboard.vice.com/en_us/article/this-1000-device-lets-hackers-hijack-satellite-communications

[19] فرانشسكي-بيكييراي (Franceschi-Bicchierai)، 2015.

[20] ليليان أبلون، مارتن س. ليبيكي، وأندريا أ. غولاي (Lillian Ablon, Martin C. Libicki, and Andrea A. Golay)، "أسواقٌ لأدوات جرائم الفضاء الإلكترونيّ والبيانات المسروقة: بازار المخربين (القراصنة) الإلكترونيين" (*Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*)، سانتا مونيكا، كاليفورنيا: مؤسسة RAND، RR-610-JNI، 2014. اطلع عليه بتاريخ 9 مارس/آذار، 2017،
http://www.rand.org/pubs/research_reports/RR610.html

[21] أبلون وآخرون (.Ablon et al)، 2014، ص. ix.

[22] جوردان روبرتسون ومايكل رايلي (Jordan Robertson and Michael Riley)، "التدافع نحو أسلحة الفضاء الإلكترونيّ ما بعد حادثة سنودن" (The Post-Snowden Cyber Arms Hustle"، بلومبرغ بزنس ويك (*Bloomberg Businessweek*) ، 18 يناير/كانون الثاني، 2017. اطلع عليه بتاريخ 17 أبريل/نيسان، 2017،
https://www.bloomberg.com/news/features/2017-01-18/the-post-snowden-cyber-arms-hustle

[23] ماتاثياس شوارتز (Mattathias Schwartz)، "الحرب الإلكترونية للبيع" (Cyberwar for Sale)، مجلة نيويورك تايمز (*The New York Times Magazine*)، 4 يناير/كانون الثاني، 2017. اطلع عليه بتاريخ 17 أبريل/نيسان، 2017، https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html

[24] روبرتسون ورايلي (Robertson and Riley)، 2017.

[25] لورنزو فرانشسكي-بيكييراي وجوزيف كوكس (Lorenzo Franceschi-Bicchierai and Joseph Cox)، "داخل سوق المراقبة التي توفر 'برمجيات المُلاحَقَة'، حيث الناس العاديون يراقب كلٌّ منهم هاتف الآخر" (Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones)، مذربورد (*Motherboard*)، 18 أبريل/نيسان، 2017. اطلع عليه بتاريخ 18 أبريل/نيسان، 2017،
https://motherboard.vice.com/en_us/article/inside-stalkerware-surveillance-market-flexispy-retina-x

[26] كيم زِتّر (Kim Zetter)، "كيف تصنع نظاماً خاصاً بك للمراقبة بالجملة على طريقة وكالة الأمن القومي" (How to Make Your Own NSA Bulk Surveillance System)، وايرد (Wired)، 27 يناير/كانون الثاني، 2016. اطلع عليه بتاريخ 3 مارس/آذار، 2017،
https://www.wired.com/2016/01/how-to-make-your-own-nsa-bulk-surveillance-system/

عن هذا المنظور

يدرس هذا المنظور التحليليّ فرضية أنّ استخبارات الإشارات (SIGINT) هي وظيفةٌ حكوميةٌ متأصلة، وذلك عن طريق الكشف عن المقاربات والتكنولوجيات غير الحكومية التي تسمح للمواطنين العاديين بإجراء أنشطة استخبارات الإشارات. نستكشف أربعة مجالاتٍ من التكنولوجيا تزدهر فيها استخبارات الإشارات غير الحكومية: التوعية بأحوال المجال البحريّ؛ المسح المحيطيّ لطيف الترددات الراديوية؛ التنصت، والتشويش، والاستيلاء على أنظمة الأقمار الاصطناعية؛ ومراقبة الفضاء الإلكترونيّ. نوفر بعد ذلك مجالاتٍ تدعو الحاجة فيها لبحثٍ ونقاشٍ إضافيَّين من أجل إنشاء حلولٍ قانونية، وتنظيمية، وحلولٍ في السياسات والعمليات ورأس المال البشريّ، في ما يتعلق بالتحديات التي توفرها هذه القدرات الجديدة بالنسبة للحكومة.

أُجرِيَ هذا البحث ضمن مركز سياسات الفضاء الإلكتروني والاستخبارات (Cyber and Intelligence Policy Center) التابع لمعهد أبحاث RAND للدفاع الوطنيّ (RAND National Defense Research Institute)، وهو مركزٌ للأبحاث والتطوير يعمل بتمويلٍ فيدراليّ، وبرعاية مكتب وزير الدفاع (Office of the Secretary of Defense)، وهيئة الأركان المشتركة (Joint Staff)، وقيادة المقاتلين الموحدة (Unified Combatant Commands)، وقوات البحرية (Navy)، وقوات مشاة البحرية (Marine Corps)، ووكالات الدفاع (defense agencies)، ومجموعة استخبارات الدفاع (defense Intelligence Community). للمزيد من المعلومات حول مركز سياسات الفضاء الإلكترونيّ والاستخبارات، الرجاء زيارة الموقع الإلكترونيّ: www.rand.org/nsrd/ndri/centers/intel أو الاتصال بالمدير (معلومات الاتصال متوفرةٌ على الصفحة الإلكترونية).

عن المؤلفين

كورتني واينباوم (Cortney Weinbaum) هي أخصائيةٌ في عِلم الإدارة في مؤسسة RAND. أمضت 14 عاماً في مجموعة الاستخبارات (Intelligence Community) وفي وزارة الدفاع (Department of Defense)، حيث كانت تقوم بتحسين السياسات، والممارسات، والتكنولوجيات. في السابق، قامت بمهمة ضابط استخباراتٍ ومدير برامج، حيث قامت بتطوير أنظمةٍ لجمع الترددات الراديوية، واستخبارات القياس والتوقيع الكهرومغناطيسيّ (electromagnetic measurement and signature intelligence).

ستيفن برنر (Steven Berner) هو مهندسٌ أول في مؤسسة RAND. قاد نشاطات مؤسسة RAND في الوكالة الوطنية للاستخبارات الجغرافية المكانية (National Geospatial-Intelligence Agency) لمدة تسعة أعوام، وشَمَلَ ذلك وضع استراتيجيةٍ وخارطة طريقٍ للأبحاث والتطوير في برامج الوكالة الوطنية للاستخبارات الجغرافية المكانية. يملك السيد برنر أكثر من 40 عاماً من الخبرة في برامج الأقمار الاصطناعية والفضاء الجويّ التي تعالج التداخل في مجالات التكنولوجيا، والسياسات، والأمن القوميّ.

بروس ماكلينتوك (Bruce McClintock) هو محللٌ مساعدٌ للسياسات في مؤسسة RAND، وقائد لواءٍ متقاعدٌ من القوى الجوية الأمريكية (U.S. Air Force). قام بمهمة مساعدٍ خاص لقائد قيادة الفضاء التابعة للقوى الجوية (Air Force Space Command)، والمسؤول الدفاعيّ الأول وملحق وزارة الدفاع في السفارة الأمريكية في موسكو، روسيا. هو قائدٌ طيار لديه أكثر من 3,500 ساعة طيرانٍ في 35 نوعاً مختلفاً من الطائرات، بالإضافة إلى عمليات الأمن القوميّ المتعلقة بشؤون الفضاء.

للمزيد من المعلومات حول هذا المنظور التحليلي، يرجى زيارة الموقع www.rand.org/t/PE273

RAND CORPORATION

www.rand.org

Arabic Translation
"SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain"
PE-273/1-OSD