الحمائية الرقمية:

تصاعد مخاطر الاعتماد على "البرمجيات غير الوطنية"

إيهاب خليفة

رئيس وحدة التطورات التكنولوجية، المستقبل للأبحاث والدراسات المتقدمة، أبوظبي

بدأت قناعة تسود لدى الدول وأجهزتها الأمنية والعسكرية بأن الاعتماد على التقنيات الرقمية الأجنبية قد أصبح أمراً يمثل تهديداً ماساً بالأمن القومي لها، إذ كشفت العديد من الوقائع أن هذه التقنيات يمكن توظيفها للتجسس على الدولة المستوردة لها، وهو ما دفع بعض الدول لمنع استخدامها، والشروع في تطوير بدائل محلية.

يتزايد الاعتماد في مختلف الدول على البرمجيات الذكية والسوفت وير الأجنبي بصورة يومية في مجالات الحياة كافة، مما يطرح أسئلة عديدة حول معايير الثقة والأمان في هذه المنتجات، خاصة تلك التي يتم استخدامها في المؤسسات المعنية بالأمن القومي أو تلك المسؤولة عن إدارة البنية التحتية للدول، مثل محطات الكهرباء والطاقة والسدود ونظم المواصلات والاتصالات وغيرها.

وتكشف بعض السياسات التي تبنتها الدول الغربية مؤخراً عن تصاعد المخاوف من إمكانية احتواء المنتجات التكنولوجية المستوردة من الخارج على ثغرات يمكن أن يتم توظيفها في فترة تالية لشن حرب إلكترونية أو على الأقل سرقة معلومات عسكرية واستراتيجية.

ويسعى هذا التحليل لتقدير التداعيات الأمنية والاقتصادية للاعتماد على التكنولوجيا الأجنبية، مع إلقاء الضوء على طبيعة العلاقة بين الشركات التكنولوجية والمؤسسات الأمنية، ومدى إمكانية استخدام منتجات الأولى كمنصة للتجسس من قبل الحكومات الأجنبية. وكذلك رصد عدد من المؤشرات المتعلقة بتصاعد ما يمكن تسميته "الحمائية الرقمية" وتداعياتها.

أولاً: تداعيات الاعتماد على التقنيات الأجنبية

يزداد الاعتماد البشري على التقنيات الرقمية والذكية، مثل البرمجيات والخوارزميات وتطبيقات الذكاء الاصطناعي وإنترنت الأشياء بوتيرة متسارعة، ليس فقط للاستخدامات الأمنية والعسكرية التي طغت عليها هذه التقنيات، مثل الروبوتات والدرونز والسيارات ذاتية القيادة والأسلحة الإلكترونية، ولكن كذلك للاستخدامات المدنية، مثل قطاع الصحة والنقل والمواصلات وكذلك المعاملات المالية والمصرفية والتجارية وغيرها، لذلك أصبح امتلاك القدرة على إنتاج هذه التكنولوجيا وتطويرها وتطويعها، يتمتع بنفوذ قوي في العلاقات الدولية، بل ويمتلك القدرة على تهديد أمن الدول والمجتمعات.

وبسبب الفجوة العلمية والتكنولوجية الكبيرة، ينقسم العالم حالياً إلى قسمين رئيسيين، دول منتجة للتكنولوجيا ومحتكرة لها، ودول أخرى مستهلكة لها، وعادة لا تقوم الدول التي تطور هذه التقنيات التكنولوجية، سواء كانت أجهزة أو أسلحة أو برمجيات، ببيع حقوق الملكية الفكرية لهذه المنتجات أو إتاحتها للدول التي تقوم باستيرادها، لضمان استمرار التفوق التكنولوجي

والعلمي بينهما، مع الاحتفاظ بتحقيق عوائد مالية ضخمة من بيع هذه المنتجات.

ونظراً لأن العولمة الاقتصادية فرضت تقاسم عملية الإنتاج بين عدة دول، نجد على سبيل المثال، أن الولايات المتحدة تقوم بتصنيع معظم الأجهزة الإلكترونية ولوحات الكمبيوتر الرئيسية من الصين، ليس هذا فحسب، بل أن بعض الأجهزة التابعة لشركات أمريكية كبرى، مثل شركة آبل وجوجل ومايكروسوفت يتم تصنيع أجزائها أيضاً في الصين، نظراً لانخفاض تكلفة الإنتاج، وهو ما يثير الشكوك حول إمكانية اختراق هذه الأجهزة من قبل السلطات الصينية ببرمجيات خبيثة قبل إعادة تصديرها من جديد. ويفرض الوضع السابق، في حال صحته، مجموعة من التحديات التي تواجه الدول جراء استيراد هذه الأجهزة والبرمجيات من الخارج، ويمكن توضيح ذلك في التالي:

1- التهديدات الأمنية: لم تعد صناعة البرمجيات والسوفت وير صناعة بسيطة وسهلة، بحيث يمكن تحليل برمجية معينة والإلمام بكافة أبعادها وعناصرها، ومعرفة ما إذا كانت تحتوي على ثغرات أو أبواب خلفية أم لا، بل أصبحت صناعة معقدة ومتشابكة مع غيرها، ويتضح ذلك في إنشاء منصات رقمية عملاقة (Platforms) لإدارة المنشآت والنظم المدنية والعسكرية، مثل نظام سكادا (SCADA) الذي يستخدم في إدارة البنى التحتية للدولة، فضلاً عن المنصات التي تقوم بإدارة خطوط الإنتاج العملاقة ومراقبة حركة السير والتنقل في الأماكن العامة والمناطق الحدودية، وارتباطها بعدد كبير من الحساسات (Sensors) المنتشرة في الأماكن المختلفة لتوفير معلومات دقيقة وآنية عن المواقع الجغرافية، بالإضافة إلى ارتباطها مع أجهزة إنترنت الأشياء وخدمات الحوسبة السحابية، فأصبحت صناعة السوفت وير صناعة معقدة، يصعب اكتشاف الثغرات الأمنية الموجودة بها، خاصة إذا كانت هذه الثغرة مصممة عن عمد من قبل الشركة التي أنتجت السوفت وير.

ولا تخلو بعض هذه التقنيات والبرمجيات من أبواب خلفية وثغرات وبرمجيات خبيثة مزروعة فيها عمداً لتوظيفها في عمليات التجسس والاختراق الإلكتروني إذا دعت الحاجة لذلك، فمثلاً تتهم الولايات المتحدة الأمريكية الصين دائماً بشن هجمات إلكترونية على مقاولي وزارة الدفاع الأمريكية وشركات الأسلحة لسرقة تصميمات بعض الأسلحة الحديثة، مثل الدرونز وحاملات الطائرات والطائرات الأمريكية من طراز "إف 16" (F-16) و"إف 36" (F-36)[1]، لذلك ظهرت بعض الدعوات في المؤسسات الأمنية الأمريكية للمطالبة بحظر استيراد الأجهزة المستخدمة في هذه المؤسسات من الصين.

ويلاحظ أن معظم الأجهزة الإلكترونية والذكية وأجهزة إنترنت الأشياء المستوردة والموجودة في المنازل يمكن تلغيمها بقنابل منطقية (logic bombs) أو أبواب خلفية، أي تعمد وضع ثغرات تسمح بالسيطرة على هذه المنتجات عن بعد وإعادة توجيهها واستخدامها في شن هجمات إلكترونية كبرى على الدول، أو حتى تدمير نفسها بصورة ذاتية، مما يتسبب في خسائر مادية، بل وبشرية في بعض الأحيان، سواء على مستوى الدول أو الأفراد.

2- الخسائر الاقتصادية: يتسبب الاعتماد على التقنيات الرقمية المستوردة من الخارج في نوعين من الخسائر الاقتصادية، يتمثل أولهما في الخسائر المباشرة، أي في اختلال الميزان التجاري لصالح الدول المصدرة لهذه التكنولوجيا. أما الخسارة غير المباشرة، فتتمثل فيما يلي:

- **سرقة براءات الاختراع وحقوق الملكية الفكرية:** ويتم ذلك عن طريق استغلال الثغرات والأبواب الخلفية المزروعة عمداً في الأجهزة والبرمجيات لشن هجمات إلكترونية على الشركات وسرقة براءات الاختراع وحقوق الملكية الفكرية وتقليدها وبيعها في الأسواق. وتتهم الولايات المتحدة الصين دوماً بهذا النوع من السرقات، حيث تنفق الشركات الأمريكية مئات الملايين من الدولارات على عمليات البحث والتطوير، ثم تقوم الشركات الصينية عبر القراصنة بسرقة نتائج هذه الأبحاث[2]، ومن ثم تفقد الولايات المتحدة ميزاتها التنافسية لصالح الصين بمرور الوقت.

> أكد أحد كبار المسؤولين في الاستخبارات الأمريكية أنهم قاموا على مدار سنوات بالبحث عن ثغرات في برنامج كاسبرسكي، لكنهم لم ينجحوا في العثور على ثغرة مؤثرة تدعم استنتاجاتهم بأنه يمكن أن يتم توظيفه من قبل الاستخبارات الروسية في اختراق الأجهزة الأمريكية.

- **الاستحواذ على الشركات التكنولوجية الأجنبية:** وتهدف الدول من خلال استخدام هذا الأسلوب إلى نقل المعرفة التكنولوجية من مقرها الرئيسي وتوطينها، وهو يعد هدفاً مشروعاً. ويمثل هذا الأسلوب أحد ثوابت الاستراتيجية الصينية التي تسعى جاهدة للاستحواذ على شركات التكنولوجيا الأوروبية والأمريكية. وقد تضاعف عدد الشركات الأوروبية التي تم الاستحواذ عليها من قبل الشركات الصينية ومجموعة "سوفت بانك" اليابانية في الفترة من عام 2014 وحتى 2016، من حوالي 22 شركة إلى 49 شركة[3]. وفي بعض الحالات، يتم الاستحواذ على شركات تكنولوجية تعمل في قطاعات حيوية واستراتيجية، وهو ما يهدد بنقل المعلومات التي تمتلكها هذه الشركات إلى الدولة الأجنبية التي استحوذت على الشركة.

ثانياً: مؤشرات تصاعد الحمائية الرقمية

اتجهت بعض الحكومات حول العالم إلى محاولة فرض قيود على بعض الشركات الأجنبية العاملة في مجال التكنولوجيا خشية أن تقع ضحية لعمليات التجسس والاختراق الإلكتروني، ومن هذه النماذج:

1- منع الاستحواذ على الشركات التكنولوجية الحيوية: ومن أبرز الأمثلة على ذلك قيام الرئيس الأمريكي دونالد ترامب بالتدخل لمنع مستثمرين صينيين من الاستحواذ على شركة "لاتيس لأشباه الموصلات" (Lattice Semiconductor) المتخصصة في صناعة الشرائح الدقيقة (Microchip) في صفقة قيمتها 1.3 مليار دولار لأسباب تتعلق بالأمن القومي[4].

وشرع عدد من الدول الأوروبية في تبني الإجراء نفسه، إذ يبحث الاتحاد الأوروبي مقترحاً بفرض قيود على استحواذ الصين على الشركات الأوروبية التي تعمل في مجالات حساسة، مثل البنية التحتية، والطاقة، والنقل، والفضاء، والذكاء الاصطناعي، والروبوتات، وأشباه الموصلات[5].

2- وقف الاعتماد على الأجهزة الإلكترونية الأجنبية: حيث يرى ريتشارد كلارك، المسؤول السابق عن حماية البنية التحتية ومكافحة الإرهاب في البيت الأبيض، أن كل الشركات الأمريكية مخترقة من الصين بسبب استيراد أجهزة الراوتر والشرائح الإلكترونية والهاردوير منها، وهو ما يجعل الولايات المتحدة أكثر عرضة للحرب الإلكترونية والتجسس والتخريب الإلكتروني من قبل الصين[6].

ولعل ما يضفي مصداقية على الاتهام السابق قيام الولايات المتحدة في أغسطس 2017 بإصدار توجيهات جديدة تقضي بوقف استخدام الدرونز، التي تصنعها الشركة الصينية "إس زد دي جيه آي" (SZ DJI)، وذلك نظراً لوجود ثغرات أمنية في منتجاتها. وتجدر الإشارة إلى أن الشركة تهيمن على حوالي 70% من سوق الدرونز المخصصة للاستخدامات المدنية والتجارية في العالم[7].

3- مخاوف الاعتماد على البرمجيات الأجنبية: فقد تبنت الحكومة الأمريكية مؤخراً قراراً بمنع الوكالات الفيدرالية الأمريكية من استخدام منتجات شركة كاسبرسكي الروسية التي تعمل في مجال الأمن الإلكتروني. فقد أصدرت إلين ديوك، القائمة بأعمال وزير الأمن الداخلي الأمريكي، توجيهاً ملزماً يأمر الوكالات المدنية الفيدرالية بوقف استخدام برنامج كاسبرسكي على أساس أن الشركة لها صلات بالحكومة الروسية وأن برامجها تمثل تهديداً أمنياً.

وقد أعرب البيان الصادر عنها، أن وزارة الأمن الداخلي قلقة بشأن وجود علاقات بين بعض مسؤولي كاسبرسكي والمخابرات الروسية ووكالات حكومية أخرى، فضلاً عن سماح القانون الروسي لوكالات الاستخبارات الروسية بأن تطلب المساعدة من كاسبرسكي، بل وإجباره على اعتراض الاتصالات التي تتم عبر الشبكات الروسية.

واعترضت الشركة الروسية على هذه الاتهامات، ونفت وجود أي علاقة غير شرعية تربط بينها وبين أي حكومة حول العالم، بما في ذلك الحكومة الروسية، بالإضافة إلى التأكيد على أن القانون الروسي المشار إليه ينطبق على شركات الاتصالات ومزودي خدمة الإنترنت، وليس الشركات العاملة في مجال أمن الحواسيب، مثل كاسبرسكي.

ولم تطمئن الحكومة الأمريكية لهذه الردود من جانب الشركة، وهو ما يرتبط بوجود اعتقاد جازم لدى أجهزة الاستخبارات الأمريكية بأن هناك علاقات بين كاسبرسكي والكرملين، سواء كان ذلك في إطار تعاون مشترك بينهما، أو من خلال اختراق الكرملين الشركة التي تقع في موسكو[8]، ويرتبط ذلك بما يلي:

- **انتماء رئيس الشركة إلى مجمع الاستخبارات الروسي:** إذ إن يوجين كاسبرسكي، المؤسس والرئيس التنفيذي للشركة، قد تعلم في معهد "كريبتوجرافي" المدعوم من جهاز الاستخبارات الروسي السابق (KGB)، وخدم في الاستخبارات العسكرية الروسية عقب تخرجه عام 1987[9].
- **وجود تعاون بين الشركة وجهاز الاستخبارات الروسي "الإف إس بي":** فقد ذكر موقع بلومبيرج الإخباري، قبل شهرين من إثارة القضية، أنه اطلع على رسائل إلكترونية بين الرئيس التنفيذي يوجين كاسبرسكي وكبار موظفي الشركة، تشير إلى مشروع سري للأمن على الإنترنت قامت بتنفيذه الشركة بناء على طلب جهاز "الإف إس بي"، يستهدف حصول الأجهزة الروسية على معلومات عن القراصنة الذين يقفون خلف الهجمات الإلكترونية حول العالم، وإن كان من الملحوظ أن هذا لا يمثل دليلاً يدين الشركة، خاصة أن كل شركات التكنولوجيا الكبرى تتعاون مع أجهزة الاستخبارات في بلدانها[10].
- **اتهام روسيا بتورطها في سرقة بيانات تابعة لوكالة الأمن القومي الأمريكي:** وتتعلق هذه البيانات بتكنولوجيات أمريكية تم تطويرها لاختراق شبكات الكمبيوتر والتجسس على الأفراد حول العالم، حيث أشارت التحقيقات الأمريكية إلى أن أحد المقاولين المتعاملين مع وكالة الأمن القومي الأمريكي قام في عام 2015 بأخذ هذه البيانات معه إلى المنزل للعمل عليها عبر جهاز اللاب توب الخاص به والذي يعمل عليه برنامج كاسبرسكي، وهو ما مكن القراصنة الروس من الولوج إلى الجهاز وسرقة البيانات حسب التقارير الأمريكية[11]، الأمر الذي تم اعتباره تهديداً صريحاً للأمن القومي الأمريكي.

وتجدر الإشارة إلى أن أحد كبار المسؤولين في الاستخبارات الأمريكية قد أكد أنهم قاموا على مدار سنوات بالبحث عن ثغرات في برنامج كاسبرسكي، لكنهم لم ينجحوا في العثور على ثغرة مؤثرة تدعم استنتاجاتهم بأنه يمكن أن يتم توظيفه من قبل الاستخبارات الروسية في اختراق الأجهزة الأمريكية[12].

وعلى الجانب الآخر، فإن الرئيس الروسي فلاديمير بوتين لطالما حذر الشركات التكنولوجية في روسيا من استخدام مكونات تكنولوجية أجنبية، سواء كانت سوفت وير أو هارد وير، وأشار إلى أن الشركات التي ستعتمد على مكونات غير محلية لن تتعامل معها الحكومة الروسية في بعض المجالات لأن ذلك يمثل تهديداً للأمن القومي السيبراني الروسي، مؤكداً أن ما تتم كتابته على أجهزة الكمبيوتر يتم إرساله على الفور إلى الولايات المتحدة الأمريكية[13]، في إشارة إلى برنامج مايكروسوفت أوفيس.

4- البحث عن بدائل وطنية لخدمات الإنترنت: بدأ هناك توجه قوي لدى العديد من الدول لتوطين خدمات البريد الإلكتروني، وهو ما ارتبط في جانب منه بالأزمة الدبلوماسية بين الولايات المتحدة الأمريكية وجمهورية ألمانيا الاتحادية عام 2013 على خلفية اتهامات بقيام وكالة الأمن القومي الأمريكي بالتجسس على هاتف المستشارة الألمانية أنجيلا ميركل منذ عام 2002[14]. فقد اتجهت الحكومة الألمانية منذ ذلك الوقت إلى تأمين الاتصالات الحكومية، سواء تلك التي تتم هاتفياً أو

في المجال السيبراني. وبدأت الحكومة الألمانية تقديم خدمات الإيميل عبر شركات محلية وليس أمريكية[15]، مثل شركة تليكوم (Telekom) وجيه إم إكس (GMX)، وويب دي (web.de)، حتى لا تقع مرة أخرى ضحية لتجسس وكالة الأمن القومي الأمريكي.

ولم يقتصر الأمر على ألمانيا فقط، إذ قامت الحكومة الإيرانية في عام 2013 بالإعلان عن تقديم خدمات البريد الإلكتروني الوطني، وذلك بعد أن قامت بإغلاق مقدمي هذه الخدمة من الشركات الأجنبية مثل جوجل وياهو[16]، أما الحكومة الهندية فقد منعت المكاتب الحكومية من استخدام خدمات البريد الإلكتروني لشركات، مثل جوجل وياهو وهوت ميل[17] أيضاً، في محاولة لتوطين خدمات البريد الإلكتروني في الهند.

وفي نوفمبر 2014 صوّت أعضاء البرلمان الأوروبي في مدينة ستراسبورج الفرنسية بأغلبية 384 صوتاً مقابل 174 صوتاً لصالح قرار بفصل خدمات البحث التي تقدمها شركات الإنترنت عن بقية خدماتها الأخرى، مستهدفة من هذا التصويت شركة جوجل، التي قالت إنها تستحوذ على 90% من سوق البحث الإلكتروني في بعض الدول الأوروبية، وعلى الرغم من أن القرار رمزي وغير ملزم، بل وغير واقعي، نظراً لضعف المنافسة بين جوجل وغيرها من الشركات، إلا أنها تبقى إشارة على عدم رضا الاتحاد الأوروبي عن سيطرة جوجل على سوق البحث الإلكتروني في أوروبا[18]، ورغبة منها بصورة غير مباشرة على تشجيع الشركات الأوروبية على إنشاء محرك بحث أوروبي بعيداً عن هيمنة جوجل الأمريكية.

أما الصين، فقد تبنت توجهاً راديكالياً، إذ قامت الحكومة الصينية بالتضييق على شركة جوجل الأمريكية بدءاً من عام 2009، حتى قامت في النهاية بحجب جميع خدماتها في الصين بما فيها محرك البحث والبريد الإلكتروني (Gmail) وخرائط جوجل، في الوقت ذاته الذي طورت فيه الحكومة الصينية محرك البحث الخاص بها، وهو محرك "بايدو" (Baidu)، في محاولة منها لتوطين صناعة محركات البحث[19].

وفي الختام، يمكن القول إنه على الرغم من وجود العديد من المحاولات الرامية إلى توطين بعض الصناعات والمنتجات التكنولوجية، فإنه مازالت هناك تحديات كبرى تقف حائلاً أمام تحقيق ذلك، خاصة في ضوء تفاوت القدرات التكنولوجية بين الدول المختلفة، وصعوبة تطوير بدائل محلية تناظر مثيلاتها الأجنبية، وهو ما يقتضي من الدول كافة فرض قيود شديدة على الشركات التي تتعامل مع المؤسسات الأمنية والعسكرية للتأكد من سلامة المنتج من أي أدوات تخريب يمكن توظيفها لتهديد الأمن القومي للدولة، وهو تحدٍ ليس بالهين بالنظر إلى عجز أجهزة الاستخبارات الأمريكية عن إدانة برنامج كاسبرسكي بشكل قاطع، وهو ما يعني في التحليل الأخير أنه قد لا يكون هناك، أحياناً، حل سوى توطين الصناعات التكنولوجية.

1- Bill Gertz, NSA Details Chinese Cyber Theft of F-35, Military Secrets, **The Washington Free Beacon**, January 22, 2015, accessible at: https://goo.gl/rRN4Za (Last accessed: October 1, 2017).

2- **Ibid.**

3- Nic Fildes, Asian groups buy into European tech, **Financial Times**, June 7, 2017, accessible at: https://goo.gl/NSguvT (Last accessed: October 15, 2017).

4- China's plan to buy up foreign technology meets increasing resistance from US and Europe, **South China Morning Post**, September 15, 2017, accessible at: https://goo.gl/QHXaL8 (Last accessed: October 2, 2017).

5- **Ibid.**

6- Adrian Kingsley-Hughes, Hardware imported from China could leave U.S. open to cyber-threats, **Zdnet**, March 30, 2012, accessible at: https://goo.gl/SJ93hH (Last accessed: October 1, 2017).

7- Alwyn Scott, US army halts use of Chinese made drones over cyber concerns, **Reuters**, August 7, 2017, accessible at: https://goo.gl/AQBWgt

8- U.S. Bans All Federal Agencies From Using Kaspersky Software, **Bloomberg**, September 13, 2017, accessible at: https://goo.gl/GwiUpw (Last accessed: October 10, 2017).

9- Elias Groll, Amid Washington Russia Frenzy, Kaspersky Faces Backlash, **Foreign Policy**, August 11, 2017, accessible at: https://goo.gl/G9PBm4 (Last accessed: October 15, 2017).

10- Kaspersky Lab Has Been Working With Russian Intelligence, **Bloomberg**, July 11, 2017, accessible at: https://goo.gl/mqaWx7 (Last accessed: October 12, 2017).

11- U.S. House committee calls new hearing on Kaspersky software, **Reuters**, October 6, 2017, accessible at: https://goo.gl/aqZ2Am (Last accessed: October 10, 2017).

12- Elias Groll, **op.cit.**

13- Putin tells Russia's tech sector: Ditch foreign software or lose out, **CNBC**, Sept 9, 2017, accessible at: https://goo.gl/Y9hX76 (Last accessed: October 10, 2017).

14- تقرير: الولايات المتحدة تجسست على هاتف ميركل منذ 2002، **موقع بي بي سي**، 26 أكتوبر 2013، موجود على الرابط التالي: https://goo.gl/BcTmiA (تاريخ المطالعة: 19 أبريل 2014).

15- Germans switch to national email providers after US scandal, **Euobserver**, August 29, 2013, accessible at: https://euobserver.com/justice/121232 (Last accessed: October 15, 2017).

16- Iran opens national email service, **The National**, July 8, 2013, accessible at: https://goo.gl/E8ZvyD (Last accessed: October 15, 2017).

17- Indian Government bans third party email services, including Gmail and Yahoo, **Security Affairs**, March 1, 2015, accessible at: https://goo.gl/zsRL5P (Last accessed: October 15, 2017).

18- البرلمان الأوروبي يصّوت على تقسيم جوجل، ليبقى التساؤل الأبرز حول كيفية التنفيذ؟، **موقع ICN.com الإلكتروني**، 30 نوفمبر 2014، موجود على الرابط التالي:http://goo.gl/3bfNnJ (تاريخ المطالعة: 15 يناير 2015).

19- China cracks down on reporting of Google conflict, **The Guardian**, March 26, 2010, accessible at: https://www.theguardian.com/technology/blog/2010/mar/26/google-china (Last accessed: October 15, 2017).