المستقبل
للأبحاث والدراسات المتقدمة

اسم الموضوع : معضلة هواوي:

عنوان الموضوع : تحديات تأمين شبكات الجيل الخامس في الولايات المتحدة

تاريخ النشر : 08/09/2019

اسم الكاتب : روبرت وليامز

الموضوع :

عرض: د. رغدة البهي، مدرس العلوم السياسية، بجامعة القاهرةعلى الرغم من الثورة التي قد تُحدثها شبكات الجيل الخامس في الاقتصاد الرقمي، من خلال توظيف التطبيقات الجديدة (السيارات ذاتية القيادة، وأتمتة المصانع، والشبكات الكهربائية الذكية، والمدن الذكية) التي تعتمد على اتصالات فائقة السرعة، إلا أنها تشكل مخاطر عدة على الأمن القومي للدول الغربية، ولا سيما مع اعتمادها على شركة هواوي الصينية التي تعد أكبر منتج للمعدات اللازمة لتشغيل شبكات الجيل الخامس، والتي تربطها علاقات وثيقة بالحكومة الصينية. وفي هذا السياق، تبرز أهمية التقرير المعنون "تأمين شركات الجيل الخامس: التحديات والتوصيات"، المنشور على موقع مجلس الشئون الخارجية منتصف يوليو الماضي، للكاتب "روبرت وليامز" (المدير التنفيذي لمركز بول تساي بكلية الحقوق جامعة ييل)، والذي جادل فيه بأن إصدار "ترامب" أمرًا تنفيذيًّا يحظر استخدام معدات هواوي في الشبكات الأمريكية لا يعني تأمين تلك الشبكات بالضرورة. ولذا، لا بد من اعتماد استراتيجيةٍ أوسع تشمل كلاً من: التدابير الفنية، ومتطلبات الأمن السيبراني، والاستثمار في التدريب ومهارات البحث، وغيرها.تكنولوجيا الجيل الخامس:عرّف الكاتب شبكات الجيل الخامس بمجموعةٍ من المعالجات الدقيقة التي ترسل حزم البيانات بسرعةٍ فيما بينها؛ حيث سترسل الأجهزة (بما في ذلك: الهواتف الذكية، والسيارات، والروبوتات) البيانات وتتلقاها عبر موجات الراديو بترددات الجيل الخامس، وذلك من خلال الاتصال بجيلٍ جديد من وحدات الراديو الصغيرة الخلوية التي تشكل شبكة الوصول اللا سلكي التي تربط بين الأجهزة الفردية وأجهزة التوجيه والمحولات التي تشكل الشبكة الأساسية.وتختلف شبكات الجيل الخامس عن الأجيال السابقة في موقع الوظائف الحرجة؛ ففي RAN، الأجيال السابقة، تحدث الوظائف الحساسة في قلب شبكات الاتصالات، والتي تشمل: مصادقة البيانات وتوجيها، بينما تقوم أجهزة شبكة الوصول اللا سلكي الأخرى (أو ما يسمى الحافة) بتوصيل أجهزة المستخدم بالشبكة الأساسية.وفي شبكات الجيل الخامس، يتلاشى ذلك التمييز. فتتطلب الاستخدامات المتقدمة اتصالات كبيرة الحجم مع زمن انتقال محدود، كالذي تتطلبه أجهزة الاستشعار المضادة للتصادم في سيارة ذاتية القيادة على سبيل المثال، إذ إنها تعتمد بالأساس على بياناتٍ فوريةٍ وموثوقة.ولذا، يجب تقليص المسافة بين الأجهزة التي تتواصل مع بعضها بعضًا لتوفير تلك السرعة العالية. وبالتالي، يتزايد تعقيد شبكات الجيل الخامس مقارنة بالأجيال السابقة، والتي تم تصميمها بشكلٍ أساسي لخدمات الصوت والبيانات للمستخدمين.ومن ثمّ، تقوم شبكات الجيل الخامس بثلاث مهام رئيسية؛ يتمثل أولها في سرعات التنزيل السريعة للمستخدمين. ويتصل ثانيها بالاتصالات الموثوقة عالية السرعة والمصممة حيث تتواصل مليارات (IoT)، للمركبات المستقلة وغيرها من التطبيقات التي لا تتطلب ثغرات في الاتصال. ويرتبط ثالثها بالاتصالات الضخمة من آلةٍ إلى أخرى، أو إنترنت الأشياء الأجهزة باستمرار فيما بينها.ففي الأجيال السابقة من شبكات المحمول تم الاعتماد على الأجهزة المتصلة بالشبكة في إطار بنيةٍ مركزيةٍ حاكمة، بينما تتصل شبكات الجيل الخامس بمليارات من أجهزة إنترنت الأشياء المتصلة ببعضها بعضًا في بيئةٍ شبيهةٍ بالشبكة.مخاطر متزايدة:يشير الكاتب إلى تعدد مجالات شبكات الجيل الخامس لتشمل: المركبات ذاتية القيادة، والشبكات الكهربائية الذكية، والطب الذكي، والاتصالات العسكرية، وغيرها. وعلى هذا النحو، يصعب التمييز بين الأجزاء الرئيسية أو الحرجة في البنية التحتية لشبكة الجيل الخامس عن مثيلتها الفرعية.ومع تزايد اعتماد الشركات والأفراد على تلك الشبكات، تتزايد مخاطر سرقة البيانات، واستهداف الشبكات بواسطة الهجمات السيبرانية. وتتزايد بالمثل نقاط الضعف المحتملة والثغرات الأمنية، مما يقوض من إمكانية اكتشاف الأنشطة السيبرانية الضارة.ووفقًا للكاتب، تتمثل أبرز التحديات التي تواجه تلك الشبكات في إمكانية التلاعب بمعداتها الرئيسية، وذلك التي تسمح باعتراض وإعادة توجيه البيانات أو تخريب الأنظمة الحيوية، حتى في أعقاب اجتياز الأنظمة (Backdoors) "على شاكلة البوابة السرية التي تُعرف باسم "الباب الخلفي لاختبارات الأمان، نظرًا لاستمرار إرسال التحديثات إليها من قبل الشركات المُصنّعة. ناهيك عن إمكانية استهداف القراصنة السيبرانيين للخوارزميات التي تعمل بموجبها أنظمة الذكاء الاصطناعي، ذلك أن إنترنت الأشياء يوسع بشكلٍ كبيرٍ من فرص ونتائج تلك الهجمات. وقد يكون من الصعب اكتشاف الهجمات التي تنسخ البيانات أو تعدلها؛ فعلى الرغم من خرق الأنظمة، تعمل الشبكات الرئيسية بشكلٍ طبيعي.هواوي والجيل الخامس:وطبقًا للكاتب، تعتبر هواوي واحدةً من أكبر الشركات المنتجة للمعدات اللازمة لتشغيل شبكات الجيل الخامس على مستوى العالم. وهي قادرةٌ على توسيع حصتها في السوق، بالنظر إلى انخفاض تكلفة منتجاتها، واستثماراتها في البحث والتطوير، وقدرتها على تقديم حلولٍ شاملةٍ فعالةٍ تشمل كلاً من: الأجهزة، والشبكات، ومراكز البيانات، وغيرها.وفي المقابل، تتعدد المخاوف الأمنية الأمريكية من هواوي بفعل: مخاطر الأمن السيبراني الملازمة للجيل الخامس، وممارسات هواوي التجارية السابقة، وطبيعة العلاقة بين شركات التكنولوجيا الصينية والحكومة الصينية. ولحماية الأمن القومي الأمريكي، وضع أمرُ "ترامب" التنفيذي الأساسَ لوزارة التجارة الأمريكية لمنع الشركات الأمريكية من استخدام معدات هواوي. فاتسعت بذلك القيود الأمريكية التي فرضت العام الماضي فيما يتعلق باستخدام هواوي من قبل الوكالات الأمريكية والمقاولين الفيدراليين.كما أضافت وزارة التجارة شركة هواوي و(68) شركةً تابعةً إلى قائمة الكيانات الخاضعة لقيود التصدير بسبب مخاطرها على الأمن القومي والسياسة الخارجية الأمريكية. وعلى الرغم من تعهد "ترامب" للرئيس الصيني "شي جين بينغ" -في قمة مجموعة العشرين في يونيو الماضي- بتخفيف قيود التصدير إلى حدّ ما، لا يتضح بعد إلى أي مدى سَتُحَرم هواوي من استيراد الموصّلات الأمريكية والرقاقات التي تعد ضروريةً لمختلف عمليات الشركة.الهواجس الأمنية: عدّد الكاتب الأدلة على رداءة الممارسات الهندسية لشركة هواوي، بل وإمكانية استغلالها من قبل قراصنة الكمبيوتر؛ فقد أشار مركز تقييم الأمن السيبراني في المملكة المتحدة (وهو هيئة رقابة تقوم بمراجعة أمان معدات هواوي) في مارس 2019 إلى جملة من المشكلات المتعلقة بنهج هواوي في تطوير البرمجيات، وهو النهج الذي يُولّد مخاطرَ متزايدةً بشكلٍ كبيرٍ على المشغلين.وتتعدد الدلائل أيضًا على انتهاك شركة هواوي المتكرر للقوانين المحلية في البلدان التي تعمل فيها. ففي يناير الماضي، اتهمت وزارة العدل الأمريكية الشركة بالاحتيال، وغسل الأموال، وانتهاك العقوبات الأمريكية على إيران، وسرقة الأسرار وهي شركة ناشئة) CNEX وفي يناير الماضي أيضًا، اعتقلت الحكومة البولندية مدير مبيعات هواوي بتهمة التجسس. كما اتهمت .T-Mobile التجارية من شريكها التجاري الأمريكي في الولايات المتحدة) هواوي ونائب رئيس مجلس الإدارة بالتآمر لسرقة أسرارها التجارية. وعليه، تسهم تلك الإشكاليات وغيرها -بالإضافة إلى سرية هواوي وملكيتها الغامضة- في تزايد المخاوف من أنشطة الشركة ونواياها؛ خاصة وأن هواوي وغيرها من شركات الاتصالات الصينية مطالبة بمساعدة الحكومة الصينية في "العمل الاستخباراتي". كما تزايد دعم بكين لشركات التكنولوجيا الصينية في السنوات الأخيرة، وشنت حملةً عالميةً لرعاية سرقة الملكية الفكرية الأجنبية، وإطلاق برامج مراقبة رقمية شاملة. وبالنظر إلى ذلك، فإن استقلالية شركة هواوي عن الحكومة الصينية تمثل تحديًا كبيرًا.ويجادل المسئولون الأمريكيون والأوروبيون بأن الدعم الصيني يمنح شركات مثل هواوي مزايا تجارية غير عادلة تحول دون تطوير ونشر شبكات الاتصالات العالمية. وبالمثل، اتهمت بكين عملية وضع معايير الجيل الخامس بالتسييس.وتواجه الحكومات الوطنية صعوباتٍ في تأمين التكلفة حال قررت استبعاد هواوي أو مزودي المعدات الآخرين من شبكات الجيل الخامس الوطنية. أما البلدان النامية التي تركز على الفوائد الاقتصادية لبناء تلك الشبكات، فمن المرجح أن يكون التجسس مصدر قلقٍ ثانوي.وبالنسبة للولايات المتحدة، لن يسفر استبعاد أي شركة عن البنية التحتية لشبكة الولايات المتحدة أو شبكات حلفائها عن القضاء على تهديدات التجسس أو التخريب. كما أثبت المتسللون الإيرانيون والروس وغيرهم بالفعل قدرتهم على اختراق الشبكات الأمريكية التي لم تستخدم المعدات الصينية.التوصيات المقترحة:يجادل الكاتب بأن أمن شبكات الجيل الخامس يتطلب اعتماد نهج متعدد يتضمن كلاً من: التدابير الفنية، والتعديلات التنظيمية، ونظام المسئولية القانونية والدبلوماسية، والاستثمارات في التدريب على مهارات البحث والأمن السيبراني، وغيرها. وفي هذا السياق، طرح الكاتب جملةً من التوصيات التي يمكن إجمالها على النحو التالي:أولاً- العمل عن كثب مع مختلف الحلفاء الأمريكيين لتطوير مبادئ مشتركة للحد من المخاطر والثغرات الأمنية.ثانيًا- تحفيز قدرة مقدمي خدمات الهواتف المحمولة على تحديد ومنع الاستغلال والهجمات الضارة باستخدام أدوات التعلم الآلي.ثالثًا- اعتماد سياساتٍ تنظيميةٍ ووزارة الدفاع وغيرها من الوكالات لإعادة تخصيص الترددات الوسيطة التي تمتلك حكومة (FCC) قائمةٍ على الشفافية وحوافز السوق.رابعًا- التنسيق بين لجنة الاتصالات الفيدرالية الولايات المتحدة أجزاء كبيرةً منها للأغراض التجارية.خامسًا- إلزام المصنعين بالكشف عن ممارساتهم لضمان أمن إنترنت الأشياء في كافة أطوار عملية تصنيع منتجاتهم من قبل لجنة الاتصالات الفيدرالية.سادسًا- إدراج لجنة الاتصالات الفيدرالية في فرقة العمل المعنية بإدارة مخاطر تكنولوجيا المعلومات والاتصالات.سابعًا- تحسين نظام المسئولية القانونية لتحسين الأمن السيبراني في القطاع الخاص. ثامنًا- تطوير قطاع الاتصالات لمعايير طوعية تسترشد بمثيلتها التي تطبقها المحاكم في قضايا المساس بالأمن السيبراني، كي توفر الأساس لتسعير مخاطر الإنترنت. تاسعًا- تفعيل الريادة الأمريكية في وضع المعايير العالمية وتعزيز المصالح الأمريكية في مجال الأمن السيبراني.وختامًا، يجب أن تهدف سياسة الولايات المتحدة إلى التأمين الاستباقي للشبكات الأمريكية، بجانب تعزيز التكنولوجيا الأمريكية دون سياسات الحماية الاقتصادية. فعلى الرغم من اتخاذ خطواتٍ جادة لحماية الأمن القومي الأمريكي في البنية التحتية للجيل الخامس، تظل واشنطن بحاجةٍ إلى الانفتاح على الاستثمار والمعرفة الدافعة للابتكار التي جعلت منها رائدةً في مجال التكنولوجيا.المصدر:Robert Williams, Securing 5G Networks Challenges and Recommendations, Council on Foreign Relations July 15, 2019.