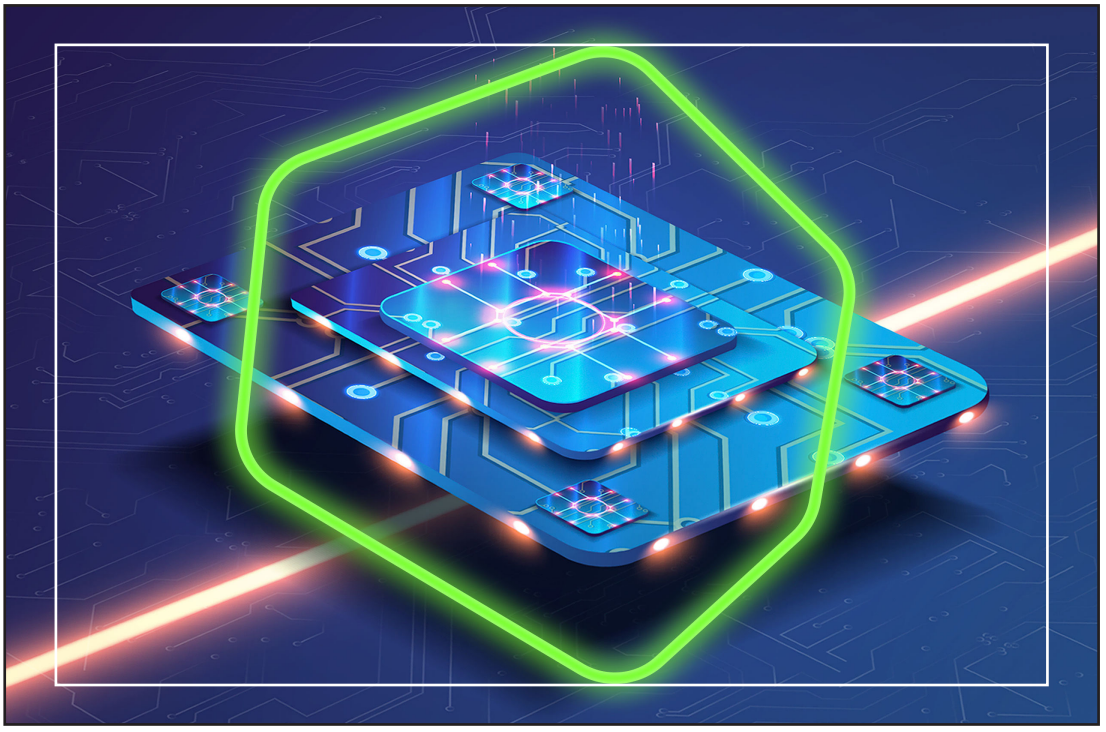
مركز البيان للدراسات والتخطيط
Al-Bayan Center for Planning and Studies

تفتح لنا سياسة الرئيس «بايدن» للأمن السيبراني عصر ما بعد الكم

آرثر هيرمان



ترجمة وتحرير مركز البيان للدراسات والتخطيط

عن المركز

مركزُ البيان للدراسات والتخطيط مركز مستقلٌّ، غيرُ ربحيّ، مقرّه الرئيس في بغداد، مهمته الرئيسة -فضلاً عن قضايا أخرى- تقديم وجهة نظر ذات مصداقية حول قضايا السياسات العامة والخارجية التي تخصّ العراق بنحو خاصٍ ومنطقة الشرق الأوسط بنحو عام. ويسعى المركز إلى إجراء تحليل مستقلّ، وإيجاد حلول عمليّة جليّة لقضايا معقدة تهمّ الحقليْن السياسي والأكاديمي.

ملاحظة:

الآراء الواردة في المقال لا تعبر بالضرورة عن اتجاهات يتبناها المركز، وانما تعبر عن رأي كتابُها.

ترجمة: د.باسم علي خريسان

www.bayancenter.org
info@bayancenter.org

Since 2014

تفتح لنا سياسة الرئيس «بايدن» للأمن السيبراني عصر ما بعد الكم

آرثر هيرمان *

تلقَّت إدارة «بايدن» عديداً من الضربات بسبب سياساتها، من الانسحاب الفوضوي للقوات الأمريكية من أفغانستان إلى أعلى معدَّل تضخُّم منذ (40) عاماً إلى الأزمة الإنسانية على الحدود الجنوبية لأمريكا. ولكن في الشهر الماضي، حقَّقت نجاحاً كبيراً في ترتيب مكانة الحكومة في مجال الأمن السيبراني، وتمهيد الطريق لمستقبل سيبراني آمن.

أصدر البيت الأبيض مذكرة الأمن القومي التي تركز -لأول مرة- على مخاوف الأمن القومي الأمريكي من التهديد المستقبلي لأجهزة (الكمبيوتر الكمومية)[1] واسعة النطاق إلى البيانات المشفَّرة، ما يعني كل شيء من السجلات الحكومية والبيانات السرية إلى بطاقات الائتمان والمعاملات المصرفية.

بدلاً من استخدام البتات الرقمية لمعالجة البيانات كسلسلة من الآحاد والأصفار، كما تفعل أجهزة الكمبيوتر التقليدية، تستخدم أجهزة الكمبيوتر الكمومية «الكيوبت»، والتي يمكن أن تمثِّل أي مجموعة من (0، و1) في وقت واحد. يسمح هذا لقوة الحوسبة بالنمو بصورة كبيرة مع زيادة عدد البتات الكمومية، -على سبيل المثال- يمكن لجهاز كمبيوتر كمي بسعة (2000 إلى 4000) كيلوبت، فك تشفير جميع أبنية تشفير المفتاح العام تقريباً، تلك المستخدمة في كل شيء، بدءاً من البنوك وبطاقات الائتمان إلى شبكة الطاقة. إذ تعتمد هذه البنى على أرقام أكبر من أن تحللها أجهزة الكمبيوتر التقليدية، لكن الكمبيوتر الكمي يمكنه فعل ذلك وسيحققه.

1 - أنموذجٌ حوسبيٌّ نظريٌّ تُعالجُ عن طريقه البيانات وعمليات الحوسبة عن طريق قوانين الكم، فوحدة البيانات الأساسية التي تستخدم في الحوسبة التقليدية، والتي تسمى البت استُبدلَت بوحدة بياناتٍ أخرى تدعى «البت الكمومي» (qubit) الذي يستند إلى الذرات والتراكيب الجزيئية المتناهية الدقة، الفرق بين الوحدتين هو أنَّ البت يعطي واحدةً من قيمتين؛ إمَّا (0 أو 1) ولذلك يسمَّى الثنائية، في حين البت الكمومي فسيعطي قيماً عديدةً هي إمَّا (0 أو 1) أو التراكب بين (0 و 1)، وهذا يعني لن يعتمد الكومبيوتر الكمومي أسلوباً محدداً في عمله، وستكون هنالك نتائجاً وحلولاً عديدة لكلِّ حالةٍ، وهذه القيم الجديدة الناتجة عن التراكب بين (0 و 1) ستكون مبهمةً للحواسيب التقليدية. https://www.arageek.com/l

* زميل أول في معهد هدسون ومدير مبادرة التحالف الكمومي. وهو المؤلف الذي وصل إلى نهائيات جائزة بوليتزر مؤخراً عن كتابه «قلب الفايكنج: كيف غزا الإسكندنافيون العالم» (١٢٠٢).

يختلف الخبراء حول الوقت الذي سنرى فيه أجهزة كمبيوتر كمومية بهذا الحجم والقدرة. أفاد تقرير حديث لمؤسسة (RAND) أنَّ الأمر قد يستغرق (15) عاماً؛ ومع ذلك، صرَّح الرئيس التنفيذي لشركة (Google) علناً أنَّه يعتقد أنَّ ذلك يمكن أن يحدِّث في أقرب وقت بعد خمس أو عشر سنوات من الآن، هنالك شيء واحد واضح: الدولة الوحيدة التي لديها الموارد للقيام بذلك إلى جانب الولايات المتحدة الأمريكية هي الصين، وهو النظام نفسه الذي شنَّ حرباً سيبرانياً على أمريكا والدول الديمقراطية على مدى عقدين من الزمن.

مع وضع هذا التهديد في الاعتبار، أصدر البيت الأبيض وثيقةً تاريخيةً هي مذكرة الأمن القومي (NSM-8)، التي تدفع بالأمن السيبراني للحكومة إلى حقبة ما بعد الكم: الخطوة الرسمية الأولى لجعل جهاز الأمن القومي الأمريكي جاهزاً آمناً في مجال الكم.

أعطت المذكرة وكالة الأمن القومي (30) يوماً لبدء تحديث مجموعة خوارزمية الأمن القومي التجاري (CNSA)[2]، وهي عملية ستشمل زيادة تشفير مقاوم للكم، و(CNSA) هي مجموعة من الخوارزميات الآمنة المعتمدة للاستخدام من قبل جميع مستخدمي البيانات المشفرة، بما في ذلك القطاع الخاص.

من المفترض أن تحدِّد الوكالات التي تتعامل مع أنظمة الأمن القومي جميع «حالات التشفير التي لا تتوافق مع خوارزميات مقاومة الكم المعتمدة من وكالة الأمن القومي» أو (CNSA) المحدث –في غضون (180) يوماً–، وأن تضع «جدولاً زمنياً لنقل هذه الأنظمة إلى استخدام التشفير المتوافق، لتضمين التشفير المقاوم للكم».

هذه الوثيقة هي الأولى التي خرجت من جهاز الأمن القومي بالبيت الأبيض الذي يذكر فيها على وجه التحديد التشفير المقاوم للكم في سياق التخطيط الفيدرالي الحالي للأمن السيبراني. يعدُّ هذا انتصاراً كبيراً لمبادرة التحالف الكمومي في معهد هدسون، والتي كانت تدفع بقضية الأمن الكمي في السنوات الأربع الماضية، ولعلم المعلومات الكمومية عموماً.

من المهم في الوقت نفسه إدراك أنَّ الخطوة التالية والأهم هي التنفيذ. هنا إذ يتعيَّن على «الكونجرس» أن يصعِّد بالإشراف والتمويل والتوكيد من أنَّ ما يجب القيام به لمواجهة تهديد

2 – مجموعة من خوارزميات التشفير الصادرة من قبل وكالة الأمن القومي كبديل لل (ASN) جناح (B) تشفير الخوارزميات.
https://stringfixer.com/ar/Commercial_National_Security_Algorithm_Suite

الأمن الكمي في المستقبل يُنجز. إذ يتضمَّن ذلك طلب إحاطة كاملة من البيت الأبيض للجان «الكونجرس» الرئيسة، جنباً إلى جنب مع الوكالات الفيدرالية الأخرى، حول تداعيات (NSM-8) على مستقبل أمَّتِنا السيبراني. سنحتاج في التحليل النهائي إلى نهج حكومي شامل للتعامل مع أخطر تهديد للأمن السيبراني لهذا الجيل -في الواقع-، وأكبر تهديد لهذا القرن.

وهذا فيه جانبٌ من الصِّحة لتنبيه القطاع الخاص خصوصاً، بما في ذلك قطاع الخدمات المالية وقطاع الشركات، إذ سيتطلَّب استبدال الأنظمة القائمة على (RSA) سنوات من العمل والتحديث المستمر، تقدر الدراسة الأولية التي أجريناها في مبادرة (Quantum Alliance Initiative)[3] أنَّ هجوماً كمياً على واحدة من أكبر خمس مؤسَّسات مالية في الولايات المتحدة الأمريكية يعطِّل الوصول إلى نظام الدفع (Fedwire Funds Service) من شأنه أن يتسبَّب بفشلٍ مالي متتالي، يكلِّف في أي مكان من (730 مليار دولار إلى 1.95 تريليون دولار). إذ قد يؤدي هجوم الكمبيوتر الكمومي إلى إضعاف ما يقرب من (60%) من إجمالي الأصول في النظام المصرفي؛ بسبب تدفقات البنوك وفخاخ السيولة الذاتية.

نظراً لحقيقة أنَّ الحكومة الفيدرالية تعترف أخيراً بأنَّ هذا يمثِّل تهديداً أمنياً خطيراً بما يكفي للمطالبة باتخاذ إجراء من جانب الوكالات في غضون الأشهر الخمسة المقبلة، فهذا هو السبب الإضافي الذي يجعل الصناعة الخاصة بحاجة إلى أخذ هذا التهديد على محمل الجد، والإصرار على أن تقوم واشنطن بتجميعها. وهذه هي خطة شاملة لحمايتنا جميعاً من هجوم كمي في المستقبل.

الرابط:

https://thehill.com/opinion/cybersecurity/594775-bidens-cybersecurity-order-opens-our-post-quantum-era

3 - تم إطلاق مبادرة التحالف الكمي في عام 8102، لتطوير ودعم السياسات التي تسمح للولايات المتحدة الامريكية وحلفائها بالفوز بالسباق على كمبيوتر كمي عالمي، مع العمل في نفس الوقت لضمان أن كلاهما سيكون في مأمن من هجوم إلكتروني كمي مستقبلي في غضون خمسة سنوات، منذ تأسيسها، أنشأت مبادرة التحالف الكمومي قيادة فكرية واضحة في هذا المجال الحاسم لتكنولوجيا المعلومات للقرن الحادي والعشرين.
https://www.hudson.org/policycenters/36-quantum-alliance-initiative