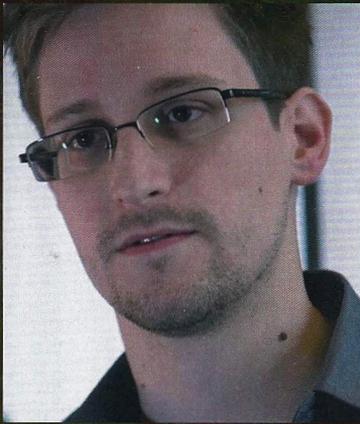


EE UU Y CHINA COMPITEN POR SER LOS PRIMEROS EN CONSTRUIR UNA DE ESTAS MÁQUINAS, CAPAZ DE ROBAR TODOS LOS SECRETOS DEL ADVERSARIO

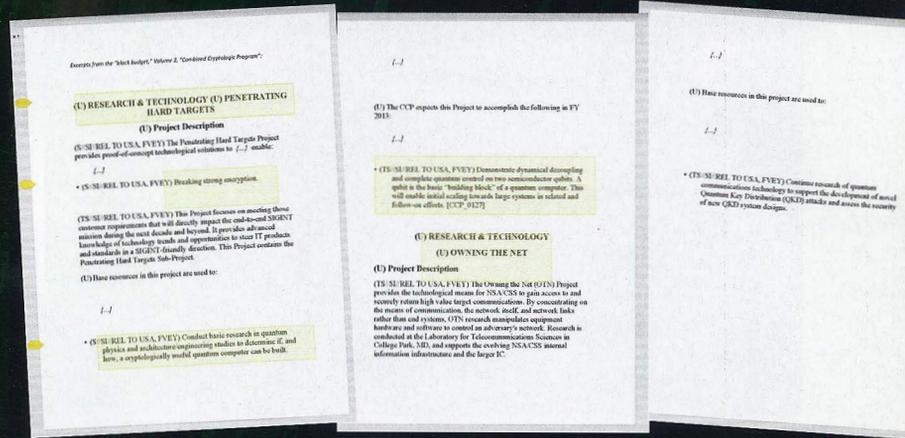
ORDENADORES CUÁNTICOS: EL ARMA TOTAL

TANTO EL GOBIERNO ESTADOUNIDENSE COMO EL CHINO ESTÁN GASTANDO INGENTES CANTIDADES DE DINERO PARA CONSTRUIR UN ORDENADOR CUÁNTICO ANTES QUE SU RIVAL, PUES ESTA MÁQUINA SERÍA CAPAZ DE ROMPER CUALQUIER SISTEMA DE ENCRYPTACIÓN EN UNOS SEGUNDOS. POR TANTO, EL PRIMERO EN FABRICAR UNA DE ESTAS COMPUTADORAS –UN ARTILUGIO QUE OPERARÍA TENIENDO EN CUENTA LOS SORPRENDENTES PRINCIPIOS DEL MUNDO SUBATÓMICO– PODRÍA ACCEDER A TODOS LOS SECRETOS DEL OTRO A GOLPE DE *CLICK*...

TEXTO JAVIER ARRIÉS



El analista de la NSA Edward Snowden (izquierda) filtró a varios medios de comunicación los documentos (dcha.) que mostraban la existencia de una masiva red de espionaje de las comunicaciones controlada por la inteligencia estadounidense.



El 9 de junio de 2013, el diario londinense *The Guardian* y el estadounidense *The Washington Post* publicaban sendas entrevistas que cayeron como un jarro de agua fría en las agencias de inteligencia y en los despachos gubernamentales, además de sembrar el estupor en la opinión pública. El protagonista, Edward Snowden, un joven que trabajaba como técnico y analista de la Agencia de Seguridad Nacional (NSA por sus siglas en inglés) de EE UU. Snowden filtró a ambos diarios documentos que demostraban la existencia de una compleja red de espionaje masivo controlada por la inteligencia estadounidense, destapando una realidad que hasta entonces todos los gobiernos negaban: estamos inmersos en una guerra silenciosa, una ciberguerra en la que el ciudadano medio es un inconsciente actor en manos de estamentos gubernamentales, militares y servicios secretos.

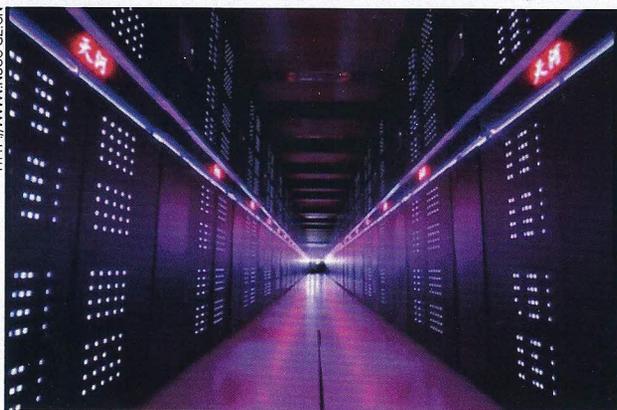
Ahora bien, los documentos de Snowden ponen de relieve que esta guerra secreta está a punto de alcanzar un nivel sólo comparable al de las obras más atrevidas de ciencia-ficción. Y es que tanto EE UU como China libran una feroz carrera para construir el primer ordenador cuántico de la historia, una verdadera revolución tecnológica que dará lugar a un nuevo paradigma en el mundo de la computación. Esta máquina, dotada con una potencia de cálculo impensable hoy en día,

sería capaz de romper cualquier sistema de seguridad actual y de capturar toda contraseña —incluidas, claro está, las de bancos e instituciones científicas y gubernamentales— en cuestión de minutos mediante un algoritmo, un método de cálculo que lleva el nombre de su desarrollador: el matemático Peter Shor. En definitiva, un ordenador cuántico podría descifrar todas las formas de codificación, incluso las de más alta seguridad, que se emplean para proteger secretos de Estado, transacciones financieras e información médica y de negocios. Además, tendría la capacidad de buscar información en bases de datos a velocidades inimaginables actualmente.

LO MÁS CERCANO A LA MAGIA

Pero, ¿cómo funciona un ordenador cuántico? Durante décadas, los componentes básicos de una computadora han ido reduciendo su tamaño hasta límites asombrosos. Sin embargo, cuando dichas piezas alcanzan escalas infinitesimales dejan de funcionar correctamente, ya que los electrones sufren el denominado efecto túnel, uno de los fenómenos más curiosos y misteriosos de la física cuántica. En el mundo de lo macroscópico en el que nos movemos, si lanzamos un objeto contra una pared, éste rebota. Pero en el universo microscópico, un electrón puede atravesar literalmente el canal por el que circula y aparecer en

HTTP://WWW.NISCC.GZ.CN



Tianhe-2

(izda.) es una computadora construida en China que está considerada la más rápida del mundo, superando incluso a la estadounidense *Cray Titan* (abajo).



otro que no debiera. De modo que el flujo de información podría ir por vías indebidas. No queda otra, por tanto, que abandonar la tecnología tradicional y empezar a aprovechar las características del mundo de lo ínfimamente pequeño, donde es reina y soberana la mecánica cuántica.

En los ordenadores actuales, la información se transmite a través de impulsos eléctricos. La unidad mínima de información es el bit, que sólo puede tomar dos estados, «0» ó «1», o empleando el símil de una bombilla, apagado o encendido. Sin embargo, en una computadora cuántica se utilizan los llamados bits cuánticos o qubits (quantum bits). La diferencia es que además de los dos estados descritos –«0» y «1»–, el qubit también puede encontrarse en una superposición cuántica de ambos estados. Con dos bits tradicionales podemos tener hasta cuatro valores posibles, y el conjunto de ambos sólo puede estar en uno de esos cuatro valores en cada momento. Pero

en el mundo cuántico las cosas cambian... Dos qubits pueden estar en cuatro estados ¡simultáneamente! Esto significa que podemos realizar cuatro operaciones a la vez, el sueño de todo analista informático. De modo que los qubits no sólo permitirán transferir cantidades mucho mayores de información sino, sobre todo, realizar numerosas operaciones al mismo tiempo.

Lo verdaderamente inquietante es que con toda probabilidad el ciudadano de a pie no podrá acceder a dicha tec-

D-Wade, lo más parecido a un ordenador cuántico, se encuentra en el Centro de Investigación Ames de la NASA (abajo).

nología, que sólo será utilizada por instituciones políticas y militares. Si ya somos víctimas de una vigilancia intensiva en medio de la vorágine tecnológica en la que vivimos, con el uso de ordenadores cuánticos por manos indebidas nuestra privacidad pelagra hasta un nivel insospechado.

LUCHA DE TITANES

Como apuntábamos, gracias a las filtraciones de Snowden ahora sabemos que la Agencia de Seguridad Nacional de EE UU (NSA) está trabajando en la construcción de una supercomputadora cuántica con la cual sería posible acceder a prácticamente todos nuestros datos. El proyecto forma parte del programa de investigación *Penetration Hard Targets* (Penetrando Objetivos Difíciles), un nombre que ya dice mucho sobre los objetivos del mismo. Este plan, que evidentemente alude a objetivos informáticos de difícil acceso y bien protegidos, cuenta con una financiación de 79,7 millones de dólares. La carrera por encon-





trar el **superordenador capaz de capturar cualquier clave** civil o militar ya está en marcha...

Pero China no se queda atrás. No en vano, técnicos del gigante asiático han construido la que de momento es la computadora más rápida del mundo, el *Tianhe-2*, también conocida como *Milky Way-2* o *TH2*, desbancando a la estadounidense *Cray Titan*. Pero *TH2* no deja de ser una máquina convencional. Lo que realmente preocupa a muchos gobiernos occidentales es que China también está invirtiendo grandes sumas de dinero para construir un superordenador cuántico que pondría en peligro las claves de bancos, instituciones, ejércitos, etc. Ya en 2010, un equipo de la Universidad de Ciencia y Tecnología de China sorprendió al mundo con una demostración de computación cuántica utilizando un átomo de nitrógeno en el interior de un diamante a temperatura ambiente.

El interés del Gobierno chino en conseguir el primer ordenador cuántico quedó bien patente



SECRETOS

de Estado altamente confidenciales estarán a merced del país u organización que logre fabricar el primer ordenador cuántico.

cuando en 2013 financió, a través de la Fundación Nacional de Ciencias Naturales de China, hasta 90 proyectos destinados a la investigación cuántica. Universidades, equipos de científicos y laboratorios militares están involucrados en una serie de iniciativas para lograrlo. Una de las más ambiciosas gira en torno a la construcción de un ordenador cuántico empleando materiales superconductores. Su principal responsable, Wang Haohua, físico de la Universidad de Zhejiang, aseguró que su Gobierno está tan interesado en construir el primero de la historia, que no repara en gastos para lograrlo. En palabras de Haohua, «el valor de la computadora cuántica para los militares y el Gobierno

es tan grande que su costo les parece irrelevante».

CHINA: GIGANTE CUÁNTICO

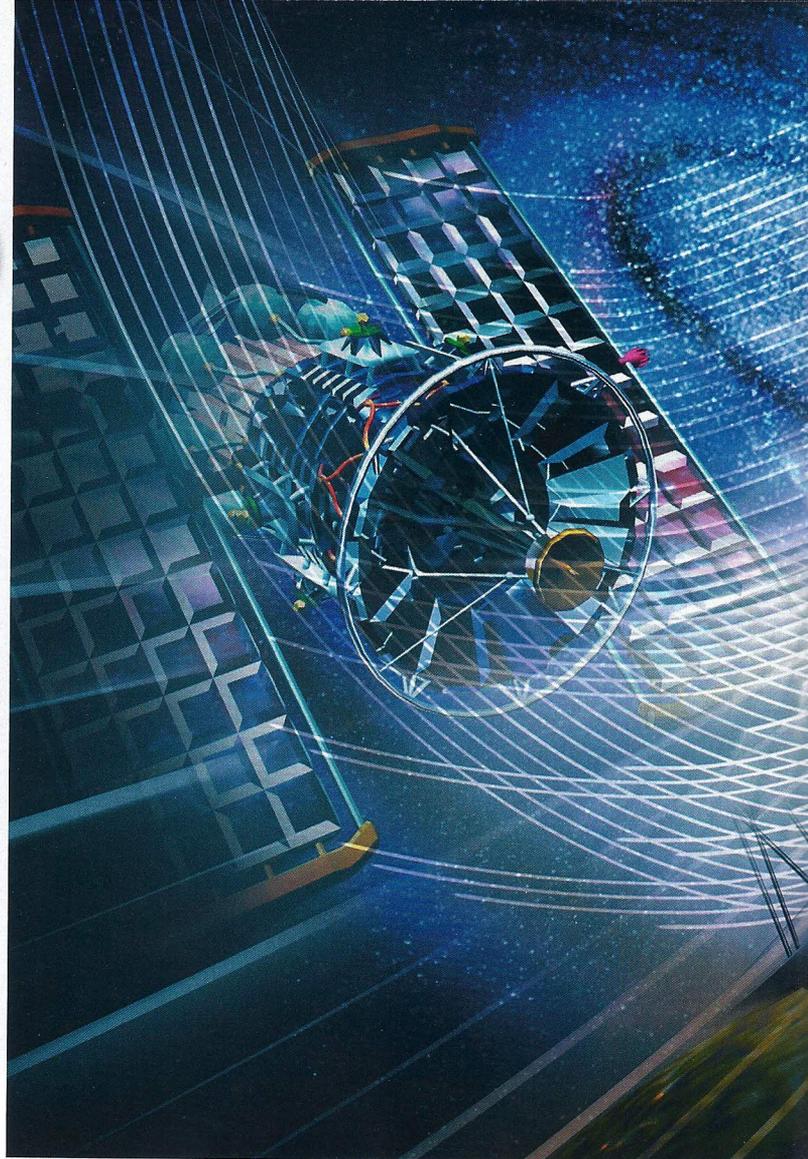
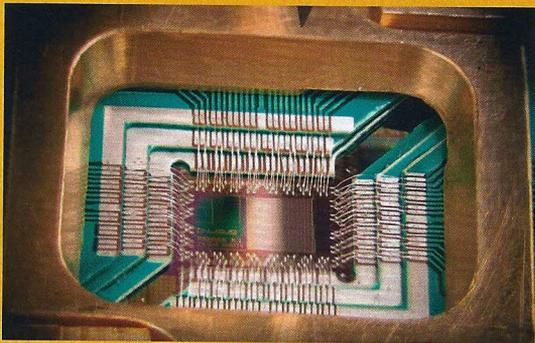
A primeros de enero de 2014, una turbadora noticia aparecida en el diario *South China Morning Post* ponía el dedo en la llaga, al mostrar que China está avanzando de manera firme en este terreno. Según el citado periódico, en la Instalación Experimental de Campos Magnéticos Estables de Alta Potencia, ubicada en un complejo de tres pisos en la isla de Hefei, se está investigando con la creación de campos magnéticos de gran intensidad –hasta 45 Teslas–, una proeza que sólo ha podido ser emulada en el Laboratorio Nacional de Potentes Campos Magnéticos de EE UU, la cual quedó registrada en el *Libro Guinness de los récords*. El complejo chino probablemente logrará superar los 45 Teslas.

El desarrollo de un campo magnético de esta intensidad y que pudiera ser mantenido de forma estable es, al parecer, una de las piezas clave en el

“Una computadora de esta clase sólo estará a disposición de ejércitos y servicios de espionaje”

¿SABÍAS QUÉ...?

La empresa canadiense *D-Wave Systems* anunció que había logrado fabricar un ordenador cuántico 5.000 veces más rápido que cualquiera convencional. La computadora fue adquirida en 2013 por *Google* y la *NASA* al precio de 15 millones de dólares. Está alojada en el Centro de Investigación Ames de la *NASA*, en California, en una sala casi a cero grados. No obstante, sus muchos detractores afirman que en realidad, aunque use qubits, el *D-Wave* utiliza un modelo clásico y por lo tanto no puede considerarse cuántico.



avance de la computación cuántica que se está desarrollando en China. El proyecto más avanzado lo lidera el Dr. Chen Hongwei, de la Academia de Ciencias China. De momento, Chen asegura que ya han obtenido resultados muy alentadores con imanes pequeños. Eso sí, reconoce que esta tecnología no estará disponible para el ciudadano de a pie. «Un ordenador cuántico que operase en un entorno tan extremo no tendría ningún uso comercial o personal... Pero los gobiernos pueden quererlo para fines especiales». ¿Qué fines especiales? Ahí está la cuestión. Su uso sería evidentemente militar, convirtiéndose en el arma fundamental de la ciberguerra, el conflicto en la sombra en el que vivimos inmersos sin ser conscientes de ello.

La creación de redes de espionaje propias en las que los ordenadores cuánticos serían las armas perfectas para penetrar en los sistemas gubernamentales, castrenses, científicos y financieros del enemigo, es el sueño de toda estrategia militar de cualquier país. En ese sentido, China ya está dando sus primeros pasos de gigante... Una noticia aparecida reciente-

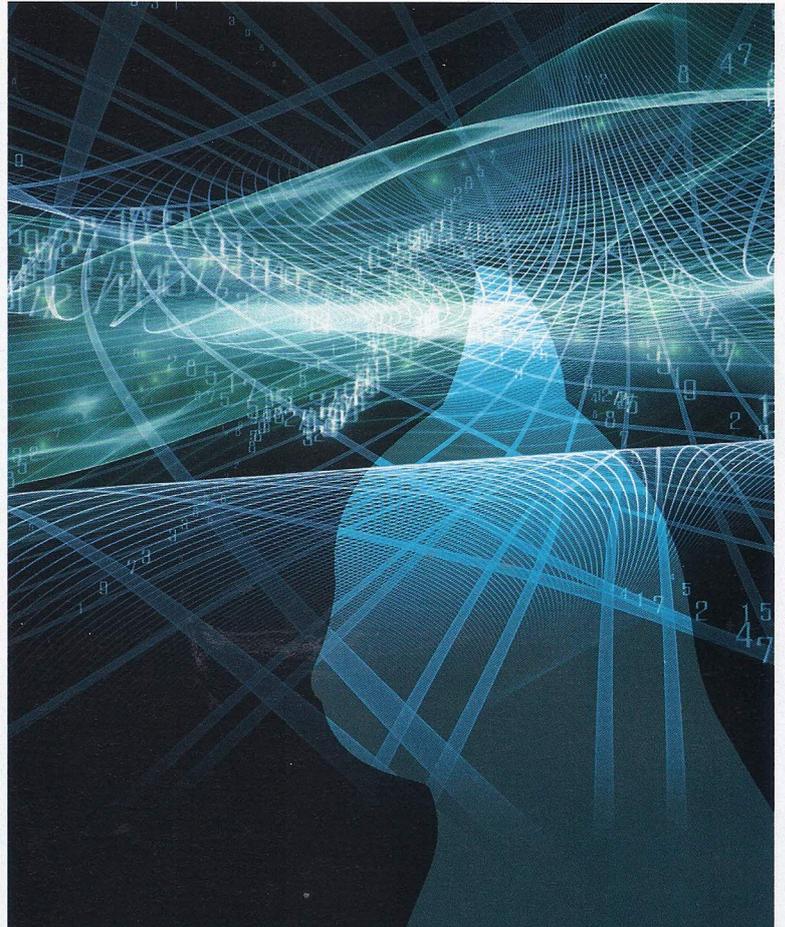
“Ningún sistema de encriptación sería obstáculo para un ordenador cuántico”



mente en el *South China Morning Post* asegura que el gigante asiático se va a embarcar en un ambicioso plan para crear una red de vigilancia mediante satélites –mucho mayor que las que poseen en estos momentos tanto EE UU como Europa–, la cual podría estar completamente operativa en dos años. Hasta 50 satélites de vigilancia serían puestos en órbita con un coste total de 20.000 millones de yuanes (más de 32.000 millones de dólares). Su red de satélites actual sólo abarca China y el área circundante, pero el nuevo proyecto ampliaría dicha cobertura a todo el planeta.

UNA RED PLANETARIA DE CIENCIA FICCIÓN

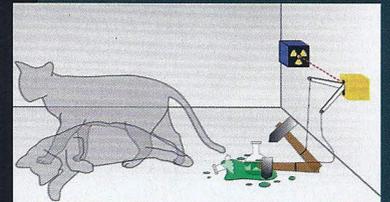
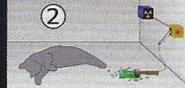
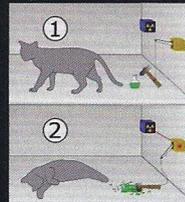
Aumentar la red de satélites implicaría también que China tendría que ampliar sus estaciones de tierra, tanto dentro como fuera de sus fronteras. Ahora cabe preguntarse qué ocurriría si los satélites chinos cubrieran



todo el planeta y los datos recogidos fueran tratados en un ordenador cuántico. Estaríamos ante una red de espionaje de una eficacia jamás vista. El escenario de los nuevos conflictos incluirá el ciberespionaje y la guerra electrónica. Las consecuencias serían seguramente una escalada de ciberataques entre naciones y organizaciones que incluirían a EE UU, China y Rusia, además de potencias emergentes como la India, Brasil e incluso naciones islámicas.

La mayoría de los ciudadanos desconoce que sus datos, sus movimientos, su vida, lo que piensan o lo que hacen, su privacidad en suma, es cada vez más frágil, hasta el punto de que pronto ninguna clave —personal, bancaria, sanitaria, de nuestro correo o de las redes sociales a las que accedemos a diario— ni ningún sistema de encriptación que utilicemos estarán a salvo de la potencia de un ordenador cuántico... ■

Los planes de China son construir una red mundial de satélites, cuyos datos serán analizados por ordenadores cuánticos.



EL ESCURRIDIZO GATO DE SCHRÖDINGER

La superposición cuántica, tan necesaria para que funcione una computadora cuántica, fue expuesta en un experimento teórico creado por el físico austriaco Erwin Schrödinger. Imaginemos un gato encerrado en una caja en la que hay una botella de veneno y un dispositivo que se activa si se desintegra una partícula radioactiva que hay en su interior. Ahora bien, hay un 50% de posibilidades de que la partícula se desintegre y, por lo tanto, la mitad de probabilidades de que el minino sobreviva al experimento o no. Así ocurre en el mundo microscópico regido por la física clásica, porque en la física cuántica nuestro hipotético gato cuántico estará en una «superposición de estados» compuesta de

los estados «vivo» y «muerto». Sólo cuando abramos la caja, el sistema compuesto por el gato pasará a estar o vivo o definitivamente muerto. En suma, es la observación, la interacción con el sistema formado por la caja y su contenido, la que determina el «colapso» en un sentido u otro de esa «situación múltiple», pero hasta que no se abra la caja el gato permanece en ese «estado superpuesto». Algo así sucede con las partículas subatómicas, que se encuentran en todo el universo a la vez, como si fueran ondas de dimensiones infinitas. Sólo se «colapsan», convirtiéndose en partículas y dando forma a nuestra realidad tridimensional, cuando una conciencia las observa.