

La Carrera por la Supremacía Cuántica

Los últimos desarrollos tecnológicos han consolidado los inicios de la computación cuántica, una tecnología que se distingue de la computación comúnmente entendida, por su uso de principios del mundo subatómico. Estas tecnologías podrían llevar a la rápida solución de tareas complejas, generando alarma por las posibles aplicaciones de estos computadores en materias de defensa. El desarrollo de estos computadores era hasta hace poco solo una teoría, pero con la presentación del primer computador cuántico con 50 Qubits en 2017, por IBM, ha empezado una carrera por generar computadores con más Qubits, y, por tanto, con mayores capacidades de cómputo. Ello ha llevado, a su vez, a una carrera entre las potencias para obtener usos prácticos, y controlar estos nuevos ingenios de manera pionera, consiguiendo la denominada “supremacía cuántica”.

Los impactos de esta tecnología son variados, por cuanto pueden llevar a la obsolescencia de tecnologías actualmente usadas, como la tecnología de sigilo de radar, las telecomunicaciones seguras, o mejorar la inteligencia artificial a niveles nunca antes vistos.



Computador cuántico Sycamore, de 53 Qubits, fabricado por Google en 2019, instalado en su laboratorio Goleta, en California. Fuente: Erik Lucero, vía Google.

Uso de las tecnologías cuánticas

La diferencia sustancial de esta nueva lógica, con respecto a la computación “tradicional”, radica en la aplicabilidad del “Principio de Incertidumbre”. Este principio implica que las partículas pueden estar en varios estados físicos simultáneamente. Esto en la computación se logra con los llamados Qubits, bits informáticos que se encuentran en ambos estados posibles (0 o 1) al mismo tiempo, lo que permite elevar la capacidad de procesamiento de manera exponencial, ya que el Qubit realizará todos los cálculos posibles al mismo tiempo, a diferencia de un bit normal que debe emplearse de manera secuencial y lineal.

Otro principio de importancia a nivel cuántico es el fenómeno del entrelazamiento, consistente en la vinculación de dos o más Qubits, de tal manera que los cambios realizados en uno impliquen la modificación de su par enlazado, sin importar la distancia que los separe. Esto lleva a una velocidad de transmisión de información casi instantánea, superando a cualquier sistema de transferencia de información físico, cableado o inalámbrico.

La literatura ha definido, por lo menos, tres vertientes principales para los usos de los ordenadores cuánticos, siendo estos: la computación, los sensores, y la comunicación cuántica.

La computación cuántica permitiría incrementar los poderes de cómputo, que superarían a los mejores supercomputadores actuales. El principal impacto para la seguridad se verá en el desarrollo de la criptografía, basada en operaciones matemáticas de difícil cálculo para los ordenadores normales, tardando varios años en poder descifrar las encrypciones. Por esto, las capacidades de

un ordenador cuántico de solucionar estas tareas en cortos periodos, de unas horas o minutos, haría prácticamente inútil cualquier intento de cifrado y encriptado usado en la actualidad, creando enormes vulnerabilidades de ciberseguridad a los gobiernos y grandes empresas, pues sus arquitecturas de ciberseguridad se volverían fácilmente hackeables.

Otra utilidad futura de la computación cuántica está en el desarrollo de simuladores del mundo físico, que podrían dar lugar a modelos más eficientes y rápidos de simular los impactos sobre nuevos materiales y modelos de construcción. Esto podría revolucionar los procesos de diseño de aeronaves y otros vehículos, acelerando su desarrollo de manera exponencial, así como medir sus capacidades teóricas con alta exactitud, evitando costosos procesos de diseño.

El segundo elemento, los sensores cuánticos, aprovecharían efectos subatómicos, para generar sistemas de medición que sobrepasen en sensibilidad y rapidez a los sistemas actuales. “En cuanto los átomos se enfrían hasta una millonésima de grado por encima del cero absoluto, se convierten en partículas detectoras perfectas para sensores cuánticos. Se ha demostrado la detección de tiempo, gravedad, rotación y campo magnético en el laboratorio con precisiones de récord”, explica el profesor Kai Bongs de la Universidad de Birmingham (Reino Unido) y coordinador de proyecto ISENSE. Por ejemplo, se puede crear sistemas de radar de amplio alcance, con alta resistencia a interferencias, que invaliden las capacidades de sigilo de vehículos modernos. Otro uso importante sería en la generación de sistemas de navegación predictivos, que podrían manejar sistemas, como aeronaves no tripuladas, con altísima precisión, inclusive sin necesidad de conexión por GPS, u otros sistemas de posicionamiento satelital.

En tercer lugar, las comunicaciones cuánticas posibilitarían una segunda revolución de las comunicaciones, pues darían lugar a la creación de redes de información más seguras y rápidas. Esto, unido a infraestructuras específicas, como constelaciones satelitales cuánticas, podría dar lugar a un nuevo Internet cuántico, con velocidades de interconexión y seguridad sin precedentes. Asimismo, estos sistemas darían lugar a comunicaciones militares más seguras ante las interferencias, dando mayor seguridad futura a las capacidades 4C (comando, control, computadores y comunicaciones) a nivel operativo.

Carrera entre potencias

Estas tecnologías se encuentran en una intensa investigación para corroborar su viabilidad, siendo China y los Estados Unidos los países más adelantados, además de otros actores con crecientes inversiones en el área. Entre algunas de estas se pueden contar: Alemania, Australia, Canadá, Corea del Sur, Francia, el Reino Unido, Japón, Rusia y los Países Bajos. Todos estos países ya han generado planes estratégicos nacionales, con participación público-privada, destinados al desarrollo de la computación cuántica para sus usos estratégicos nacionales, tanto en defensa como en otras instancias. Al 2022 se estima, a nivel global, una inversión de 30 mil millones de dólares para el desarrollo del sector, según la compañía de capacitaciones en la industria cuántica QURECA.

De los actores mencionados, China se encuentra a la cabeza del desarrollo de tecnologías de comunicación y sensores cuánticos, creando, en 2016, su primer sistema de comunicaciones encriptadas entre las ciudades de Beijing, Shanghái, Hebei y Jinan. Además, el país cuenta con los primeros elementos de computación cuántica satelital, con el proyecto de Experimentos Cuánticos a Escala Espacial (QUESS) y su primer satélite de este programa, Micius (o Mozi), ayudando a la interconexión entre las ciudades ya

BOLETÍN INFORMATIVO Y DE ANÁLISIS N° 16-2022 Santiago, 30 de mayo de 2022, Hoja N° 2

mencionadas, en una red terrestre-espacial. Además, China generó el primer link de comunicaciones cuántico a nivel intercontinental, con la ayuda de la Academia de Ciencias de Austria en 2016. Beijing espera expandir esta red de comunicaciones por medio de una mega constelación satelital, creando primero una conexión con Europa, y generar una red global para el 2030. China, además, está investigando sobre el uso de radares y sensores cuánticos más resistentes a las interferencias, los cuales, si resultan efectivos, podrían inutilizar la ventaja americana de tecnologías de sigilo al radar, como los presentes en sus aviones F-35 Lightning II, pero de momento, estos sistemas aún no han probado su funcionalidad en todos los ambientes.

En el caso de Estados Unidos, se han empezado a dirigir grandes esfuerzos en esta área, con la *National Quantum Initiative* (NQI) de 2018, a cargo de la Fundación Nacional de Ciencias y el Departamento de Energía, buscando la creación de un sistema de 3 pilares para el desarrollo cuántico, a decir, con la comunidad civil, militar, y los servicios de inteligencia, en relación a la naturaleza de uso dual de estas tecnologías (civil y militar). Washington cuenta además con la cooperación de las empresas tecnológicas con más experiencia en el área, como IBM y Google. Ambas compañías esperan crear computadores cuánticos con miles de Qubits en la presente década, para posteriormente expandirlos a millones de Qubits. Con esto, EEUU tiene en la actualidad una importante ventaja frente al resto del mundo en esta materia.

La NQI llevó a la creación de la *National Quantum Coordination Office* (NQCO), que busca impulsar múltiples iniciativas y centros de estudios, enfocados en la computación cuántica. Además, el Acta de Autorización de Defensa de 2020, permite al Departamento de Defensa ayudar a la creación de centros de estudios, con instituciones de investigación de la Armada y la Fuerza Aérea cooperando activamente con otros actores públicos y privados.

En el plano internacional, EE.UU. también ha mostrado iniciativa de coordinar sus esfuerzos con aliados cercanos, firmando memorándums de cooperación con Japón en 2019; el Reino Unido y Australia en 2021; y Finlandia y Suecia en 2022. Estos países han mantenido esfuerzos individuales para mejorar sus avances en este ámbito, principalmente fomentando sus empresas privadas que utilicen esta emergente tecnología. Esto además se relaciona con las nuevas iniciativas de la alianza militar de la Organización del Tratado del Atlántico Norte (OTAN), para la incorporación de tecnologías emergentes y disruptivas con posibles usos de defensa, entre las que se encuentran las tecnologías cuánticas. Esto ha llevado a la OTAN a establecer una estrategia común en 2021, y crear un centro de investigación cuántica en Dinamarca en 2022.

El tercer actor con desarrollos en el área es la Unión Europea (UE), siendo Alemania, Francia y Países Bajos sus integrantes con mayores desarrollos de esta tecnología, por lo menos en términos de inversión monetaria. En 2018 se crea la iniciativa *Quantum Technology Flagship*, que espera crear una sinergia entre actores privados y públicos, para una creciente industria cuántica, la cual ha visto un incremento de inversiones de 2 mil millones de dólares desde 2015. También, se ha iniciado el *European High Performance Computing Joint Undertaking*, que planea crear una serie de supercomputadoras cuánticas para 2023, conectándose a su red existente de supercomputadoras tradicionales, generando un sistema híbrido, que permita mejores tareas de simulación e investigación en múltiples áreas. Otro proyecto en desarrollo es el *European Quantum Communications Infrastructure* (EuroQCI), desde 2019. Este busca crear la infraestructura de una red de comunicaciones aseguradas cuánticamente, para toda el área europea, en cooperación con la Agencia Espacial Europea.

Además de esto, muchos países miembros de la UE han presentado avances en el área de manera individual, producto de una gran trayectoria de investigaciones desde la década pasada. Por ejemplo, Alemania ha presentado su propia estrategia nacional cuántica en 2018, la denominada *Roadmap Quantum computing*, enfocada en el desarrollo de hubs regionales involucrando a universidades, empresas y el gobierno germano, con una inversión estimada en 2.6 mil millones de euros al 2022. Esto ha llevado a proyectos como la puesta en marcha de su primer ordenador cuántico comercial en 2021, en conjunto con IBM.

Francia, ha hecho lo mismo con el desarrollo de un plan cuántico estratégico en 2020, y la inversión de 1.8 mil millones de euros en la industria cuántica hasta 2025. Autoridades como la ministra de defensa francesa, Florence Parly, han mencionado la importancia de los futuros sistemas cuánticos en la seguridad del país gallo, manteniendo que los futuros sistemas de navegación y guiado con tecnologías cuánticas serán necesarios en el futuro.

Los Países Bajos también han enfocado esfuerzos, emprendiendo un plan estratégico hacia una industria nacional en 2019, desarrollando un marco de cooperación mediante la iniciativa *Quantum Delta NL*, con una inversión inicial de 615 millones de euros. Actualmente, el país ocupa el tercer lugar a nivel mundial por investigaciones y patentes en computación cuántica, especialmente en las áreas de criptografía y comunicaciones.



El computador cuántico Q System One de IBM, de 20 Qubits, el primer ordenador de su tipo en Alemania, presentado en 2021. Fuente: Ross Franklin, vía Deutsche Welle.

Las tecnologías cuánticas aún se encuentran en sus primeros experimentos para ser una alternativa computacional viable, pero sus posibles impactos, en términos de nuevos inventos y la obsolescencia de los métodos criptográficos, la han vuelto un interés estratégico para múltiples actores, llevando a crecientes inversiones en el área, con grandes impactos en las futuras capacidades de defensa nacional de los países con altas inversiones en esta área.

Finalmente, el desarrollo de esta tecnología de uso civil-militar, generará una importante ventaja estratégica de las capacidades de defensa frente a nuevas amenazas, como los impactos sobre la ciberseguridad global, producto de la supremacía cuántica. Los impactos en múltiples áreas de la defensa llevarán a una moderna carrera armamentística, como la generación de comunicaciones más rápidas y seguras; ayudando en el diseño de nuevos vehículos de combate y sus subsistemas; o la creación de nuevos ingenios militares. En definitiva, a pesar de las dificultades tecnológicas de la adopción masiva de estos inventos, los próximos años serán capitales para la expansión y consolidación de esta revolución tecnológica.

BAS