

# La OTAN impulsa la primera estrategia cuántica de su historia

Dr. Raúl José Martín Palma

Catedrático de Física Aplicada. Universidad Autónoma de Madrid

**A** principios del pasado año la OTAN hacía público un resumen de su estrategia en el área de las tecnologías cuánticas, ya que se considera que pueden tener un importante impacto en la seguridad y la defensa. El objetivo fundamental de la citada estrategia, aprobada por los ministros de Asuntos Exteriores de la OTAN el 28 de noviembre de 2023, es garantizar que la Alianza esté «cuánticamente preparada» (*Quantum-ready*, según la terminología empleada).

El resumen publicado por la Alianza asume como postulado básico que los avances que se están produciendo en las tecnologías cuánticas nos están acercando progresivamente a un profundo cambio tecnocientífico que tendrá implicaciones de largo alcance en nuestras economías, seguridad y defensa. Por tanto, la OTAN considera que dichas tecnologías constituyen un elemento clave de competencia estratégica, por lo que resulta imprescindible estar al tanto de los avances que puedan producirse en este campo y, lógicamente, tomar la delantera.

De forma específica, el citado resumen identifica una serie de áreas en las que podrían producirse cambios drásticos en lo relativo a la seguridad y la defensa. Son las siguientes: detección; posicionamiento, navegación y sincronización; imagen; comunicación y ciencias de la información; computación, modelización y simulación. En los siguientes apartados se describen brevemente. Veremos que los avances alcanzados en algunas de ellas son muy destacables, mientras que otras están prácticamente en una fase de exploración.

## DETECCIÓN

Los sensores cuánticos aprovechan la naturaleza cuántica de la luz y de la materia para determinar, con enorme precisión, diversas magnitudes físicas. Estos dispositivos están caracterizados por su capacidad para realizar medidas a escalas atómicas, de forma que son mucho más precisos. Así, utilizando exiguas cantidades de materia y energía, los sensores cuánticos pueden detectar y medir cambios minúsculos en magnitudes tales como el tiempo, la gravedad, la temperatura, la presión, la rotación, la aceleración, la frecuencia o los campos magnéticos y eléctricos. Es de destacar que los sensores cuánticos presentan una mayor inmunidad frente a las interferencias que sus equivalentes clásicos. En la actualidad, las técnicas más prometedoras para el desarrollo de detectores cuánticos son la interferometría atómica mediante átomos ultrafríos, los circuitos superconductores, las trampas iónicas y los centros nitrógeno-vacante en diamante.

Lógicamente, una precisa determinación de muy variados parámetros físicos tiene un gran potencial de aplicación en el área de la

**Se considera que las tecnologías cuánticas pueden tener un importante impacto en la seguridad y la defensa**



seguridad y la defensa. A modo de ejemplo, podrían desarrollarse sensores cuánticos magnéticos, acústicos y de gravedad optimizados para la guerra antisubmarina. También se ha propuesto el desarrollo de sensores cuánticos aerotransportados y espaciales de baja potencia y muy alta sensibilidad. Serían útiles para la detección táctica (corto alcance, activa/pasiva, encubierta, utilización de frecuencias visible/IR/THz/RF) para inteligencia, vigilancia, selección de objetivos y reconocimiento (ISTAR), así como para la vigilancia estratégica (marítima de largo alcance, espacio aéreo, espacial).

### **POSICIONAMIENTO, NAVEGACIÓN Y SINCRONIZACIÓN**

Relacionado con lo anterior, el desarrollo de instrumentos de medida de muy alta sensibilidad basados en la explotación de efectos cuánticos puede conducir a una significativa mejora de los actuales sistemas de posicionamiento, navegación y sincronización. Los sistemas globales de navegación por satélite (GPS, GLONASS, IRNSS, *Galileo* y *BeiDou*) basan su funcionamiento en una muy precisa sincronización de múltiples relojes atómicos a bordo de satélites, que son corregidos por relojes atómicos más estables posicionados en bases terrestres. Así, un aumento de la precisión de los relojes cuánticos mejorará la precisión del posicionamiento y la navegación.

Unas tecnologías de posicionamiento, navegación y sincronización mejoradas permitirán llevar a cabo operaciones en entornos operativos complejos, como operaciones autónomas de larga duración bajo el agua o bajo tierra, o incluso en áreas denegadas para sistemas de posicionamiento global.

### **ADQUISICIÓN DE IMAGEN**

Los sistemas cuánticos para la adquisición de imágenes abarcan una extensa panoplia de dispositivos que van desde cámaras tridimensionales a radares, pasando por dispositivos LiDAR (*Light Detection and Ranging*). La imagen cuántica puede considerarse un subcampo de la óptica cuántica, disciplina que se ocupa de la explotación de las correlaciones entre fotones. El objetivo perseguido sería la completa supresión del ruido y el aumento de la resolución del objeto cuya imagen se pretende adquirir. Los protocolos para la obtención de imágenes cuánticas tendrían aplicación en el desarrollo de radares cuánticos, la detección de objetos en entornos «ópticamente impermeables» y en la adquisición de imágenes médicas.

De forma específica, un radar cuántico funciona de manera similar a uno clásico. Es decir, se envía una señal hacia el objetivo y el sistema de radar se encarga de adquirir y procesar la señal reflejada. Sin embargo, utilizando una aproximación basada en mecánica cuántica sería posible, al menos teóricamente, lograr una precisión mejorada y nuevas capacidades. Aunque ninguno de ellos es perfecto, existen diversos protocolos desarrollados como el radar cuántico interferométrico, la iluminación cuántica, el radar cuántico híbrido o el radar cuántico *Maccone-Ren*.

### **COMUNICACIÓN Y CIENCIAS DE LA INFORMACIÓN**

La comunicación cuántica puede ser definida como el intercambio de información a través de una red cuántica. Los canales de transmisión habituales son el espacio libre o fibra óptica y, por lo



general, el fotón es el portador de la información cuántica que desea transmitirse. Desde un punto de vista práctico, sin embargo, la red cuántica debe contener otros elementos como repetidores o interruptores cuánticos para evitar las pérdidas que se producen en transmisiones a grandes distancias. Desde un punto de vista físico, la comunicación cuántica está basada en el fenómeno del entrelazamiento cuántico, el principio de incertidumbre de Heisenberg y el teorema de no clonación. Ésta última es una característica clave en la comunicación, ya que establece que la información cuántica no puede ser copiada.

Una característica fundamental de la comunicación es el encriptado de la información transmitida. En este sentido, la criptografía cuántica ofrece la posibilidad de sustituir los esquemas de cifrado convencionales por métodos de comunicación seguros como la distribución de claves cuánticas. Ésta es, en nuestros días, la aplicación práctica más madura dentro del campo de la comunicación cuántica. La propiedad única y crucial de la distribución de claves cuánticas es la capacidad que proporciona a dos usuarios para detectar la presencia de un tercero que intente obtener de forma ilícita la clave utilizada. Esta característica hunde sus raíces en una propiedad fundamental de la mecánica cuántica: el proceso de medir un sistema cuántico produce una perturbación en el sistema. Por tanto, un tercero que intente «escuchar» la clave debe medirla de alguna manera, lo que introducirá anomalías detectables en la señal transmitida.

El desarrollo de sistemas criptográficos indescifrables y la capacidad de descifrar mensajes codificados utilizando los métodos criptográficos actuales llevarán a importantes desafíos para los sistemas C4ISR actuales.

## COMPUTACIÓN, MODELIZACIÓN Y SIMULACIÓN

La computación cuántica está basada en la utilización de información cuántica para realizar cálculos. Es bien sabido que la unidad elemental de medida de información «clásica» es el bit, que sólo puede tomar los valores 0 o 1. Sin embargo, el portador elemental de información cuántica es el bit cuántico o qubit (del inglés *quantum bit*). Un qubit puede estar en dos estados o niveles habitualmente denominados  $|0\rangle$  y  $|1\rangle$ . Por ejemplo, el espín de un electrón puede encontrarse en los estados «hacia arriba» o «hacia abajo». Otro ejemplo lo constituye la polarización de un fotón, cuyos estados serían «polarización vertical» y «polarización horizontal». Sin embargo, y aquí reside la importancia de la computación cuántica, un qubit también podría estar en un estado que sea una combinación lineal compleja de los estados  $|0\rangle$  y  $|1\rangle$ . Esta característica se conoce como superposición cuántica.

El enorme interés actual en el desarrollo de ordenadores cuánticos viene dado por la posibilidad de aumentar las capacidades de computación en varios órdenes de magnitud. Sin embargo, no se prevé que lleguen a sustituir completamente a los ordenadores clásicos. De cualquier manera, la computación cuántica permitirá

superar el límite teórico de los ordenadores de diseño clásico para acometer problemas analíticos específicos, por ejemplo, llevando a cabo tareas de optimización y simulación. Adicionalmente, la implementación de técnicas de modelado y simulación sofisticadas permitirá la toma de decisiones operativas y organizacionales complejas de forma más eficiente. La computación cuántica también habilitaría nuevas formas de desarrollar materiales avanzados, fármacos y biotecnologías. Contribuiría, por otra parte, al desarrollo de inteligencia artificial de próxima generación, por ejemplo, a través de uso de redes neuronales cuánticas para la identificación de imágenes y objetivos.

### LA VISIÓN DE LA ALIANZA

En este contexto, la OTAN plantea fomentar el desarrollo de un denominado «ecosistema cuántico» seguro, resiliente y competitivo. Éste debería ser capaz de responder al rápido ritmo de evolución de la tecnología en la industria cuántica. Es, por tanto, imprescindible el desarrollo y la implementación de las tecnologías críticas habilitadoras que permitan avanzar en este campo. Para conseguir lo anterior será necesario fomentar la cooperación entre los países aliados en oportunidades de desarrollo tecnológico y en la protección de la fuerza laboral cualificada. También es clave llevar a cabo un eficiente intercambio de información. Lógicamente, cobra gran importancia la disuasión y la defensa de los sistemas y redes propios frente a ataques cuánticos o de cualquier otro tipo.

De forma específica, se propone avanzar hacia los siguientes hitos:

- Identificación de las aplicaciones, experimentos e integración de tecnologías cuánticas militares y de doble uso más prometedoras que cumplan con los requisitos de planificación de defensa y desarrollo de capacidades.
- Desarrollo, adopción e implementación de marcos, políticas y estándares, tanto para software como para hardware, que lleven a una mejora de la interoperabilidad.
- Cooperación en el desarrollo de tecnologías cuánticas para mantener la ventaja tecnológica de la OTAN y las capacidades de los aliados.
- Identificación, comprensión y capitalización de los avances en evolución de las tecnologías cuánticas, incluso con tecnologías habilitadoras y en convergencia con otras tecnologías emergentes y disruptivas.

- Desarrollo de una «comunidad cuántica» que colabore estratégicamente con gobiernos, industria y mundo académico de todos los «ecosistemas de innovación» de la OTAN.

- Transición de los sistemas criptográficos a una criptografía cuántica segura.

- Actualización y ejecución dinámica de las estrategias, políticas y planes de acción cuánticos pertinentes.

- Toma de conciencia y actuación de los países aliados encaminadas a prevenir, voluntariamente, las inversiones e interferencias adversas en los «ecosistemas cuánticos» propios. Esta medida puede incluir el examen de las cadenas de suministro relevantes a nivel nacional.

**Estas tecnologías tienen potencial para ofrecer nuevas capacidades, por lo que hay que estar alerta a los avances**

Dentro de este contexto, es de destacar que las líneas de actuación definidas por el Ministerio de Defensa en el documento «Estrategia de Tecnología e Innovación para la Defensa» (actualizado en 2020) coinciden con muchas de las que la OTAN incluye en su visión estratégica. En particular, dentro de las tecnologías emergentes con potencial aplicación futura a la defensa, se incluyen la computación cuántica, la comunicación e información cuántica, los sensores y la metrología cuántica, además de la simulación cuántica. España ya había hecho los deberes.

### CONCLUSIONES

Es cierto que las tecnologías cuánticas tienen un enorme potencial para ofrecer nuevas capacidades, motivo por el cual hay siempre que estar alerta a cualquier avance en este área. Pero tampoco deben sobrestimarse sus capacidades. La que se ha denominado «primera revolución cuántica» llevó al desarrollo de tecnologías que hoy son tan conocidas como la energía nuclear, el transistor, los láseres, las imágenes por resonancia magnética o las cámaras digitales. También a la fabricación de armas nucleares. Sin embargo, no se espera que en el marco de esta «segunda revolución cuántica» sean creadas nuevas armas. Esta nueva revolución estaría principalmente caracterizada por alcanzar un elevado grado de manipulación y control de sistemas cuánticos individuales. La mayoría de los dispositivos cuánticos que actualmente están en fase de estudio o desarrollo caen en la categoría de tecnologías de doble uso. Por este motivo somos testigos en la actualidad de una muy intensa actividad de investigación y desarrollo en el área de las tecnologías cuánticas. De hecho, desde los sectores público y privado se están invirtiendo enormes cantidades de recursos económicos.