

Tecnología Cuántica, Paz y Seguridad: Manual Básico

Zhanna L. Malekos Smith y Giacomo Persi Paoli

Agradecimientos

El apoyo de los patrocinadores principales del UNIDIR proporciona los cimientos de todas las actividades del Instituto. Esta publicación ha sido financiada por la Unión Europea en el marco del Programa de Seguridad y Tecnología del UNIDIR, que también cuenta con el apoyo de los Gobiernos de Alemania, Chequia, Francia, Italia, Noruega, los Países Bajos y Suiza, así como de Microsoft.

Merecen un agradecimiento especial el Dr. Irving Lachow y el Prof. Andrew Reddie de la Universidad de California, Berkeley, así como el diligente equipo de ayudantes de investigación de West Point, la Academia Militar de los Estados Unidos: la teniente primera Christina Huynh y los cadetes Jason Ingersoll, Christopher T. Konin, Conner R. Leggett y Riley Hoyes.

Sobre el UNIDIR

El Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) es un instituto autónomo de las Naciones Unidas financiado con contribuciones voluntarias. UNIDIR, uno de los pocos institutos de políticas del mundo dedicado al desarme, genera conocimientos y promueve el diálogo y medidas en materia de desarme y seguridad. Tiene su sede en Ginebra, y ayuda a la comunidad internacional a desarrollar las ideas prácticas e innovadoras necesarias para hallar soluciones a problemas críticos para la seguridad.

Nota

Las denominaciones empleadas en esta publicación y la forma en que aparecen presentados los datos que contiene no implican, de parte de la Secretaría de las Naciones Unidas, juicio alguno sobre la condición jurídica de países, territorios, ciudades o zonas, o de sus autoridades, ni respecto de la delimitación de sus fronteras o límites. Las opiniones expresadas en la presente publicación son responsabilidad exclusiva de sus autores. No reflejan necesariamente las opiniones de las Naciones Unidas, de UNIDIR o de la Unión Europea, así como tampoco de sus funcionarios o patrocinadores.

Citación

Malekos Smith, Zhanna L. y Persi Paoli, Giacomo. "Tecnología cuántica, paz y seguridad: manual básico". Ginebra, Suiza: UNIDIR, 2024.

Sobre los autores



Zhanna L. Malekos Smith JD es investigadora visitante en UNIDIR y profesora de Derecho Internacional en el Instituto de las Naciones Unidas para Formación Profesional e Investigaciones (UNITAR). Además, es investigadora superior adjunta del Proyecto de Seguridad Aeroespacial y del Centro para Estudios Estratégicos e Internacionales (CSIS) de Washington DC, investigadora visitante del Consejo Carnegie de Ética y Asuntos Internacionales e investigadora en el Instituto Cibernético del Ejército en la Academia Militar estadounidense de West Point. Anteriormente, Malekos Smith fue profesora adjunta en el Departamento de Ingeniería de Sistemas de West Point y profesora de Estudios sobre Ciber guerra en la Escuela de Guerra Aérea de los Estados Unidos. Ha sido capitana y abogada de la Abogacía General de las Fuerzas Aéreas de los Estados Unidos, y fue asignada al programa del Cuerpo de Entrenamiento de Oficiales de la Reserva (ROTC) del Instituto Tecnológico de Massachusetts. Las opiniones expresadas en el presente documento son exclusivamente las de la autora y no las de las Naciones Unidas, el Gobierno de los Estados Unidos o el Departamento de Defensa de los Estados Unidos.



El Dr. Giacomo Persi Paoli es Director del Programa de Seguridad y Tecnología del UNIDIR. Su experiencia abarca el ámbito de la ciencia y la tecnología y, muy en particular, las implicaciones de las tecnologías emergentes para la seguridad y la defensa. Antes de incorporarse al UNIDIR, Giacomo fue Director Asociado de RAND Europe, donde dirigió la cartera de ciencia, tecnología e innovación en defensa y seguridad y estuvo al frente del Centro de Estudios de Futuro y Prospectiva de RAND. Es Doctor en Economía por la Universidad de Roma (Italia) y posee un Máster en Ciencias Políticas por la Universidad de Pisa (Italia).

Abreviaturas y acrónimos

IA	Inteligencia artificial
SAA	Sistema de armas autónomo
SAD	Sistema de Apoyo a las Decisiones
GNSS	Sistema mundial de navegación por satélite
TIC	Tecnología de la información y las comunicaciones
ISR	Inteligencia, vigilancia y reconocimiento
GTCA	Grupo de trabajo de composición abierta
PQC	Criptografía poscuántica
QKD	Distribución cuántica de claves
SQUID	Dispositivo superconductor de interferencia cuántica

Índice

Agradecimientos	1
Sobre el UNIDIR.....	1
Nota	1
Citación	1
Sobre los autores	2
Abreviaturas y acrónimos.....	2
Resumen.....	4
1. Introducción: el auge de la tecnología cuántica	6
2. Conceptos fundamentales de la mecánica cuántica	7
3. Exploración de las aplicaciones militares de la tecnología cuántica.....	9
3.1 Detección cuántica.....	10
3.2 Imagen cuántica.....	11
3.3 Sistemas de radar cuántico.....	12
3.4 Comunicaciones cuánticas.....	13
3.5 Distribución cuántica de claves.....	13
3.6 Computación cuántica.....	14
4. Implicaciones para la seguridad internacional de la tecnología cuántica	14
4.1 Seguridad global de las TIC.....	15
4.2 Inteligencia, vigilancia y reconocimiento con capacidad cuántica.....	16
4.3 Sistemas de apoyo a la toma de decisiones y sistemas de armas autónomos	16
4.4 Vigilancia y verificación	17
5. Ejemplos de iniciativas nacionales y regionales en materia cuántica	18
6. Conclusión	21

Resumen

Este manual ofrece a los encargados de la formulación de políticas y los diplomáticos una visión general de la tecnología cuántica y su impacto previsto en la seguridad internacional, centrándose tanto en sus posibles beneficios como en sus riesgos, en los ámbitos militar y civil. Los avances cuánticos prometen cambios transformadores en la detección, la computación, la comunicación y la criptografía, y ofrecen capacidades mejoradas de inteligencia, vigilancia y reconocimiento (ISR), así como avances críticos en la seguridad de la información y la resiliencia criptográfica. Sin embargo, estas mismas tecnologías también introducen retos susceptibles de desestabilizar los marcos de seguridad que sustentan la paz mundial.

La detección cuántica, por ejemplo, representa un paso de gigante en la medición de precisión, con aplicaciones que van desde las operaciones militares hasta la verificación del desarme. Esta capacidad podría mejorar enormemente las técnicas de vigilancia esenciales para el control de armamentos, al permitir la detección de alta sensibilidad de materiales nucleares y otros marcadores medioambientales críticos. Los sensores cuánticos también poseen un gran potencial en el ámbito marítimo, donde podrían poner al descubierto activos subacuáticos hasta ahora indetectables, como los submarinos, lo que supondría un reto estratégico para las tecnologías tradicionales de sigilo naval.

Se prevé que la computación cuántica, aún en desarrollo, revolucione campos que requieren un procesamiento avanzado de datos, como la criptografía, las simulaciones complejas y la automatización impulsada por la inteligencia artificial. A medida que esta tecnología madure, podría poner en peligro los sistemas criptográficos existentes que protegen las infraestructuras críticas y las comunicaciones sensibles. Ello pone de relieve la necesidad de efectuar con urgencia la transición a normas criptográficas poscuánticas a fin de proteger los datos gubernamentales, militares y civiles frente a futuras ciberamenazas.

Más allá del ámbito de la seguridad de la información y las comunicaciones, los sensores cuánticos y la computación cuántica pueden tener un impacto en la paz y la seguridad internacionales en un sentido más amplio, tanto positivo como negativo. Así, la tecnología cuántica podría aportar mayor precisión a las técnicas de verificación, reforzar los esfuerzos de no proliferación y ofrecer capacidades de vigilancia a distancia con suficiente sensibilidad como para detectar actividad nuclear desde el espacio, ampliando aún más el alcance de la vigilancia a disposición de la comunidad internacional.

Existe un interés generalizado entre los Estados por el desarrollo de las capacidades cuánticas, espoleado por el potencial de ventaja competitiva y de mejora de la seguridad. Algunos Estados han incorporado el desarrollo cuántico a sus estrategias de seguridad

nacional, a menudo formando asociaciones público-privadas que aceleran la investigación y cierran la brecha entre la innovación científica y la aplicación práctica. Estas iniciativas subrayan la necesidad de una colaboración multilateral para hacer frente a las crecientes asimetrías en las capacidades cuánticas, que podrían agravar las brechas digitales existentes entre los Estados que llevan la delantera en tecnología cuántica y los países en desarrollo.

De cara al futuro, se precisan marcos de gobernanza sólidos, asociaciones intersectoriales y una atención especial al fomento de la capacidad para apoyar a una mano de obra versada en materia cuántica. La cooperación multilateral será esencial para establecer normas que regulen el uso responsable de la tecnología cuántica, promover la estabilidad en lugar de la competencia y garantizar que los avances cuánticos beneficien a todos. Un enfoque holístico de la tecnología cuántica —que aborde su ciclo de vida completo— ayudará a los Estados a prever y mitigar sus oportunidades y sus retos para la paz y la seguridad internacionales.

1. Introducción: el auge de la tecnología cuántica

El aumento de la investigación, la innovación y la inversión en tecnología cuántica se está convirtiendo en un fenómeno mundial¹. Se trata de una tecnología muy prometedora que podría aportar avances significativos en aras de un buen número de Objetivos de Desarrollo Sostenible².

A pesar de los atractivos beneficios de la tecnología cuántica, esta también genera inquietud debido a los riesgos que entraña para la paz y la seguridad internacionales. El Secretario General de las Naciones Unidas advirtió a la Asamblea General en 2022 de que los ordenadores cuánticos podrían “destruir la ciberseguridad y aumentar el riesgo de que se produzcan anomalías en sistemas complejos. No tenemos ni por asomo una arquitectura global para hacer frente a cualquiera de estos retos”³.

Sin duda, está por ver en qué medida las tecnologías cuánticas pueden configurar el carácter futuro de la guerra, o de la seguridad en general, sobre todo teniendo en cuenta el estado frágil e incipiente de los sistemas cuánticos⁴. A pesar de esta ambigüedad y habida cuenta de que la ciencia y la tecnología cuánticas podrían revolucionar tan profundamente el campo de la informática, en aras de la seguridad mundial, es importante invertir en la educación temprana y la adquisición de conocimientos.

Los Estados están mostrando un gran interés por esta tecnología, como evidencia el aumento de las inversiones en investigación sobre tecnología cuántica⁵ y el elevado número de referencias a la cuántica hechas por los Estados Miembros durante las sesiones oficiales del Grupo de trabajo de composición abierta (GTCA) de las Naciones Unidas sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso⁶.

¹ Alina Clasen, “Germany Strives to Catch Up with US, China in Quantum Tech Race”, Euractiv, 12 May 2023, <https://www.euractiv.com/section/digital/news/germany-strives-catch-up-with-us-china-in-quantum-tech-race/>.

² Open Quantum Institute, *Progress Report 2024: Quantum for All Initiative* (Geneva: Gesda, October 2024), <https://gesda.global/wp-content/uploads/2024/10/GESDA-Quantum-For-All-Progress-Report-2024-Final.pdf>.

³ United Nations, “‘Our World Is in Big Trouble’, Secretary-General Warns General Assembly, Urging Member States to Work as One United Nations”, Press Release SG/SM/21466, 20 September 2022, <https://press.un.org/en/2022/sgsm21466.doc.htm>.

⁴ Lauren Biron, “Five Ways QSA Is Advancing Quantum Computing”, Berkeley Lab News Center, 10 April 2023, <https://newscenter.lbl.gov/2023/04/10/five-ways-qa-is-advancing-quantum-computing/>.

⁵ Indra, “ADEQUADE: Advanced, Disruptive and Emerging QUAntum Technologies for Defence”, 2022, <https://www.indracompany.com/en/indra/adequade-advanced-disruptive-emerging-quantum-technologies-defence>.

⁶ United Nations, Office for Disarmament Affairs, “Open-ended Working Group on Security of and in the Use of Information and Communications Technologies”, <https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021>.

A las puertas ya de 2025, designado por las Naciones Unidas año internacional de la ciencia y la tecnología cuánticas, este manual básico pretende concienciar sobre las posibles implicaciones de la tecnología cuántica en la seguridad internacional. Su propósito es dotar a encargados de la formulación de políticas y diplomáticos de un marco de referencia para considerar el ecosistema de riesgos que rodea a la ciencia y la tecnología cuánticas.

Para ayudar a abordar este complejo tema, tras esta introducción, el apartado 2 ofrece una visión general de algunas iniciativas nacionales y regionales sobre cuántica. A continuación, el apartado 3 esboza varios conceptos fundamentales de la mecánica cuántica. El apartado 4 presenta las aplicaciones militares de la tecnología cuántica. Seguidamente, el apartado 5 ofrece un acercamiento preliminar a las posibles implicaciones de la tecnología cuántica en el panorama de la seguridad internacional, antes de las conclusiones presentadas en el apartado 6.

2. Conceptos fundamentales de la mecánica cuántica

La mecánica cuántica estudia el comportamiento de los átomos y las partículas. Los átomos constan de un núcleo, formado por protones y neutrones, en torno al cual orbitan electrones. Los electrones viajan en cuantos discretos (es decir, la unidad más pequeña de energía) y también pueden moverse en una onda continua, como el chorro de agua de un fregadero. Los electrones pueden ocupar varios estados simultáneamente, lo cual se denomina “superposición”⁷. Este fenómeno hace que la mecánica cuántica haya sido calificada como “extraña” por algunos físicos⁸.

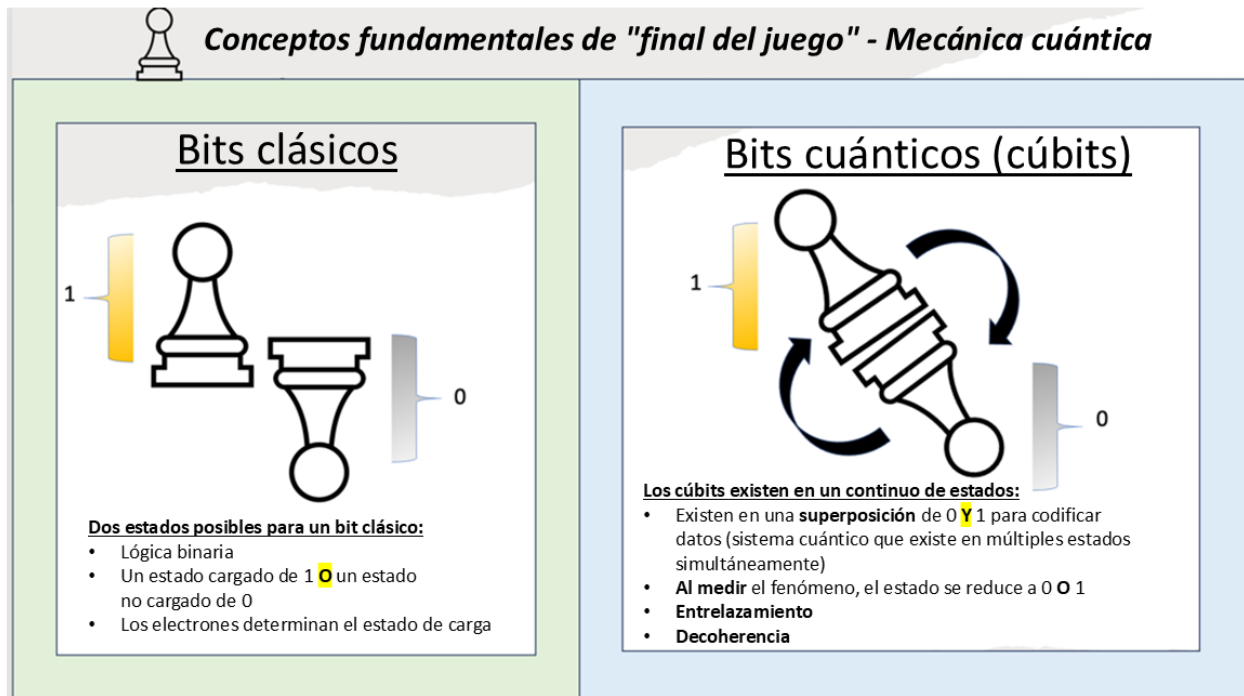
A nivel cuántico, los acontecimientos no se determinan simplemente. Por ejemplo, en lugar de dos estados discretos de carga, sin carga (expresado como 0) y cargado (expresado como 1), ambos pueden aplicarse simultáneamente, y además de forma aleatoria. El famoso experimento de la doble rendija demuestra estas propiedades únicas de los fenómenos cuánticos. Explicado de forma sucinta, los científicos observaron que, cuando las ondas de electrones pasaban por dos rendijas, producían ondas más pequeñas que se amplificaban y anulaban unas a otras hasta que chocaban con la pared posterior de la zona de pruebas. Este patrón de interferencia se produjo porque “los electrones parecen actuar como ondas hasta el momento en que son observados, o medidos, cuando vuelven a ser partículas”⁹.

⁷ Ibid.

⁸ Michio Kaku, *Physics of the Future: How Science Will Shape Human Destiny and Our Daily Lives by the Year 2100* (New York: Anchor, 2012).

⁹ Amit Katwala, *Quantum Computing: How It Works and How It Could Change the World* (London: Random House Business Books, 2021), p. 16.

Figura 1. Representación visual de los bits clásicos y los bits cuánticos



La superposición puede explicarse mejor utilizando la imagen de los peones de ajedrez de la figura 1. Imaginemos que el peón puede colocarse de pie (para indicar un estado de carga de 1) o boca abajo (para indicar un estado sin carga de 0). Los ordenadores digitales modernos funcionan con esta lógica binaria. Un bit clásico (la unidad básica de información) —o el peón clásico en este ejemplo— puede representar un 0 o un 1. En cambio, los ordenadores cuánticos son sistemas más complejos que funcionan utilizando distintas unidades de información, llamadas **bits cuánticos** o **cúbits**, que existen en una superposición de los estados 0 y 1 para codificar los datos¹⁰. El peón cuántico de la figura 1 puede existir en un continuo de estados mientras gira: un átomo "puede así contener mucha más información que un 0 o un 1", como explica el físico teórico Michio Kaku¹¹. Cuando se observan con un microscopio especializado, los cúbits parecen "signos más plateados"¹². Permiten a los ordenadores cuánticos realizar complejas tareas de modelización y resolver problemas multivariables más eficazmente que los ordenadores digitales¹³.

¹⁰ IBM, "IBM Quantum Learning", n.d., <https://learning.quantum.ibm.com/>.

¹¹ Kaku, *Physics of the Future*.

¹² Katwala, *Quantum Computing*, p. 45.

¹³ Lily Chen et al., *Report on Post-Quantum Cryptography* (Washington, DC: National Institute of Standards and Technology, April 2016), <https://doi.org/10.6028/nist.ir.8105>.

Además, los cúbits también pueden interactuar entre sí; este fenómeno se denomina “entrelazamiento”. El entrelazamiento es una condición según la cual “dos o más objetos de un sistema cuántico pueden estar intrínsecamente ligados entre sí, de forma que la medición de un objeto dicte los posibles resultados de la medición de otro, independientemente de la distancia a la que se encuentren dichos objetos”¹⁴. Esta propiedad permite a los sistemas cuánticos realizar múltiples cálculos de forma simultánea¹⁵. Sin embargo, los estados cuánticos son muy sensibles a las perturbaciones ambientales, como el sonido, el movimiento y los cambios de temperatura.

Los científicos estudian cómo aprovechar la superposición para aumentar la potencia y velocidad de computación de los ordenadores cuánticos. Uno de los muchos retos que plantean el desarrollo y la implantación de la tecnología cuántica es cómo garantizar que los cuantos, altamente sensibles, no se vean influidos por la decoherencia o la incertidumbre en la medición de frecuencias¹⁶. Ello se debe a que incluso el acto de medir sistemas cuánticos podría alterar la integridad del resultado, limitándolo a una forma binaria de 0 o 1¹⁷. Estas perturbaciones ambientales conducen a la atrofia (es decir, a la decoherencia), lo que dificulta que los sistemas cuánticos mantengan la superposición y el entrelazamiento durante periodos de tiempo lo bastante largos como para permitir la experimentación.

3. Exploración de las aplicaciones militares de la tecnología cuántica

Las propiedades fundamentales de la mecánica cuántica descritas en el apartado 2 permiten explorar múltiples aplicaciones en los ámbitos militares y de la seguridad. De hecho, las tecnologías cuánticas pueden ofrecer capacidades en computación, comunicaciones y conciencia situacional inalcanzables para la tecnología actualmente disponible.¹⁸

Este apartado ofrece una visión general introductoria de las aplicaciones más citadas en la literatura académica y general: detección cuántica, imagen cuántica, sistemas de radar cuántico, comunicaciones cuánticas, distribución cuántica de claves (QKD) y computación cuántica.

¹⁴ National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects* (Washington, DC: National Academies Press, 2019), <https://doi.org/10.17226/25196>, p. 26.

¹⁵ Alexandre Menard et al., “A Game Plan for Quantum Computing”, McKinsey & Company, 6 February 2020, <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing>.

¹⁶ Adrian Cho, “A Quantum Sense for Dark Matter”, *Science*, 28 April 2022, <https://www.science.org/content/article/crack-mystery-dark-matter-physicists-turn-super-sensitive-quantum-sensors>.

¹⁷ Ibid.

¹⁸ North Atlantic Treaty Organization (NATO), “Summary of NATO’s Quantum Technologies Strategy”, 17 January 2024, https://www.nato.int/cps/en/natohq/official_texts_221777.htm.

3.1 Detección cuántica

Los sensores cuánticos son fundamentalmente herramientas de medición. Aunque los principios físicos y los materiales empleados para construir sensores cuánticos son los mismos que los de los sensores convencionales, los primeros son ultrasensibles. Son capaces, por ejemplo, de detectar las más mínimas perturbaciones ambientales en campos eléctricos y magnéticos, así como la presencia de radiación. La principal diferencia entre los sensores cuánticos y los convencionales radica en que los primeros poseen una notable capacidad de precisión que les permite detectar la unidad más pequeña de energía o medida, llamada cuanto¹⁹.

Dada la precisión con que los sensores cuánticos pueden detectar cambios a escala infinitesimal en el tiempo y la gravedad, los científicos estudian cómo aplicar esta tecnología para mejorar la actual capacidad de detección militar, tanto con fines defensivos como ofensivos. Por ejemplo, los sensores cuánticos podrían ofrecer a los ejércitos la capacidad de mantener la precisión temporal y en el posicionamiento en entornos en los que el sistema mundial de navegación por satélite (GNSS) se ve entorpecido por interferencias electrónicas en forma de interferencia deliberada y simulación de señal²⁰.

En 2017, la Academia China de Ciencias anunció que había desarrollado un sensor, llamado Dispositivo Superconductor de Interferencia Cuántica (SQUID), que emplea sensores cuánticos para detectar cambios ambientales ultrasensibles (como, por ejemplo, campos magnéticos débiles en la actividad cerebral). El SQUID es tan ultrasensible que puede registrar actividad remota en el espacio exterior (por ejemplo, erupciones solares). Además, un SQUID puede detectar aeronaves en el marco de un sistema de defensa nacional, así como dotar a los aviones antisubmarinos de capacidades mejoradas de detección de anomalías magnéticas. Los investigadores chinos también están desarrollando varios tipos de detectores magnéticos, algunos de los cuales podrían

¹⁹ David Chandler, "Quantum Sensor Can Detect Electromagnetic Signals of Any Frequency", MIT News, Massachusetts Institute of Technology, 21 June 2022, <https://news.mit.edu/2022/quantum-sensor-frequency-0621>.

²⁰ US Department of Defense, Defense Science Board (DSB), "DSB Reports", n.d., <https://dsb.cto.mil/reports.htm>.

montarse en satélites²¹ e instalarse en aviones para localizar con precisión minerales bajo la superficie terrestre²².

Además, los sensores cuánticos se perfilan como una tecnología interesante para mejorar las capacidades de detección de submarinos bajo el agua. Ya se trate de sistemas instalados en satélites, sistemas submarinos fijos o sistemas montados en aeronaves o buques, los futuros sensores cuánticos podrían tener un efecto disruptivo en el sigilo de las operaciones submarinas, como las de los submarinos nucleares lanzamisiles balísticos, que representan un activo esencial para la disuasión nuclear. En particular:

- **Los magnetómetros cuánticos** podrían utilizarse para detectar cambios mínimos en los campos magnéticos provocados por el casco metálico o el sistema de propulsión de los submarinos. Esto ampliaría enormemente la capacidad de detección de submarinos sumergidos.
- **Los gravímetros cuánticos** podrían medir las variaciones más leves en la atracción gravitatoria, lo que permitiría revelar la presencia de la masa de un submarino. Los gravímetros cuánticos serían capaces de detectar submarinos sin que estos pudiesen recurrir a ningún método para protegerse²³.

3.2 Imagen cuántica

La obtención de imágenes cuánticas es un método de imagen especializado que permite a los científicos captar imágenes ópticas de calidad avanzada de un objeto²⁴. Este método utiliza partículas de luz entrelazadas para crear imágenes detalladas de longitudes de onda que, de otro modo, serían muy sensibles e imposibles de observar²⁵. Mediante la manipulación de pares de fotones, los científicos pueden captar imágenes de mayor calidad y resolución que con los métodos tradicionales²⁶.

²¹ Henk H.F. Smid, "An Analysis of Chinese Remote Sensing Satellites", *Space Review*, 26 September 2022, <https://www.thespacereview.com/article/4453/1>.

²² Stephen Chen, "Has China Developed the World's Most Powerful Submarine Detector?", *South China Morning Post*, 24 June 2017, <https://www.scmp.com/news/china/society/article/2099640/has-china-developed-worlds-most-powerful-submarine-detector>.

²³ Rudy Ruitenbergh, "Armed with Quantum Sensors, France Eyes Leaps in Electronic Warfare", *Defense News*, 25 June 2024, <https://www.defensenews.com/global/europe/2024/06/25/armed-with-quantum-sensors-france-eyes-leaps-in-electronic-warfare/>.

²⁴ "Quantum Imaging", *Nature*, n.d., <https://www.nature.com/collections/gehjgebjcc>.

²⁵ Fraunhofer-Gesellschaft, "Quantum Imaging: Pushing the Boundaries of Optics", *Phys.org*, 3 January 2022, <https://phys.org/news/2022-01-quantum-imaging-boundaries-optics.html>.

²⁶ Ibid.

En el ámbito de las operaciones militares, podrían desarrollarse capacidades avanzadas de obtención de imágenes infrarrojas para optimizar las capacidades de inteligencia, vigilancia y reconocimiento (ISR). Por ejemplo, los sistemas de obtención de imágenes cuánticas podrían aplicarse para detectar la presencia de gases tóxicos nocivos en los campos de batalla y ayudar en el análisis forense de armas químicas y de la composición de plásticos²⁷. Asimismo, la tecnología cuántica haría posible la llamada imagen fantasma, o *ghost imaging*, una técnica que utiliza correlaciones cuánticas entre fotones para crear imágenes de objetos sin “verlos” directamente, de manera que se podrían obtener imágenes de objetivos a través de agentes oscurecedores como nubes, niebla o humo. Esto sería de gran utilidad para el reconocimiento militar y la selección de objetivos²⁸. Un concepto similar permitiría una mejora significativa en condiciones extremas de poca luz, otro escenario de importancia primordial para el éxito de las operaciones de ISR²⁹.

3.3 Sistemas de radar cuántico

Los sistemas de radar convencionales están expuestos a los dispositivos inhibidores de señal y el ruido interferente provocado por fenómenos naturales. En cambio, un sistema de radar resiliente con capacidad cuántica podría detectar aeronaves furtivas con mayor precisión utilizando un sistema de transmisión fotónico más sofisticado³⁰.

Algunos estudiosos afirman que el impacto potencial del radar cuántico en las operaciones militares no debería ponerse en duda porque, una vez que la tecnología alcance la fase de implantación, marcará el “fin de la era del sigilo”³¹. Por el contrario, según otros expertos, el radar cuántico sigue planteando “grandes retos técnicos”, como la construcción de detectores sensibles o la estabilización de los flujos de fotones entrelazados³². Existe, en definitiva, un intenso debate entre los teóricos sobre el valor añadido que aportaría la tecnología de radar cuántico a las operaciones militares.

²⁷ Ibid.

²⁸ Rajesh Uppal, “Quantum Imaging Technique Can Have Military Applications, US and China Racing to Deploy Quantum Ghost Imaging in Satellites for Stealth Plane Tracking”, IDST, 26 June 2022, <https://idstch.com/technology/photonics/revolutionary-new-quantum-imaging-technique-can-have-military-applications/>.

²⁹ National Security Technology Accelerator (NSTXL), “Quantum Technology in the Military”, 1 February 2023, <https://nstxl.org/quantum-technology-in-the-military/>.

³⁰ Martin Giles, “The US and China Are in a Quantum Arms Race That Will Transform Warfare”, *MIT Technology Review*, 3 January 2019, <https://www.technologyreview.com/2019/01/03/137969/us-china-quantum-arms-race/>.

³¹ See, for example, Professor Seth Lloyd of the Massachusetts Institute of Technology, cited in *ibid*.

³² See, for example, Professor Jonathan Baugh of the University of Waterloo, cited in *ibid*.

En lo que respecta a las operaciones espaciales, algunos estudiosos plantean que el radar cuántico podría utilizarse en el espacio exterior para la detección de vehículos espaciales furtivos, el rastreo de movimientos de desechos orbitales minúsculos, pero peligrosos, y la vigilancia de misiles balísticos³³. Otros se muestran escépticos con respecto a su potencial de mejora de la capacidad de detección de objetos³⁴.

En conjunto, las tecnologías cuánticas de detección, imagen y radar ofrecen la posibilidad de mejorar la conciencia situacional de los ejércitos, al tiempo que podrían reducir la capacidad de sigilo militar en determinados contextos³⁵.

3.4 Comunicaciones cuánticas

De todas las categorías de tecnología cuántica presentadas en este manual, las comunicaciones cuánticas son en la actualidad las menos desarrolladas para aplicaciones militares. Las comunicaciones cuánticas utilizan el entrelazamiento —proceso por el cual los cúbits pueden comunicarse entre sí simultáneamente— para transferir datos entre distintos emplazamientos y canales de transmisión.³⁶

Mientras que la comunicación cuántica está aún en pañales, el subcampo de la QKD está algo más desarrollado en lo que respecta a las aplicaciones militares.

3.5 Distribución cuántica de claves

En el contexto militar, la seguridad de las comunicaciones es de vital importancia para garantizar la capacidad de ejercer un mando y control eficaces y lograr el éxito de la misión. En este sentido, el cifrado de datos e información siempre ha desempeñado un papel importante en el ámbito militar. La distribución cuántica de claves se basa en los principios de la mecánica cuántica para cifrar los datos. En el mundo físico, una llave sirve tanto para cerrar como para abrir sistemas. En informática, una clave puede ser una cadena de unos y ceros empleada para cifrar y descifrar información.

China logró establecer la primera red intercontinental de comunicaciones QKD tierra-satélite y satélite-tierra entre el satélite cuántico Micius y una estación terrestre de comunicaciones cuánticas sita en la provincia de Hebei en 2017³⁷. Según el comandante del sistema Micius,

³³ Chris Jay Hoofnagle and Simson Garfinkel, "Quantum Sensors—Unlike Quantum Computers—Are Already Here", *Defense One*, 27 June 2022, <https://www.defenseone.com/ideas/2022/06/quantum-sensorsunlike-quantum-computersare-already-here/368634/>.

³⁴ US Department of Defense, Defense Science Board (DSB), "DSB Reports".

³⁵ Hoofnagle and Garfinkel, "Quantum Sensors—Unlike Quantum Computers—Are Already Here".

³⁶ US National Science Foundation (NSF), "NSF and White House Office of Science and Technology Policy Initiate Collaborative Effort to Develop Critical Resources for Quantum Education", 18 May 2020, https://www.nsf.gov/news/special_reports/announcements/051820.jsp.

³⁷ "China Achieves a Quantum Jump", *China Daily*, 18 June 2017, <http://en.people.cn/n3/2017/0618/c90000-9229972.html>.

esta red de comunicaciones cuánticas es “el método de comunicación más seguro porque cualquier intento de escucha furtiva interrumpiría el entrelazamiento y sería detectado”³⁸. Este experimento tuvo gran importancia porque demostró la viabilidad de las comunicaciones cuánticas seguras en el espacio. Asimismo, un artículo de *NATO Review* afirma que la QKD podría hacer posible la “transmisión de datos ultrasegura, incluso completamente inexpugnable”, en las comunicaciones militares de defensa³⁹.

3.6 Computación cuántica

La computación cuántica es una forma avanzada de computación que se basa en los principios de la física cuántica para procesar la información. Ello brinda el potencial de solucionar problemas que los ordenadores convencionales tardarían miles de años en resolver. La computación cuántica es una tecnología facilitadora muy prometedora para todos los sectores de la sociedad, incluido el militar. Las principales aplicaciones militares son⁴⁰:

- **Criptografía y ciberseguridad**, incluidos el descifrado de códigos y el cifrado resistente a tecnologías cuánticas (véase el apartado 4)
- **Inteligencia artificial (IA) y aprendizaje automático**, que respaldan tanto los sistemas de apoyo a la toma de decisiones (SAD) más sofisticados como una nueva generación de sistemas autónomos
- **Logística y problemas complejos de optimización**, como la gestión de la cadena de suministro y la planificación de misiones
- **Simulación y modelización**, para proporcionar simulaciones más precisas y complejas de las condiciones del campo de batalla para el entrenamiento militar
- **Ciencias de los materiales**, para acelerar el descubrimiento y desarrollo de nuevos materiales para aplicaciones militares, como blindajes más resistentes y ligeros

4. Implicaciones para la seguridad internacional de la tecnología cuántica

Tras la breve visión general de la tecnología cuántica y sus posibles usos militares recogida en los apartados anteriores, este se detiene en las posibles implicaciones para la seguridad internacional en cuatro áreas clave: seguridad global de las TIC, ISR, SAD y SAA y vigilancia y verificación.

³⁸ Ibid.

³⁹ Michiel van Amerongen, “Quantum Technologies in Defence & Security”, *NATO Review*, 3 June 2021, <https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html>.

⁴⁰ National Security Technology Accelerator (NSTXL), “Quantum Technology in the Military”.

4.1 Seguridad global de las TIC

Como se menciona en la introducción, cada vez son más los Estados Miembros participantes en el GTCA sobre seguridad de las TIC que destacan las posibles amenazas que plantea la tecnología cuántica. ¿Cómo pueden manifestarse estas amenazas en la práctica?

Por ejemplo, los ordenadores cuánticos podrían descifrar muchos de los métodos de cifrado actuales, incluidos los sistemas criptográficos de clave pública más utilizados (tales como RSA y ECC). Esto pondría en peligro la seguridad de las comunicaciones gubernamentales, militares y de inteligencia sensibles, tanto a nivel nacional como entre Estados. Esta capacidad también permitiría a los actores maliciosos descifrar comunicaciones cifradas previamente interceptadas y almacenadas. Este tipo de acto malicioso en el ámbito de las TIC —denominado “cosechar ahora, descifrar después” (HNDL, por sus siglas en inglés)— consiste en extraer y almacenar datos cifrados, para descifrarlos en el futuro mediante algoritmos de criptografía poscuántica (PQC, por sus siglas en inglés)⁴¹. Esto resulta alarmante porque estos protocolos de seguridad protegen las comunicaciones y operaciones cotidianas basadas en Internet, incluidas las de servicios de importancia crítica como las finanzas y la sanidad⁴². Aunque en la actualidad ningún ordenador cuántico está equipado con suficientes cúbits como para calcular rápidamente los factores primos necesarios para descifrar comunicaciones sensibles⁴³, ello no debe hacer caer a los encargados de la formulación de políticas en la complacencia al valorar este creciente riesgo para la ciberseguridad⁴⁴.

Los Estados deben empezar a planificar cómo actualizar los sistemas sensibles a los algoritmos PQC para protegerlos mejor frente al entorno de riesgo PQC. Sin embargo, adaptar las infraestructuras críticas a las normas PQC es un reto complejo que requeriría tiempo, inversión y una cooperación bien estructurada entre los sectores público y privado. Como marco de planificación inicial, los encargados de la formulación de políticas deberían centrarse en abordar estas cuestiones y comprometerse con las partes interesadas para generar confianza en torno a la mejora de los sistemas e infraestructuras vulnerables.

⁴¹ US National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division, “Post-Quantum Cryptography”, n.d., <https://csrc.nist.gov/projects/post-quantum-cryptography>.

⁴² Ibid.

⁴³ QuTech Academy, “Shor’s Algorithm”, n.d., <https://www.qutube.nl/quantum-algorithms/shors-algorithm>.

⁴⁴ Menard et al., “A Game Plan for Quantum Computing”.

4.2 Inteligencia, vigilancia y reconocimiento con capacidad cuántica

Los sensores cuánticos están evolucionando rápidamente. Algunos técnicos consideran que pasarán del laboratorio a un contexto operativo más pronto de lo que lo hará la computación cuántica⁴⁵.

Sin embargo, es necesario ampliar la capacidad de producción de sensores cuánticos antes de poder desplegarlos en entornos operativos militares⁴⁶. Los sensores cuánticos podrían aumentar las capacidades de ISR (como se explica en el apartado 3.1), en particular para redefinir el concepto de sigilo en las operaciones en todos los ámbitos. Al menos a nivel teórico, esto a su vez podría repercutir en la seguridad y la estabilidad internacionales, dada la capacidad potencial de los sensores cuánticos para revolucionar la planificación y realización de operaciones militares, así como de disuasión nuclear (debido a su impacto en la detección de submarinos, como se explica en el apartado 3.1).

4.3 Sistemas de apoyo a la toma de decisiones y sistemas de armas autónomos

Los sistemas cuánticos también pueden acelerar la investigación en IA avanzada y capacidades de aprendizaje automático y habilitar a una nueva generación de sistemas de IA complejos que respalden/den apoyo a SAD más avanzados y una nueva generación de sistemas autónomos, incluyendo los SAA. Por ejemplo, una mayor capacidad de cálculo, unida a la posibilidad de ejecutar modelos de IA con algoritmos cuánticos, permitiría mejorar y agilizar la toma de decisiones en tiempo real (por humanos o sistemas autónomos), así como abordar complejos problemas de optimización que en muchos casos son irresolubles para los ordenadores convencionales.

Para dar algo de perspectiva sobre la magnitud de esta innovación, ya en 2019 el ordenador cuántico de Google logró completar en solo 200 segundos una tarea que a un ordenador clásico le habría llevado 10.000 años⁴⁷. Esta capacidad es esencial para las operaciones militares que implican numerosas variables y resultados posibles. Además de brindar una mayor capacidad de procesamiento de datos en tiempo real, la integración de la computación cuántica con la IA permitirá a los planificadores militares simular

⁴⁵ Marco Lanzagorta and Jeffrey Uhlmann, "Opportunities and Challenges of Quantum Radar", *IEEE Aerospace and Electronic Systems Magazine*, vol. 35, no. 11 (1 November 2020): 38–56, <https://doi.org/10.1109/maes.2020.3004053>.

⁴⁶ Marcus Doherty, "Quantum Technology: The Defence Imperative", Australian Army Research Centre, 5 May 2020, <https://researchcentre.army.gov.au/library/land-power-forum/quantum-technology-defence-imperative>.

⁴⁷ Cameron Wood and Alex Krijger, "The Convergence of Artificial Intelligence and Quantum Computing: Unravelling the Complex Geopolitical Nexus", Transformation Forums, 18 June 2023, <https://www.transformationforums.com/the-convergence-of-artificial-intelligence-and-quantum-computing-unravelling-the-complex-geopolitical-nexus/>.

diversos escenarios y resultados de forma mucho más eficiente y, por ende, tomar decisiones mejor fundamentadas.

En sectores como la sanidad, la gestión de los recursos hídricos o la seguridad alimentaria, la tecnología cuántica ya está dando resultados prometedores por su eficiencia, productividad, precisión y rapidez. Por tanto, es importante que los debates sobre el desarrollo, despliegue y uso responsables de la IA en el ámbito militar contemplen también el posible impacto de la tecnología cuántica⁴⁸.

4.4 Vigilancia y verificación

Por último, un campo de aplicación importante de la tecnología cuántica en la seguridad internacional sería la vigilancia y verificación en apoyo de la no proliferación y las salvaguardias. Se trata de elementos esenciales para garantizar el uso pacífico de la tecnología nuclear y evitar la proliferación de armas nucleares. Los sensores cuánticos se perfilan como instrumentos prometedores que podrían contribuir a estos esfuerzos de distintas maneras:

- **Mayor capacidad de detección:** Los sensores cuánticos aportan mejoras significativas en la detección de materiales y actividades nucleares. En particular, mejoran la sensibilidad y el alcance de la detección de radiaciones⁴⁹. Por consiguiente, permiten una vigilancia más eficaz de las instalaciones nucleares y las fronteras para impedir el tráfico de materiales nucleares.
- **Muestreo medioambiental mejorado:** Las tecnologías de detección cuántica podrían mejorar el análisis de las muestras medioambientales recogidas con fines de salvaguardia. Esto brinda el potencial de detectar trazas de materiales nucleares con mayor precisión⁵⁰.
- **Técnicas de verificación mejoradas:** Las técnicas avanzadas de detección cuántica permiten realizar mediciones no destructivas más precisas de cantidades y composiciones de materiales nucleares. Tales mediciones resultan esenciales para verificar las declaraciones y detectar desviación⁵¹.

⁴⁸ Open Quantum Institute, *Intelligence Report on Quantum Diplomacy for the Sustainable Development Goals (SDGs)* (Geneva: Gesda, October 2024), https://open-quantum-institute.cern/wp-content/uploads/2024/10/GESDA_OOI_Intelligence-Report-2024_Final.pdf.

⁴⁹ Samanvya Hooda, "Quantum Sensors and Submarine Invulnerability", 16 October 2023, <https://www.9dashline.com/article/quantum-sensors-and-submarine-invulnerability>.

⁵⁰ Henning Soller and Niko Mohr, "Quantum Sensing's Untapped Potential: Insights for Leaders", 17 September 2024, <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-sensings-untapped-potential-insights-for-leaders>.

⁵¹ Ibid.

- **Mayor capacidad de vigilancia a distancia:** Los futuros sensores cuánticos instalados en satélites podrían detectar actividades nucleares desde el espacio con un nivel de sensibilidad sin precedentes y mejorar, por tanto, la capacidad de vigilancia global.

5. Ejemplos de iniciativas nacionales y regionales en materia cuántica

Algunos Estados han invertido o anunciado inversiones en tecnología cuántica. Muchos también han aprovechado asociaciones público-privadas estructuradas con agentes del sector privado, desde empresas emergentes hasta grandes compañías tecnológicas⁵².

Alemania, por ejemplo, aspira a liderar la carrera mundial de la innovación cuántica, según su programa marco conceptual de tecnologías cuánticas para 2023⁵³. Este documento recoge el marco estratégico de Alemania y su plan de invertir 3.000 millones de euros para desarrollar un ordenador cuántico universal de aquí a 2026. Canadá también pretende asumir un papel central mediante su estrategia cuántica nacional de 2023, que destina 360 millones de dólares canadienses al desarrollo de la investigación, la innovación y la comercialización cuánticas⁵⁴.

En 2023, el Gobierno australiano publicó una estrategia cuántica nacional y destinó 1.000 millones de dólares australianos a acelerar la innovación cuántica⁵⁵. China, según algunas estimaciones, está invirtiendo 15.000 millones de dólares en tecnología cuántica, suma esta con la que podría superar el conjunto de todas las inversiones del resto del mundo⁵⁶. En contraste con esta cifra, la Unión Europea tiene previsto invertir 7.200 millones de dólares (6.800 millones de euros) en proyectos de computación cuántica hasta 2025⁵⁷ y

⁵² See, for example, IBM, "IBM and Government of Quebec Launch Groundbreaking Partnership to Accelerate Discovery with First IBM System in Canada", 3 February 2022, <https://newsroom.ibm.com/2022-02-03-IBM-and-Government-of-Quebec-Launch-Groundbreaking-Partnership-to-Accelerate-Discovery-with-First-IBM-Quantum-System-in-Canada>.

⁵³ Federal Ministry of Education and Research, "Quantum Technologies Conceptual Framework Programme of the Federal Government", April 2023, https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Quantum-Technologies-Conceptual-Framework-2023_english_bf_C1.pdf

⁵⁴ Government of Canada, "Overview of Canada's National Quantum Strategy", 31 July 2023, <https://ised-isde.canada.ca/site/national-quantum-strategy/en>.

⁵⁵ Government of Australia, "National Quantum Strategy", 3 May 2023, <https://www.industry.gov.au/publications/national-quantum-strategy>.

⁵⁶ Mateusz Masiowski et al., "Quantum Computing Funding Remains Strong, But Talent Gap Raises Concern", McKinsey, 15 June 2022, <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-funding-remains-strong-but-talent-gap-raises-concern>.

⁵⁷ Ibid.

Estados Unidos se comprometió a destinar 1.900 millones de dólares hasta 2025⁵⁸. Además, la Federación Rusa se comprometió a invertir 800 millones de dólares en el desarrollo de tecnología cuántica hasta 2025, y ha adoptado una hoja de ruta quinquenal sobre tecnología cuántica⁵⁹.

En Europa, la Empresa Común de Informática de Alto Rendimiento Europea (EC EuroHPC) ha anunciado sus planes para invertir 100 millones de euros en la construcción de seis emplazamientos para ordenadores cuánticos europeos, en Alemania, Chequia, España, Francia, Italia y Polonia⁶⁰. Otro ejemplo es el proyecto de la Comisión Europea ADEQUADE (“Advanced, Disruptive and Emerging QUAntum technologies for DEfence”), que cuenta con más de 30 socios de 8 Estados europeos y pretende aprovechar la tecnología de detección cuántica para aumentar las capacidades de combate⁶¹. Estas abarcan desde la mejora de las capacidades de posicionamiento, navegación y control de tiempos hasta los avances en detección por radiofrecuencia y óptica⁶². Los Gobiernos de Francia y Dinamarca colaboran en una batería de pruebas con un sensor cuántico para determinar el campo gravitatorio terrestre y estudiar cómo navegar mediante sistemas cuánticos en caso de que los servicios de navegación por satélite de posicionamiento global sufriesen interrupciones durante una crisis⁶³. Por último, con la adopción en 2023 de su estrategia cuántica nacional, el Reino Unido se comprometió a duplicar con creces la inversión en cuántica, invirtiendo 2.500 millones de libras en los próximos diez años⁶⁴. El Reino Unido también está desarrollando prototipos de sensores cuánticos para satélites compactos, llamados “CubeSats”, en el marco de una iniciativa para explorar las aplicaciones de la tecnología cuántica desde la Tierra al espacio exterior⁶⁵.

⁵⁸ Ibid.

⁵⁹ “Russia’s Quantum Patent Applications Decline Amid Sanctions”, *Moscow Times*, 14 June 2023, <https://www.themoscowtimes.com/2023/06/14/russias-quantum-patent-applications-decline-amid-sanctions-a81499>.

⁶⁰ Laura Kabelka, “Commission Announces Six Sites for European Quantum Computers”, Euractiv, 5 October 2022, <https://www.euractiv.com/section/digital/news/commission-announces-six-sites-for-european-quantum-computers/>.

⁶¹ Indra, “ADEQUADE: Advanced, Disruptive and Emerging QUAntum Technologies for DEfence”.

⁶² Ibid.

⁶³ Technical University of Denmark, “Navigation Quantum Sensor Being Tested in Greenland”, *The Mirage*, 12 June 2023, <https://miragenews.com/navigation-quantum-sensor-being-tested-in-1024820>.

⁶⁴ United Kingdom Department of Innovations, Science and Technology, “National Quantum Strategy”, 15 March 2023, <https://www.gov.uk/government/publications/national-quantum-strategy#full-publication-update-history>.

⁶⁵ Alanna Madden, “Researchers to Test Limits of Quantum Technologies with Nanoparticles in Space”, *Courthouse News Service*, 21 June 2023, <https://www.courthousenews.com/researchers-to-test-limits-of-quantum-technologies-with-nanoparticles-in-space/>.

Pasando al Indo-Pacífico, la Secretaría del Consejo de Seguridad Nacional de la India ha creado el Quantum Lab en la Escuela Militar de Ingeniería de Telecomunicaciones para mantenerse al día de las amenazas de la información cuántica a los sistemas militares, como la criptografía poscuántica (PQC)⁶⁶. El Gobierno japonés también ha anunciado que fabricará un ordenador cuántico nacional y creará cuatro centros de investigación cuántica.

En los últimos años ha quedado patente que las promesas de la tecnología cuántica están dando lugar a asociaciones cuánticas bilaterales y multilaterales, como evidencian los acuerdos firmados por Estados Unidos con Suiza, Japón y Australia⁶⁷. Las asociaciones son también una característica clave de la estrategia de tecnologías cuánticas de la OTAN, que destaca que “una alianza preparada para la cuántica requiere, ante todo, una cooperación más estrecha entre los aliados, y un ecosistema cuántico resistente que vaya más allá de la disponibilidad de financiación adecuada”⁶⁸.

Algunas previsiones anticipan que, para finales de 2027, probablemente los Estados y la industria privada hayan invertido más de 16.000 millones de dólares en computación cuántica⁶⁹.

⁶⁶ Indian Ministry of Defence, “Indian Army Establishes Quantum Laboratory at MHow (MP)”, 29 December 2021, <https://pib.gov.in/PressReleasePage.aspx?PRID=1786012>.

⁶⁷ Thomas Wong, “The United States and Switzerland Sign Joint Statement to Strengthen Collaboration on Quantum”, National Quantum Initiative, 21 October 2022, <https://www.quantum.gov/the-united-states-and-switzerland-sign-joint-statement-to-strengthen-collaboration-on-quantum/>; United States Department of State, “Tokyo Statement on Quantum Cooperation”, 19 December 2019, <https://www.state.gov/tokyo-statement-on-quantum-cooperation/>; The White House, “The United States and Australia Partner to Build Quantum Future”, 18 November 2021, <https://www.whitehouse.gov/ostp/news-updates/2021/11/18/the-united-states-and-australia-partner-to-build-quantum-future/>.

⁶⁸ North Atlantic Treaty Organization (NATO), “Summary of NATO’s Quantum Technologies Strategy”, 17 January 2024, https://www.nato.int/cps/en/natohq/official_texts_221777.htm.

⁶⁹ IDC, “IDC Forecasts Worldwide Quantum Computing Market to Grow to \$7.6 Billion in 2027”, 17 August 2023, <https://www.idc.com/getdoc.jsp?containerId=prUS51160823>.

6. Conclusión

Con su avance, la tecnología cuántica introduce en la seguridad internacional tanto un potencial transformador como riesgos complejos. Es esencial adoptar un enfoque holístico de la innovación cuántica —que tenga en cuenta todo el ciclo de vida, desde el desarrollo hasta el despliegue— a fin de comprender sus implicaciones para la estabilidad mundial y el control de armamentos. En particular, la posibilidad de que los ordenadores cuánticos pongan en peligro los protocolos criptográficos actuales subraya la importancia de la transición a las normas PQC. Esta transición será vital para proteger las infraestructuras críticas, las comunicaciones y los sistemas de defensa frente a las nuevas amenazas a la ciberseguridad.

Abordar estos retos exige una sólida colaboración entre los gobiernos, la industria y el mundo académico. Estas asociaciones intersectoriales son esenciales para cultivar una mano de obra preparada para la tecnología cuántica y mitigar las brechas digitales que podrían surgir con los avances en materia cuántica. Además, el desarrollo de marcos multilaterales de gobernanza, medidas de fomento de la confianza e iniciativas de fomento de la capacidad contribuirán a una innovación cuántica responsable.

La Ley de Amara afirma que “tendemos a sobreestimar el efecto de una tecnología a corto plazo y a subestimar su efecto a largo plazo”. Teniendo esto en cuenta, el futuro de la tecnología cuántica exige una actuación cuidadosa y coordinada.

Fomentando la cooperación y la preparación a escala mundial, la comunidad internacional puede integrar de forma responsable los avances cuánticos. De este modo las tecnologías cuánticas podrán convertirse en herramientas que promuevan la estabilidad y la seguridad, en lugar de en fuentes de conflicto y perturbación.