Revista del Instituto Español de Estudios Estratégicos
ISSN-e: 2255-3479

Iván Soto Maciá
Ingeniero informático y Máster en Inteligencia. Experto en ciberseguridad, estrategia y prospectiva

Correo: adventt@protonmail.com

Distribución cuántica de claves y su impacto geopolítico

Quantum key distribution and its geopolitical impact

Resumen

Durante los próximos años, la seguridad de la información se enfrentará a uno de los retos más significativos en la historia de la criptografía moderna, un cambio profundo en las reglas del juego: el advenimiento de los ordenadores cuánticos. El posicionamiento ante el problema de la distribución cuántica de claves resultará vital para las principales potencias globales de nuestro siglo. Estados Unidos y China representan las dos posturas prevalentes: mientras que Estados Unidos muestra un cauto escepticismo, China ha hecho una apuesta decidida. El artículo explora las razones más relevantes detrás de una y otra aproximación, los desafíos que presenta la tecnología, las expectativas de resolución y los principales avances científicos. Posteriormente, presentamos las implementaciones prácticas más importantes hasta la fecha, qué estrategia subyace detrás de estas y cómo los distintos actores pretenden proyectar su visión del futuro de las comunicaciones seguras. Un futuro favorable a sus intereses.

Palabras clave

Comunicaciones cuánticas, Computación cuántica, Supremacía, Seguridad, Confidencialidad, Disponibilidad, Resiliencia.

Abstract

Over the next few years, information security will face one of the most significant challenges in the history of modern cryptography, a profound change in the rules of the game: the advent of quantum computers. The positioning of the problem of quantum key distribution will be vital for the major global powers of our century. The US and China represent the two prevailing positions: while the US shows cautious skepticism, China has made a determined bet.

The article explores the most relevant reasons behind both approaches, the challenges presented by technology, resolution expectations and major scientific advances. Then, we present the most important practical implementations to date, what strategy is behind them and how different actors intend to project their vision for the future of secure communications. A future that is in their best interests.

Keywords

Quantum communications, Quantum computing, Supremacy, Security, Confidentiality, Availability, Resilience.

Citar este artículo:

Soto Maciá, I. (2025). Distribución cuántica de claves y su impacto geopolítico. *Revista del Instituto Español de Estudios Estratégicos*. Madrid, Ministerio de Defensa. 25, pp. 213-234.

1 Introducción

No es aventurado decir que, con el avance de la computación cuántica, durante los próximos años seremos testigo de un cambio de paradigma significativo y profundo en los protocolos de comunicación segura. Uno que requerirá tiempo de adaptación, grandes esfuerzos e inversión, y una clara visión de futuro. De lo acertado de su prospectiva, cómo construyan esa visión, cuánto esfuerzo prevean necesario y cuán bien se preparen los distintos actores dependerá el resultado para las principales potencias geopolíticas en las décadas venideras.

Frente a los ordenadores clásicos, los cuánticos ofrecen una resolución exponencialmente más rápida de problemas matemáticamente complejos y, por ello, supondrán el fin de los algoritmos actualmente preponderantes en criptografía asimétrica (por ejemplo, intercambio de claves Diffie-Hellman, RSA o los algoritmos de curva elíptica). O lo que es lo mismo, obligarán a replantearse los actuales protocolos para el intercambio de claves y firma digital asimétrica. El consenso académico es que no se trata de si será o no posible, sino de cuándo. Es decir, estamos ante un desafío fundamentalmente de ingeniería.

Ante esta situación, los esfuerzos parecen centrarse en el desarrollo de criptografía poscuántica, o *quantum-resistant*, con el NIST a la cabeza en la proposición de nuevos estándares [1]. Debido a que estos algoritmos criptográficos están diseñados para su ejecución en ordenadores clásicos, los problemas a superar tienen que ver con el incremento en la demanda de capacidad de cómputo, tiempo consumido en las comunicaciones y tiempos de adopción/adaptación por parte de los actores implicados.

Este artículo, sin embargo, se centra en una línea potencialmente complementaria, la distribución cuántica de claves (QKD, por sus siglas en inglés). Planteada por primera vez en los trabajos de G. Brassard y Charles H. Bennett entre 1979 [2] y 1984 [3], y llevada a la práctica por DARPA en 2002, QKD utiliza las propiedades fundamentales de la mecánica cuántica para generar claves de longitud variable realmente aleatorias[1] y, lo que es más relevante, garantizar la seguridad (principalmente confidencialidad e integridad) en la distribución de claves criptográficas. Es este anclaje en propiedades fundamentales el que permite aspirar a superar no solo los problemas presentes, sino también definitivamente los futuros, redefiniendo *de facto* cómo entendemos la seguridad de la información.

Aunque, actualmente, las barreras tecnológicas y económicas limitan su implementación a gran escala, el desarrollo continuo del *hardware* específico podría reducir de forma significativa los costos en el futuro, posicionándola como una solución fiable y generalizada, al menos en el *backbone* de las redes críticas. Estamos, como en el caso de los ordenadores cuánticos, ante un problema de ingeniería superable.

1 La importancia de la generación cuántica de claves, realmente aleatorias y de longitud suficiente para implementar cifrados como OTP o libreta de un solo uso, no es objeto de este artículo, si bien debería considerarse como una ventaja más de la adopción de QKD.

Este artículo pretende explorar la importancia de QKD, los esfuerzos en el desarrollo e implementación de las grandes potencias geopolíticas, su potencial para enfrentar las amenazas cuánticas y cómo las innovaciones futuras podrían generalizar su adopción.

2 Contexto y protocolos

2.1 Contexto

La criptografía ha sido, históricamente, el pilar que ha sostenido la seguridad de la información. En la era digital, la criptografía moderna garantiza los principios fundamentales de una comunicación segura: la confidencialidad, la integridad y la autenticidad de los mensajes. Y esto, a su vez, resulta básico para mantener nuestro estilo de vida. Desde el comercio electrónico, las operaciones bancarias, hasta la seguridad de las comunicaciones de mando y control militar, todo se fundamenta en modernas técnicas criptográficas.

Estos protocolos se basan, en su mayoría, en cifrado simétrico, que requiere un intercambio previo de claves. Este problema de distribución de claves está en el centro del artículo y la mejor solución que podemos ofrecer, hoy en día, es la criptografía asimétrica o de clave pública.

Como ya hemos referido en la introducción, la criptografía asimétrica basa su fortaleza en problemas matemáticamente complejos, como la factorización de números primos o el cálculo de logaritmos discretos, considerados intratables para los ordenadores clásicos. Sin embargo, los ordenadores cuánticos, que tienen como característica distintiva basar el cómputo en propiedades elementales de la materia, suponen, más que un mero salto en capacidad de procesamiento, un cambio de paradigma en las posibilidades algorítmicas y de programación. Nuevas y más eficientes formas de abordar problemas. Algoritmos como el de Shor [4], diseñados específicamente para estas arquitecturas, podrán resolver en minutos estos problemas hasta ahora intratables, dejando obsoletos, al momento, todos los sistemas actuales de distribución de claves.

Frente a los ampliamente citados esquemas criptográficos poscuánticos publicados por NIST en 2024 (uno de ellos permite la distribución de claves o KEM, por sus siglas en inglés [1]), QKD supone una solución más disruptiva, arriesgada, pero con potencialidad para llegar más lejos, para ser definitiva.

Lo que hace única a QKD es que no depende de algoritmos matemáticos, sino de principios físicos fundamentales, por lo que, a priori, su vigencia será independiente de los avances relativos a teoría de computación. Utilizando partículas cuánticas como fotones, QKD garantiza que cualquier intento de interceptar la clave a ser compartida (que posteriormente se utilizará en el cifrado simétrico), es decir, cualquier intento de obtener información respecto a la clave, la alterará y será en consecuencia detectable: en el mundo cuántico no se puede observar sin dejar huella.

Aunque este enfoque presenta muchas ventajas, Occidente no parecía, hasta la fecha, apostar por él y las agencias de inteligencia de señales subrayaban los problemas y desafíos

que presenta QKD en diversas publicaciones [5]. Estas limitaciones han sido ampliamente discutidas, destacando por relevancia, en mi opinión: (i) el problema de la autenticación de la fuente (ii) el alto coste del *hardware* necesario (iii) las limitaciones técnicas de las redes cuánticas actuales, y (iv) los problemas de denegación de servicio. No obstante, el estado del arte avanza a diario, y las inversiones de los grandes estados, fundamentalmente China, evidencian lo que está en juego. A su vez, poco a poco, parece que Occidente se une a la carrera.

La historia de la tecnología demuestra que lo que anteriormente hemos referido como problemas de ingeniería tienden a convertirse en algo trivial con el paso del tiempo. Cuando esa niebla se disipe, lo que tendremos encima de la mesa es una posible solución final al problema de generación y distribución de claves.

2.2 Protocolos

La familia de protocolos QKD cumple ya más de cuarenta años desde las primeras estandarizaciones, por lo que las publicaciones acerca de estos, su modo de funcionamiento y los principios subyacentes son numerosas [6].

Así pues, no pretendemos entrar, en este punto, en detalles técnicos, pero es de reseñar que todos ellos comparten muchos puntos comunes. Partiremos de la necesidad de emisor y receptor (por convención, Alice y Bob) de compartir una clave secreta que emplearán, posteriormente, para cifrar simétricamente. Para todos los protocolos QKD aceptados como estándar, se precisan dos fases: (i) la fase de transmisión cuántica, donde el emisor y el receptor envían o miden estados cuánticos, y (ii) la fase de posprocesamiento, donde se genera la clave segura.

Además, en los protocolos QKD son necesarios dos canales, un canal cuántico y un canal clásico donde tiene lugar el proceso de intercambio de mensajes una vez hemos acordado la clave secreta.

Sobre estos puntos comunes, distinguiremos dos familias de protocolos QKD:

2.2.1 Basados en una canal cuántico emisor-receptor (comúnmente conocidos como prepare and measure)

Aquellos canales en los que la transmisión de la clave se inicia con un rayo de fotones codificados mediante el método de polarización. En la lectura, se aplicarán filtros cristalinos que, de forma similar a unas gafas de sol, filtrarán o no el fotón en función de su polarización. Así, destacamos los siguientes protocolos:

– BB84: en 1984 los mencionados G. Brassard y Charles H. Bennett propusieron el primer protocolo de Distribución de Claves Cuánticas, conocido como BB84 por sus apellidos y el año de su publicación. Además de ser el primero, el resto de los protocolos *prepare and measure* son variaciones de BB84 por lo que se aplican en las mismas circunstancias, y están sujetos a las mismas ventajas y limitaciones.

La fase de transmisión cuántica consiste fundamentalmente en que, partiendo de dos bases de polarización, rectilínea[2] y diagonal[3], Alice enviará los bits de la clave secreta codificados eligiendo, para cada uno de ellos, una de las bases de forma aleatoria. Bob, a su vez, medirá los fotones recibidos aplicando, asimismo, una de las dos bases también de forma aleatoria.

En la fase de posprocesamiento, Alice y Bob comparten públicamente las bases que han usado. De este modo, en aquellos bits donde hayan usado la misma base, la lectura será correcta y pasarán a formar parte de la clave, mientras que aquellos bits donde la base del emisor y del receptor difieran serán descartados. Cualquier intento de obtener información del canal cuántico por parte de un tercero modificará la polarización de los fotones, generando errores de medición por parte de Bob, y en consecuencia errores en la clave secreta generada. En dicho caso, Alice y Bob abortan la comunicación.

- B92: publicado por Charles Bennett en 1992, es una variante del anterior en el que el emisor usa únicamente dos estados de polarización no ortogonales.
- SARG04: otra variante de BB84, muy similar, pero especialmente robusta frente a los ataques *photon-number splitting*, que afectan especialmente a BB84 y B92.

2.2.2 Basados en entrelazamiento cuántico

Basan su funcionamiento en un principio diferente que la familia de protocolos derivados de BB84: el entrelazamiento cuántico. En el ámbito de QKD el entrelazamiento cuántico significa que, en el caso de dos partículas entrelazadas, cualquier medición aplicada a una de ellas afecta instantáneamente el estado de la otra. De este modo, las partículas están perfectamente correladas y es posible lograr una sincronización direccional en las observaciones. Esto es cierto independientemente de la distancia entre las partículas entrelazadas. Sin embargo, es imposible predecir antes de la medición qué estado se observará, por lo que no es posible comunicarse a través de partículas entrelazadas sin discutir las observaciones a través de un canal clásico. Destacamos los protocolos:

- BBM92 y E91: publicados respectivamente por Charles Bennett, Gilles Brassard y David Mermin en el 92 y Artur Ekert en el 91. En estos casos, debe existir una fuente confiable que emita los fotones entrelazados a Alice y Bob, como parte del canal cuántico.

Como atestiguaremos posteriormente, en el caso de la red cuántica más importante desplegada hasta la fecha, la red china, ambas tipologías de protocolos tienen aplicación práctica, siendo los protocolos de la familia BB84 los más habituales en *backbones* metropolitanos e interurbanos (terrestres) y los protocolos de la familia BBM92 y E91 los usados para la comunicación satelital global.

2 Corresponde a medir la componente vertical del espín, con estados 0 y 1.

3 Corresponde a medir la componente horizontal del espín, con estados + y -.

3 Desafíos y expectativas de resolución

Cualquier tecnología emergente enfrenta una serie de desafíos que dificultan su implementación a gran escala. Estos problemas, en mi opinión, no son insuperables, pero requieren de un esfuerzo coordinado de la comunidad científica, la industria y los Gobiernos, algo que suena poco factible en la dinámica de carrera actual.

3.1 Autenticación de la fuente

Reseñado porque aparece, recurrentemente, como uno de los grandes problemas de QKD, no es, de hecho, un problema propiamente dicho, sino una limitación esencial. En dicho sentido, estamos ante un falso debate. QKD es una solución, como su nombre indica, al problema de distribución de claves (y, colateralmente, al problema de la generación de claves aleatorias), no una solución «integral» criptográfica. Seguirá requiriendo de apoyo para el proceso de autenticación de la fuente (claves precargadas, o la futura criptografía asimétrica poscuántica), del mismo modo que seguirá necesitando de canales clásicos para la transmisión del mensaje propiamente dicho, mediante criptografía simétrica tradicional.

Conviene puntualizar, no obstante, que hablamos de la autenticación inicial de la fuente en un canal punto a punto (con escasa probabilidad de intervención de terceros), dado que, una vez se ha generado y distribuido la primera clave secreta, esta misma puede sustituir a las claves precargadas sirviendo para la autenticación de las partes (y continuar actualizando el proceso con cada nueva clave generada y distribuida).

3.2 Dependencia del hardware

En este sentido es donde podemos encontrar perspectivas más alentadoras en el futuro cercano.

En relación con el coste del *hardware*, es cierto que para implementar QKD se necesita *hardware* especializado, como fuentes de fotones individuales, detectores avanzados y redes de fibra óptica dedicadas. Estos equipos, además de ser caros, todavía no se producen a gran escala, lo que los hace inaccesibles para la iniciativa privada. Esto es aún más acuciante en el caso de las redes basadas en satélites cuánticos.

No obstante, la historia de la tecnología nos ha enseñado que, con el tiempo, los costos tienden a disminuir a medida que se producen avances en la fabricación y aumenta la demanda. En el caso de QKD, la miniaturización de los componentes y la producción de *hardware* más asequible serán factores clave. Las tecnologías fotónicas integradas, por ejemplo, prometer reducir significativamente el coste al permitir que muchos componentes esenciales de QKD se fabriquen de forma integrada.

En cuanto a la vinculación *hardware* de QKD, es decir, la imposibilidad de emular principios físicos fundamentales mediante *software* es un problema que, si bien persistirá,

puede avanzarse en gran medida en su mitigación. En dicho sentido, por ejemplo, son destacables los avances en *Device-independent Quantum Key Distribution* (DI-QKD, por sus siglas en inglés), que promete cierto desacoplamiento de las especificaciones *hardware* concretas [7], relajando la necesidad de modelar físicamente parámetros específicos. Basado en el protocolo Ekert 91 y, dependiente de un entrelazamiento de alta calidad, distintas pruebas de concepto han sido ofrecidas al respecto durante los últimos años. De continuar su avance, podría ser una solución, colateralmente, a todos los ataques que explotan vulnerabilidades técnicas asociadas a los equipos QKD actualmente operativos.

3.3 Limitaciones técnicas

Otro gran desafío es la limitación en la distancia que pueden cubrir las redes QKD. En las fibras ópticas (medio prevalente en las redes interurbanas) los fotones que trasportan la información se atenúan rápidamente, lo que hace que la señal pierda fuerza después de unos pocos cientos de kilómetros. Aunque los satélites han demostrado ser efectivos para superar ese problema, su uso aún es experimental y extremadamente costoso, por lo que su adopción masiva aún enfrenta barreras significativas.

Al respecto, una de las soluciones más prometedoras para superar las limitaciones de distancia son los repetidores cuánticos. Estos dispositivos, aún en pleno proceso de investigación, actúan como un repetidor de señal al uso: permiten que las señales cuánticas se retransmitan sin perder su integridad. Aunque esta tecnología todavía no está lista para el despliegue comercial, los avances en este campo están siendo vertiginosos y podrían impactar en la distancia de distribución de forma muy acusada.

Otra de las limitaciones técnicas a destacar es la dificultad de integración de la infraestructura QKD en las actuales o *Legacy*. Como hemos comentado, QKD requiere protocolos y equipos completamente nuevos, lo que complica su adopción, en un entorno ya suficientemente estresado en la adaptación e implantación de criptografía poscuántica. Esto supone un dilema para empresas y Gobiernos, y es la causa probable de la priorización de inversiones en criptografía poscuántica frente a QKD en la esfera occidental.

En este sentido, los ojos están puestos en el desarrollo de estándares de interoperabilidad. Los protocolos QKD, por definición, necesitan ser interoperables con los protocolos de cifrado clásico (dependen de canales clásicos de cifrado simétrico), pero hay aún mucho trabajo por hacer en aquello que queda fuera del ámbito QKD, como la autenticación del canal o los protocolos de firma digital.

Este es, sin duda, el ámbito en el que puede liderar el tercer actor en discordia, Europa, que sigue siendo un referente en cualquier aspecto relacionado con normar o estandarizar. Resultan especialmente relevantes los esfuerzos del Comité Europeo de Normalización (CEN) y Normalización Electrónica (CENELEC) en materia de tecnología cuántica. En lo tocante a QKD, destaca el papel del Instituto Europeo de Normas de Telecomunicaciones (ETSI, por sus siglas en inglés) y su grupo de trabajo dedicado a la estandarización de QKD (ETSI ISG-QKD), o la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés), que publicó en 2020 el

estándar *Overview on networks supporting quantum key distribution*. No obstante, por la madurez del campo, QKD aún no ha pasado por un proceso de estandarización riguroso, como el ya referenciado y llevado a cabo por NIST para criptografía poscuántica. Aún está por determinar quién será el actor hegemónico en ese sentido.

3.4 Problemas de denegación de servicio

El camino hacia un QKD resiliente no va a ser sencillo. Como hemos apuntado, la seguridad de QKD reside en la imposibilidad de obtener información sobre la clave distribuida sin modificarla y generar, en consecuencia, errores de medición entre emisor y receptor original (Alice y Bob). Por ello mismo, es relativamente sencillo realizar ataques que no busquen descifrar la clave, sino interrumpir o degradar el sistema, haciéndolo inoperable o extremadamente lento. En sistemas críticos, estos ataques de denegación de servicio (DoS, por sus siglas en inglés) suelen tener un impacto crítico, la disponibilidad acostumbra a ser tan relevante (en ocasiones más) como la confidencialidad.

Los ataques DoS sobre sistemas QKD pueden tomar distintas formas. Mediante la saturación del canal cuántico, un atacante inunda el canal con señales no deseadas, por ejemplo, fotones adicionales. Esto provoca un aumento de la tasa de error cuántico (QBER, por sus siglas en inglés) y que Alice y Bob descarten constantemente las claves generadas, retrasando o interrumpiendo el intercambio. La sobrecarga de detectores consiste en enviar pulsos de luz de intensidad superior a la esperada, dañando físicamente este equipo, particularmente sensible [8]. Para finalizar, ya hemos comentado que una comunicación que implique QKD depende, en último término, de un canal clásico, por lo que no deja de ser susceptible a cualquier ataque al mismo, si bien estas vulnerabilidades no son achacables, evidentemente, a las tecnologías QKD.

Como soluciones específicas, merece la pena destacar la implementación de filtros ópticos avanzados para el bloqueo de señales no deseadas antes de que lleguen a los detectores, configurados con el patrón de características de Alice (si bien esto convierte el canal en algo aún más específico para un emisor y receptor concreto). Sin embargo, la respuesta por defecto de estos filtros ópticos es la desconexión del canal, lo que evita que se dañen los detectores, pero no solventa en ningún caso el objetivo original del DoS.

Frente a estas modalidades de ataque, construir resiliencia, aumentar la protección física y dotar de duplicidad (rutas alternativas) llegado el caso, se antoja incluso más relevante que en infraestructuras clásicas, donde prácticamente la totalidad de rutas, elementos de distribución y protocolos son interoperables. Adicionalmente, estas rutas alternativas deben ser gestionadas en tiempo real y en virtud de las observaciones cuánticas y la constancia de un ataque DoS sobre las mismas. En dicho sentido, una de las líneas de investigación más prometedora es la que pretende incorporar la tradicional gestión de redes definidas por *software*[4] (SDN, por sus siglas en inglés) a los protocolos QKD

4 IBM describe las redes definidas por *software* como un enfoque en el que mediante el uso del *software* se crea y opera una serie de redes de superposición virtual que funcionan juntamente con una

[9]. Incorporando los componentes propios de una red óptica QKD como parte de la capa de abstracción y gestión SDN, y estableciendo una monitorización constante de QBER y la tasa de generación de claves secretas (SKR, por sus siglas en inglés), es posible detectar degradaciones de servicio y, rápidamente, identificar rutas alternativas para evitar o mitigar el efecto del ataque DoS. Todo esto, en unos tiempos mucho más ajustados que los obtenidos mediante una gestión directa de la infraestructura QKD. No obstante, en último término, no estamos más que ante la construcción y gestión eficiente de rutas alternativas y resiliencia operacional.

En consecuencia, y de momento, podemos concluir que los canales QKD están más expuestos a los ataques DoS que los canales clásicos, y ninguna de las medidas de mitigación actuales parecen poder solventar este punto. El apoyo en las propiedades físicas de las partículas cobra su peaje, lo que ganamos de confidencialidad en el canal, debemos estar dispuestos a entregarlo en concepto de disponibilidad. Como alternativa, invertir más en la construcción de resiliencia en una infraestructura de por sí costosa.

Distribución de claves mediante criptografía postcuántica frente a la distribución cuántica de claves

Característica	Criptografía postcuántica	Distribución cuántica de claves
Principio de funcionamiento	Algoritmos criptográficos basados en problemas matemáticos resistentes a ataques cuánticos	Propiedades fundamentales de la mecánica cuántica para garantizar la seguridad
Dependencia de *hardware* especializado	No presenta dependencias, y puede ejecutarse en infraestructuras digitales clásicas	Sí, requiere de equipos cuánticos especializados, aún no producidos a gran escala y de alto coste
Limitaciones técnicas	Moderadas, requiere análisis de interoperabilidad de protocolos dependientes de criptografía clásica	Relevantes, limitaciones asociadas a la distancia de distribución de claves por atenuación de la señal, y a la interoperabilidad con infraestructura clásica
Resiliencia	Ninguna debilidad intrínseca	Altamente vulnerable a ataques de denegación de servicio
Madurez tecnológica	Alta, con estándares publicados para el intercambio de claves (FIPS 203, ML-KEM) que han sido incluidos en paquetes de funciones criptográficas (OpenSSL 3.5, desde abril de 2025)	Baja, aún en desarrollo y con despliegues experimentales
Escalabilidad	Alta, fácilmente implementable en redes actuales	Baja a media, limitada por distancia, atenuación y necesidad de repetidores cuánticos
Complejidad y coste de implementación	Moderada, requiere de actualización de protocolos y *software/hardware,* pero no rediseño físico	Alta, requiere de nueva infraestructura física cuántica
Latencia y rendimiento	El proceso de intercambio de claves es rápido, a pesar de que las claves son del orden de 10 veces el tamaño de una clave clásica	Más lento que la criptografía postcuántica, depende del canal cuántico y el protocolo de intercambio
Detección de intrusión	No, protección basada en complejidad matemática	Sí, detección inherente

Figura 1. Fuente: elaboración propia

red subyacente física. Las SDN proporcionan el potencial de minimizar el tiempo práctico necesario para administrar la red.

4 Posicionamiento geopolítico

4.1 ¿Quién va por delante en la carrera cuántica?

Respecto al posicionamiento de las grandes potencias en tecnología cuántica (QSI, por las siglas en inglés de *Quantum Information Science*, concepto que engloba tanto comunicaciones cuánticas como computación cuántica, entre otros), un análisis superficial nos obligaría a concluir que China lleva la delantera. Bajo cualquier métrica cuantitativa, la distancia es importante frente a su más inmediato perseguidor, Estados Unidos. No obstante, como en la física cuántica, la lectura no es tan trivial:

– Volumen de inversión: si algo se puede afirmar es que las grandes potencias, particularmente China y Estados Unidos, están dedicando considerables esfuerzos en QSI, si bien hay marcadas diferencias. Para China, el liderazgo en QSI es una cuestión estratégica de largo alcance y así lo refleja en su decimotercero (2016-2020) y decimocuarto (2021-2025) plan quinquenal. Respaldando su aseveración con cifras, asegura haber invertido más de quince billones de dólares americanos hasta la fecha (2023), frente a la estimación de 3,8 billones de Estados Unidos [10] en el mismo periodo. Sin embargo, es difícil precisar el verdadero alcance de la inversión china debido a la tradicional opacidad de su gasto gubernamental. Algunos informes sugieren que el gasto real podría ser menor, lo que refleja un patrón común en el que los ambiciosos objetivos de financiación no siempre se cumplen plenamente.

  Al margen de los detalles y atendiendo a la evidencia empírica, o lo que es lo mismo, a las infraestructuras cuánticas desplegadas sobre el terreno, no obstante, no cabe ninguna duda de que la inversión china es significativamente superior a la estadounidense, europea, japonesa, etc.

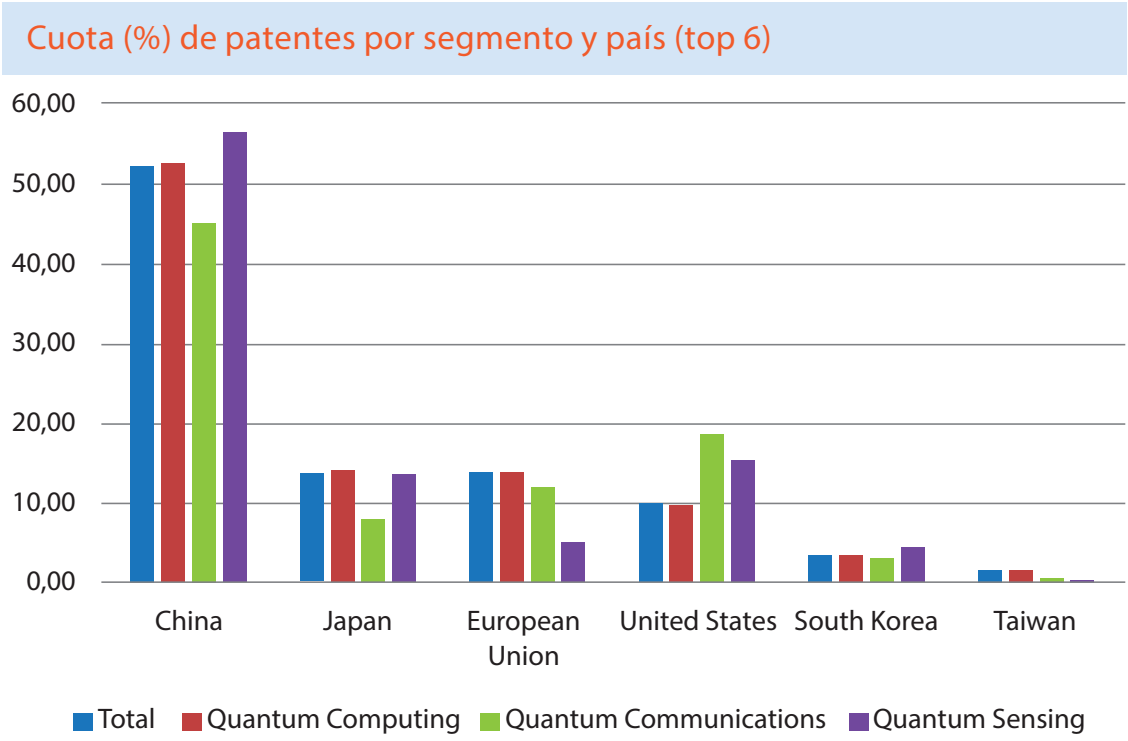

Figura 2. Fuente: McKinsey & Company Quantum Monitor 2023 [11]

– Naturaleza de la inversión: siguiendo el patrón habitual, la inversión china es fundamentalmente pública y el criterio de decisión parte de una fuente única, el partido (lo que se demostrará relevante a la hora de determinar la estrategia). De todo el tejido empresarial chino, solo catorce empresas han contribuido significativamente, de acuerdo con el criterio de patentes y publicaciones (destacan Huawei, Alibaba, QuantumCTek o Ruban Quantum Technology, si bien la participación estatal en estas empresas hace dudar de la calificación de inversión privada). Esto contrasta fuertemente con Estados Unidos, donde la inversión es de naturaleza fundamentalmente privada (impulsada por IBM, Google, Microsoft o Intel). En materia de *start-ups*, la inversión estadounidense es diez veces superior a la china [10].
– Patentes: si atendemos al número de patentes domésticas, China destaca con un volumen muy superior al de Estados Unidos [11]. La tipología de patentes refleja el foco chino en las comunicaciones, particularmente en QKD, como veremos en posteriores apartados. Estados Unidos, sin embargo, lidera en número de patentes internacionales [10], lo que subraya su vocación de establecer estándares más allá de sus fronteras. En el caso de China, la naturaleza de la investigación y la compartición de conocimiento es asimétrica, cerrada al exterior.
– Publicaciones: de nuevo, China lidera significativamente el ranking de publicaciones [10]. Es habitual, en otros campos tecnológicos como la inteligencia artificial, mencionar que cantidad no es calidad, y en términos de calidad (citas, referencias, *H-index*) e impacto, Estados Unidos se mantiene por delante. No es el caso de QSI, donde la calidad de las publicaciones chinas también está (ligeramente) por delante de las estadounidenses. De nuevo, la distribución de publicaciones QSI por tipología evidencia que la estrategia china es distinta a la estadounidense, lo que trataremos a continuación.

4.2 Diferentes estrategias para la supremacía cuántica

Lo cierto es que, atendiendo a los criterios anteriormente comentados (inversión, naturaleza de la inversión publicaciones y patentes), puede observarse que la estrategia de las dos grandes potencias es marcadamente diferente.

Tomemos como punto de partida una taxonomía de los campos de estudio más prometedores de QSI que diferencie entre computación cuántica, comunicaciones cuánticas y tecnología de sensores/sensorización. Para todos los criterios mencionados, el liderazgo chino es apabullante en comunicaciones cuánticas [10], [11] y [12], en sensorización la situación es pareja, mientras que, en computación cuántica, Estados Unidos lidera ampliamente.

Como ejemplo ilustrativo, en cuanto a las publicaciones asociadas a comunicación cuántica (fundamentalmente QKD) China lidera con el 38 % global, frente al 12,5 % de Estados Unidos, con un H-index de 48 frente a 43. En el caso de computación cuántica, el volumen de publicaciones es similar (23 % de cuota china frente al 21 % estadounidense), pero el H-index americano es muy superior (52 chino frente a 92 estadounidense).

En cuanto a patentes internacionales, durante el periodo 2016-2021, China publicó 3601 patentes en comunicación cuántica frente a las 551 de Estados Unidos, mientras que, en relación con la computación cuántica, la situación es la opuesta, con 1408 patentes por parte de China y 2509 por parte de Estados Unidos [12].

La determinación china de liderar la tecnología cuántica en 2035 es fuerte y parte central del plan de Xi Jinping para mejorar la competitividad del país. Lo que constituye una anomalía es que, a diferencia de otros actores (no todos), la investigación y el despliegue de infraestructura de comunicaciones cuánticas sigue siendo una prioridad dentro de su estrategia a medio y largo plazo. En dicho sentido, nadie ha impulsado planes tan ambiciosos como los chinos.

4.3 QKD, estado del arte

China se ha consolidado como líder indiscutible en QKD, tanto en términos de inversión como de implementación práctica, en una apuesta que ya puede considerarse de largo recorrido: desde 2008, mucho antes del reflejo tangible en los planes quinquenales, las declaraciones de físicos como Chen Zengbing [13] apuntaban en esa dirección. Pero, quizá, el gran espaldarazo a nivel de inversiones se dio en 2013, tras las filtraciones de Snowden, que generaron un gran impacto y sensación de inseguridad en el politburó.

El plan de China implica construir una red QKD que abarque los grandes troncales (*backbones*) de comunicación, aplicando distintas tecnologías en función de la capilaridad [14]. Fundamentalmente:

- Comunicación cuántica en *backbones* metropolitanos mediante fibra óptica y emisores receptores miniaturizados.
- Comunicación cuántica en *backbones* interurbanos donde los repetidores cuánticos jugarían un papel fundamental.
- Comunicación cuántica global, entre distintos *backbones* interurbanos mediante retransmisión satelital.

Alcanzaron el primer hito la comunicación cuántica urbana entre 2011 y 2013, cuando las redes metropolitanas de Hefei y Jinan fueron plenamente operativas. A estas, les siguieron las redes metropolitanas de Beijing y Shanghái y, finalmente, alcanzaron el segundo hito: desde 2017 puede considerarse funcional la mayor red terrestre QKD del mundo, con una extensión de más de 2000 kilómetros en el *backbone* principal, que une Beijing, Jinan, Hefei y Shanghái.

Respecto al tercer hito, una comunicación cuántica global, su avance más significativo fue el lanzamiento del primer satélite cuántico, «Micius», en 2016, que permitió realizar las primeras transmisiones QKD a escala global: es decir, transmisiones QKD capaces de distribuir claves entre, por ejemplo, Asia y Europa. Con esto, China mostraba que otra red global, un internet cuántico, era posible. Un primer paso más allá de las redes locales e interurbanas. A «Micius» le ha seguido en 2022 un segundo satélite, «Jinan-1», con un grado de miniaturización reseñable, y entre dos y tres veces más rápido en la

generación de claves. El periodo entre 2025 y 2027 será clave, con el lanzamiento previsto de varios satélites de órbita terrestre baja y media, que complementarán las funciones de los anteriores [15].

Dicho de otra manera, la apuesta por lograr una red QKD completa (*satellite-to-ground*) se mantendrá en el tiempo. Actualmente, la combinación entre los 3 niveles comentados, es decir, desde «Micius» hasta los nodos del *backbone* Beijing-Shanghái ya permite la distribución de claves en comunicaciones de más de 4600 kilómetros [16].

Evidentemente la red no es plenamente autónoma. Para lograr una comunicación punto a punto sigue precisando de capas de acceso y distribución basadas en tecnologías tradicionales, y nunca se ha pretendido que fuera de otra manera. Se trata de proteger las comunicaciones sensibles entre los nodos más relevantes de la red. El resto de los pasos para lograr una comunicación punto a punto segura dependerán de la confidencialidad de la comunicación: los primeros beneficiarios de la red de comunicaciones cuántica serán el ejército y las agencias gubernamentales, extendiéndose posteriormente a sectores críticos de la economía, como el sector financiero, intensivo en el uso de comunicaciones altamente sensibles.

El liderazgo de China en QKD le otorga una ventaja estratégica clave en seguridad y comunicaciones. Esta capacidad permite a China asegurar sus redes críticas (de momento militares, gubernamentales y financieras) frente a posibles ataques futuros de computación cuántica, algo que pocos países pueden afirmar. Además, su capacidad para exportar infraestructura cuántica a otros países podría consolidar su influencia geopolítica, especialmente en el ámbito de la Ruta de la Seda Digital.

El estado del arte es claro: China lidera los avances en QKD y mantiene una posición sólida en el resto de los campos, mientras que Estados Unidos centra sus esfuerzos en computación cuántica y sensorización, y en lo que a criptografía se refiere, prioritariamente en criptografía poscuántica.

En materia de QKD, la mayoría de los actores globales van un paso por delante de Estados Unidos. Entre los avances más reseñables, destacan:

– Europa (con el proyecto EuroQCI [17]) tiene como objetivo declarado la construcción de una infraestructura de comunicación cuántica segura que abarcará toda la UE, incluidos sus territorios de ultramar. Al igual que otros muchos países, el punto de partida es también la construcción de un *backbone* que una las instituciones gubernamentales e infraestructuras críticas, complementando a la red tradicional (que seguirá aportando la mayor capilaridad y alcance). Este objetivo es ambicioso y los plazos programados muestran compromiso y visión de futuro, pero también la habitual lentitud de la UE. 2019 fue el año de puesta en marcha del programa, las iniciativas relacionadas con el segmento terrestre arrancaron en 2023 y las asociadas con el segmento espacial lo harán con el lanzamiento del primer satélite previsto para 2025/2026.

  La infraestructura contará con un conjunto de nodos principales (a saber, Madrid, Viena, Berlín y Poznan) y, desde estos, ramificaciones hacia el resto de países miembro. Aunque estas uniones, actualmente, no van más allá de pruebas

de concepto, si es destacable el grado de avance dentro de los nodos principales. Particularmente Madrid, cuya red cuántica metropolitana (MadQCI) es la mayor de Europa, y en constante crecimiento desde 2009. Actualmente cuenta con veintiséis módulos QKD en nueve nodos, conectados por 110 kilómetros de fibra óptica. Para su gestión, MadQCI utiliza SDN, opción en crecimiento por, entre otras ventajas, las ya mencionadas en este artículo respecto a la gestión, administración y construcción de resiliencia. Su desarrollo es obra de una iniciativa de colaboración público-privada, con contribuciones de la Universidad Politécnica de Madrid, Huawei o Toshiba, entre otros.

– Reino Unido, por su parte, ha seguido un camino muy similar al de Europa continental. La red metropolitana de Londres está operativa desde 2022 [18]. En este caso, aunque con el respaldo del Gobierno, la iniciativa es fundamentalmente privada, con BT y Toshiba a la cabeza y, a diferencia de otras redes cuánticas, podría considerarse la primera red «comercial», dado que, desde su puesta en producción, está abierta a la integración de cualquier cliente que pague por ello, sea o no una infraestructura crítica para el Estado. Desde entonces, la red metropolitana ha crecido, integrando clientes como HSBC [19], con conexiones entre centros de datos en distancias de hasta 62 kilómetros.

– Japón, es quizá el país donde la iniciativa privada en QKD es más potente. Toshiba y NEC son la primera y tercera compañía por número de patentes QKD internacionales, con NTT, Fujitsu y Hitachi también como actores relevantes. Tokio cuenta, desde 2010 [20], con su propia red QKD metropolitana, y se espera que, para 2035, se haya extendido la red cuántica al resto del país, constituyendo una red de cobertura nacional. Podría decirse que, al margen de China, son los primeros en enfrentar los problemas de implementación práctica, lo que los ha llevado a replantear e incluso «reconstruir» sus redes en varias ocasiones. Como contrapartida, la influencia de sus compañías a nivel internacional es prevalente (sirva como ejemplo la implicación de Toshiba en las redes europeas).

– Corea del Sur, con compañías privadas como la suiza ID Quantique[5], SK Telecom, LG, e iniciativas públicas como ETRI en vanguardia, ha desplegado la segunda red cuántica más extensa del mundo, tras la China. Se trata de un *backbone* QKD a nivel nacional, que conecta 48 departamentos gubernamentales en más de ochocientos kilómetros de fibra [21]. En su punto de mira está convertir la red, en un futuro próximo, en un servicio comercial (en el mismo sentido que Reino Unido), permitiendo la entrada de compañías privadas en modalidad *Quantum as a Service*, es decir, arrendando el servicio. Asimismo, y sin decomisionar la actual red cuántica (basada en canales cuánticos emisor-receptor), 2025 debiera ser el año en el

5 Fundada en 2001 como *spin-off* de la Universidad de Ginebra, es considerada la primera compañía en comercializar productos QKD (desde 2007) y colaboró, junto con la mencionada universidad, en los primeros despliegues, pruebas de concepto y redes QKD experimentales europeas, en la primera década del siglo XXI.

que se añadan los primeros cien kilómetros de red operados con protocolos basados en entrelazamiento.

– India, dispone de redes metropolitanas, como la de Delhi, de aproximadamente doscientos kilómetros. Durante los últimos años ha tomado un enfoque más agresivo y militarista en su despliegue de QKD, canalizando la mayoría de los proyectos a través de la iniciativa *Innovations for Defence Excellence* (iDEX) [22].

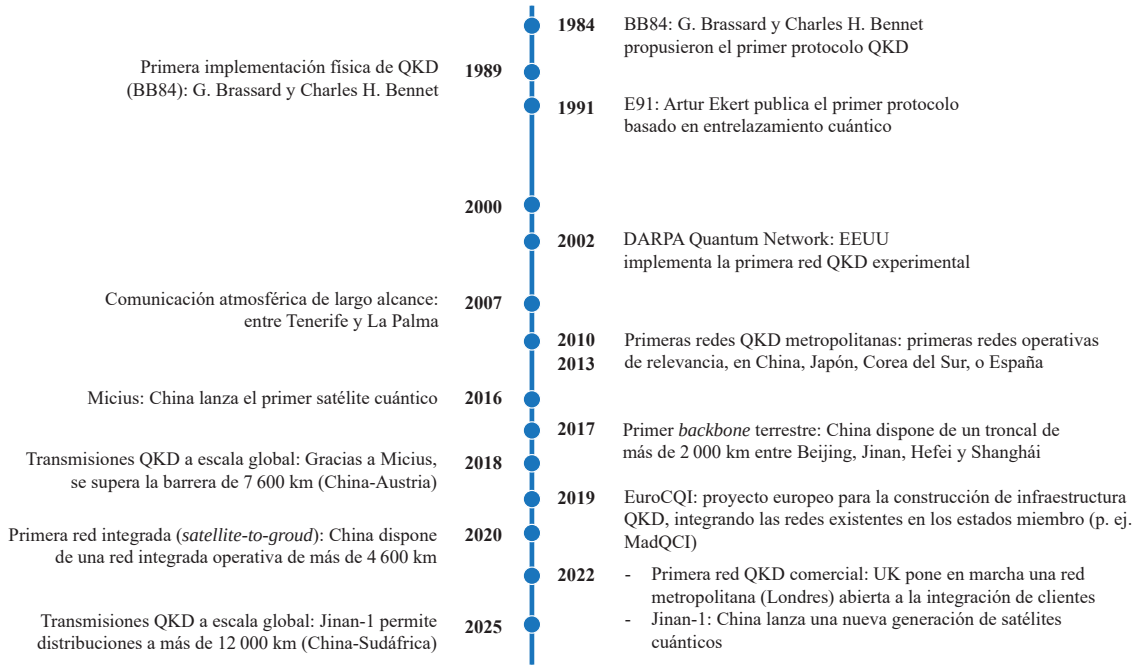

Figura 3. Hitos más relevantes en al artículo. Fuente: elaboración propia

4.4 QKD, dos aproximaciones llamativamente opuestas

Ante esta situación, como ya hemos mencionado, la posición del Gobierno estadounidense se resume en la postura oficial de la NSA [5]:

> «In summary, NSA views quantum-resistant (or post-quantum) cryptography as a more cost effective and easily maintained solution than quantum key distribution. For all of these reasons, NSA does not support the usage of QKD or QC to protect communications […]».

Esto contrasta fuertemente con lo que está ocurriendo sobre el terreno en el ámbito académico. Si bien el nivel de despliegue de infraestructura QKD en Estados Unidos es modesto (comparativamente hablando), y lo mismo podríamos decir del volumen de publicaciones y patentes, aquellos avances que transcienden a los medios sí son científicamente notorios y evidencian que no han quedado rezagados a nivel de investigación. Por ejemplo, en mayo de 2024, una iniciativa conjunta de la Universidad de Harvard y Amazon consiguió transmitir fotones entrelazados en redes de 35 kilómetros [23] (en el mismo sentido que pretende realizar Corea del Sur en 2025). Queda por resolver la cuestión de si es real el aparente desalineamiento entre la posición del Gobierno estadounidense y la de sus sectores académico y privado, que quizá no están interesados en

el QKD presente (lo que explicaría el volumen de patentes y publicaciones), pero sí en sus posibilidades futuras.

Se podría argumentar, sin embargo, que Estados Unidos juega bajo otra perspectiva, siendo firme defensor de la postura favorable de la OTAN respecto a QKD [24]. Por ello, consideramos que la mejor forma de describir la posición estadounidense es la de «cauto escepticismo».

Salvando las anteriores matizaciones, esta divergencia en el análisis sobre el futuro de QKD ha despertado la curiosidad de muchos analistas. ¿Por qué China invierte esas cantidades de dinero en el despliegue de infraestructura QKD, mientras Estados Unidos, al menos en sus declaraciones públicas, considera la tecnología como un callejón sin salida? No son pocos los que apuntan que Estados Unidos, en este caso, ha sido demasiado taxativo en su postura, y una aproximación similar a la coreana hubiera sido más prudente. Han apostado mucho a que QKD no tendrá aplicación práctica futura, ni siquiera un lugar relevante en una futura infraestructura de comunicaciones poscuántica.

En determinados ámbitos, como el de las comunicaciones militares, la disponibilidad (recordemos el problema del DoS en QKD) es tan relevante como la confidencialidad. Quizá por ello las inversiones en disrupción de comunicaciones militares no dejan de aumentar en la esfera estadounidense. Confían, plenamente, en que el problema de denegación es insuperable.

5 El futuro de QKD

El desarrollo de QKD ya está transformando las dinámicas geopolíticas, marcando una nueva era en la competencia por la soberanía nacional y la seguridad de las comunicaciones críticas. Si QKD se consolida como estándar, las potencias que logren dominar esta tecnología no solo asegurarán sus propias comunicaciones, sino que también tendrán la capacidad de influir en la infraestructura de comunicaciones globales, redefiniendo las alianzas y el equilibrio de poder en el siglo XXI.

El futuro de QKD está, además, intrínsecamente ligado a las posibilidades de desarrollo de un «internet cuántico», una red que utilice las propiedades de la mecánica cuántica para transmitir información de forma no solo segura (aspecto en el que QKD sería clave), sino eficiente y comparativamente superior al internet clásico en ordenes de magnitud difícilmente anticipables. Esto abre la puerta a nuevas formas de computación distribuida y ultra veloz, y tendría un reflejo evidente en aquellos procesos en los que el uso intensivo de capacidad de cómputo es fundamental: el ejemplo que a todos se nos viene a la cabeza es el de la inteligencia artificial.

Que el escenario anteriormente descrito se materialice dependerá de múltiples factores, que podrían resumirse en la capacidad de la comunidad científica para superar los desafíos que actualmente presenta el campo.

Por un lado, lo que hemos dado a llamar problemas de ingeniería. En dicho sentido resultará fundamental la integración de la infraestructura QKD con la infraestructura

tradicional, que garantizará que la comunicación cuántica se convierta en algo más que en una comunicación punto a punto en un conjunto de *backbones* relevantes, dejando el resto de la red vulnerable. Día a día, los investigadores empujan el límite de atenuación, incrementando las distancias en las que una comunicación QKD es posible. Otro foco de avance es el desarrollo de protocolos más eficientes, como los MDI-QKD, que elimina la necesidad de tantos elementos de medición confiables.

Por otro, los problemas que solo podrán ser mitigados, como el de denegación de servicio. De cuán bien se mitigue dependerá, en buena parte, el éxito en la implementación práctica de QKD.

El ritmo de avance científico (medido, por ejemplo, en número de patentes o publicaciones), la calidad de dicho avance, la evolución en la inversión de los distintos Estados, o el compromiso en el despliegue de costosa infraestructura por parte de la práctica totalidad de actores relevantes deja al descubierto cuál es el pensamiento de sus decisores al respecto: QKD será una pieza importante en la era de la computación poscuántica, y para algunos actores, la pieza fundamental.

6 Conclusión

Existe, de forma generalizada, un sentido de urgencia en los Gobiernos para impulsar las iniciativas cuánticas, en la seguridad de que la supremacía de estas otorgará una ventaja diferencial en el campo de la computación, la sensorización y las comunicaciones. Y esto es tanto como decir una ventaja estratégica esencial.

Lo que hace particularmente interesante la comunicación cuántica es el hecho de no encontrar consenso al respecto. Frente a otros campos de investigación como la inteligencia artificial o la propia computación cuántica, donde no hay grandes diferencias de opinión respecto a la necesidad de dominarlos y la dinámica de carrera está plenamente establecida, en el caso de, por ejemplo, QKD, nos encontramos con dos posturas diferenciadas entre los dos actores globales más significativos, China y Estados Unidos.

Inevitablemente, y en función de cómo se resuelvan los próximos años/décadas, estas apuestas no cubiertas marcarán un futuro diferente para ambos jugadores y, en consecuencia, merece especial atención y seguimiento.

Independientemente de la calidad de los centros de investigación, en el caso de una tecnología como QKD, que requiere del despliegue de infraestructura masiva y de alto coste, no existe el concepto de *fast-follower*. Si, finalmente, QKD resulta una pieza fundamental en el panorama poscuántico, Estados Unidos se encontrará en una posición de desventaja clara y con un largo recorrido en inversiones y tiempo, que realizar si quiere colocarse a la altura. Renunciar al presente de QKD es renunciar, tácitamente, a su futuro.

En este escenario futuro, el desequilibrio en su adopción generará previsiblemente consecuencias éticas y geopolíticas. China, con años de monopolio por delante, controlará una parte significativa del flujo global de información segura, mientras que el resto de actores se encontrarán en un estado vulnerable frente a interceptaciones.

Más allá de esta primera interpretación, este desfase podría redefinir el mapa global de otras maneras más sutiles. China estará en disposición de exportar infraestructura cuántica a otros países, y lo que es más relevante, de ofrecer a sus aliados estratégicos acceso a su red cuántica como incentivo, desplazando la tradicional supremacía tecnológica occidental y permitiéndoles manipular, *de facto*, cualquier información que sus aliados puedan procesar. Países del Sur Global, en busca de soberanía digital, podrían verse fuertemente atraídos por esta posibilidad, siempre y cuando sea ofrecida por el coste adecuado. Desde el punto de vista ético, el monopolio de la comunicación cuántica podría dar pie a una nueva forma de colonialismo tecnológico, donde China podría extender su modelo autoritario más allá de sus fronteras, controlando y manipulando la información conforme a sus intereses.

Todos estos factores tendrían la potencialidad de consolidar su influencia geopolítica fundada en la tecnología, su *sharp power*, y esta influencia resultar clave para imponer estándares de funcionamiento e interoperabilidad que cimenten, a su vez, más años de liderazgo en comunicaciones cuánticas. Este círculo virtuoso es algo que en occidente hemos experimentado con la computación clásica, y sumamente difícil de desestabilizar. Un cambio de paradigma como la comunicación cuántica ofrece esa posibilidad, y es vital acertar en la estrategia.

Referencias

Alferov, S. V., Bugai, K. E. y Pargachev, I. A. (2022). Study of the Vulnerability of Neutral Optical Filters Used in Quantum Key Distribution Systems against Laser Damage Attack. *JETP Letters*. 116, pp. 123-127. [Consulta: 2025]. Disponible en: https://doi.org/10.1134/S0021364022601117

Bennett, C. y Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*. 560, pp. 175-179. [Consulta: 2025]. Disponible en: https://doi.org/10.48550/arXiv.2003.06557

Brassard, G. (2005). Brief history of quantum cryptography: a personal perspective. *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*. Awaji, pp. 19-23. DOI: 10.1109/ITWTPI.2005.1543949.

Chen, Y. A., Zhang, Q., Chen, T. Y. *et al.* (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*. 589, pp. 214-219.

Comisión Europea. (s. f.). Iniciativa sobre la Infraestructura Europea de Comunicación Cuántica (EuroQCI). [Consulta: 2025]. Disponible en: https://digital-strategy.ec.europa.eu/es/policies/european-quantum-communication-infrastructure-euroqci

EQIC. (2024). A Portrait of the Global Patent Landscape in Quantum Technologies. European Quantum Industry Consortium. [Consulta: 3 enero 2025]. Disponible en: https://www.euroquic.org/wp-content/uploads/2024/03/QuIC-White-Paper-IPT-January-2024.pdf

Express Defence. (2024). Indian Army signs quantum key distribution contract under iDEX. *Financial Express*. [Consulta: 2025]. Disponible en: https://www.financialexpress.com/business/defence-indian-army-signs-quantum-key-distribution-contract-under-idex-3627043/

HSBC. (2023). HSBC becomes first bank to join the UK's pioneering commercial quantum secure metro network. *HSBC*. [Consulta: 2025]. Disponible en: https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-becomes-first-bank-to-join-the-uks-pioneering-commercial-quantum-secure-metro-network

Hugues-Salas, E. *et al.* (2018). Experimental Demonstration of DDoS Mitigation over a Quantum Key Distribution (QKD) Network Using Software Defined Networking (SDN). *Optical Fiber Communications Conference and Exposition (OFC)*. San Diego, pp. 1-3.

IDQ. (2022). IDQ and SK Broadband complete phase one of nation-wide Korean QKD Network. *IDQ*. [Consulta: 2025]. Disponible en: https://www.idquantique.com/idq-and-sk-broadband-complete-phase-one-of-nation-wide-korean-qkd-network/

Jones, A. (2024). China to launch new quantum communications satellites in 2025. *SpaceNews*. [Consulta: 3 enero 2025]. Disponible en: https://spacenews.com/china-to-launch-new-quantum-communications-satellites-in-2025/

Lord, A., Woodward, R., Murai, S., Sato, H., Dynes, J., Wright, P., White, C., Davey, R., Wilkinson, M., Clinton-Tarestad, P., Hawkins, I., Farrington, K. y Shields, A. (2023). London Quantum-Secured Metro Network. *Optical Fiber Communication Conference (OFC)*. Optica Publishing Group, paper W4K.4.

McKinsey & Company. (2023). Quantum technology patent share from 2000 to 2022, by segment and country [Graph]. *Statista*. [Consulta: 3 enero 2025]. Disponible en: https://www.academia.edu/3064-979X/2/1/10.20935/AcadQuant7590

National Security Agency. (2025). Post-Quantum Cybersecurity Resources, Quantum key distribution and quantum key cryptography. National Security Agency. [Consulta: 2025]. Disponible en: https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

NATO. (s. f.). Quantum Technologies and the Science for Peace and Security Programme. NATO. [Consulta: 2025]. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/11/pdf/231130-SPS-Quantum-1487-23.pdf

NIST. (s. f.). Post-Quantum Cryptography, Computer Security Resource Center. NIST. [Consulta: 2025]. Disponible en: https://www.nist.gov/pqcrypto

Omaar, H. y Makaryan, M. (2024). How Innovative Is China in Quantum? *ITIF*. [Consulta: 5 enero 2025]. Disponible en: https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/

Qi, C. (2024). China's Quantum Ambitions: A Multi-Decade Focus on Quantum Communications. *Yale Journal of International Affairs*. [Consulta: 3 enero 2025]. Disponible en: https://www.yalejournal.org/publications/chinas-quantum-ambitions

Sabani, M., Savvas, I., Poulakis, D. y Makris, G. (2023). Quantum Key Distribution: Basic Protocols and Threats. *Proceedings of the 26th Pan-Hellenic Conference on Informatics (PCI '22)*. Nueva York, Association for Computing Machinery, pp. 383-388. [Consulta: 2025]. Disponible en: https://doi.org/10.1145/3575879.3576022

Sasaki, M. *et al.* (2011). Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express*. 19(11), pp. 10387-10409.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Santa Fe, pp. 124-134. DOI:10.1109/sfcs.1994.365700.

Xi, G. (2008). Interview with Chen Zengbing of the University of Science and Technology of China: Interpretation of Quantum Communication That 'Will Not Be Stolen. *Beijing Science and Technology Daily*.

Zapatero, V., Leent, Tim van, Arnon-Friedman, R. *et al.* (2023). Advances in device-independent quantum key distribution. *npj Quantum Information*. 9, p. 10. [Consulta: 2025]. Disponible en: https://doi.org/10.1038/s41534-023-00684-x

Zhang, M. (2024). Harvard Researchers and Amazon Collaborate to Launch Boston's First Quantum Network. *The Harvard Crimson*. [Consulta: 2025]. Disponible en: https://www.thecrimson.com/article/2024/5/28/quantum-network-boston -cambridge/

Artículo recibido: 8 de enero de 2025
Artículo aceptado: 4 de junio de 2025