La SEI
School of Economic Intelligence
Escuela de Inteligencia Económica
Universidad Autónoma de Madrid

2019

Vol. 1, 3, pp. 19 - 28
ISSN: 2659-9805
Editor in-Chief: Javier Oubiña

JOURNAL OF ECONOMIC & BUSINESS INTELLIGENCE

Universidad Autónoma de Madrid UAM

HACIA LA AUTONOMÍA ESTRATÉGICA CUÁNTICA EN LA UNIÓN EUROPEA

Andrea G. Rodríguez*

Resumen

La creciente informatización y digitalización de la sociedad han hecho del ciberespacio un entorno estratégico. La aplicación de los principios de la mecánica cuántica al campo de la informática no sólo logrará resolver problemas que la capacidad computacional actual no permite, sino que incrementará los riesgos en ciberseguridad. Por este motivo, las inversiones en tecnologías cuánticas se han intensificado en los últimos años con el objetivo de liderar la carrera cuántica, desarrollar un ordenador cuántico plenamente operativo y proteger infraestructura crítica de ciberataques cuánticos. La Unión Europea se ha sumado a este contexto con la iniciativa Buque Insignia Cuántico, que promete poner a Europa en la vanguardia de la investigación cuántica. La carrera cuántica es una oportunidad para que Europa logre mayores niveles de autonomía estratégica con respecto a sus competidores. El presente artículo tiene el objetivo de dar una visión general de la cuestión desde el punto de vista competitivo exponiendo y comparando las principales iniciativas de China, de Estados Unidos y de la UE

Palabras clave: ciberseguridad, computación cuántica, Unión Europea, estrategia, geotecnología.

Abstract

The increasing informatisation and digitalisation of society made cyberspace a new strategic domain. The application of the principles of quantum mechanics to the field of computer science will not only solve problems that current computational capacity cannot solve, but also increases cyber risks. For this reason, investment in quantum technologies has intensified during the last years with the aim of leading the quantum race, developing a fully-functional quantum computer and protecting critical infrastructure from quantum cyberattacks. The European Union has joined in this context with the Quantum Flagship initiative, that promises to put Europe at the forefront of quantum research. The quantum race is an opportunity for Europe to reach greater levels of strategic autonomy vis-à-vis her competitors. The present paper is intended to provide a general overview of the issue from the competition perspective by presenting and comparing the main quantum initiatives in the China, the United States and the European Union.

Key words: cybersecurity, quantum computing, European Union, strategy, geotechnology.

* International Master in Security, Intelligence and Strategic Studies programme (IMSISS). University of Glasgow, Dublin City University and Univerzita Karlova (Prague). Contacto: a.agarcod@gmail.com

1. Introducción

Thomas Kuhn escribía en 1971 que "la ciencia, cuando afecta al desarrollo socioeconómico, lo hace a través de la tecnología" (pág. 283). En el ámbito militar, el desarrollo tecnológico ha sido clave para garantizar el éxito de las campañas. En 1895 el ejército japonés derrotaba al ejército chino en Asia Oriental. A pesar de ser inferior numéricamente, el Imperio Japonés había dedicado las últimas décadas al desarrollo industrial y tecnológico. La restauración Meiji fue el inicio del expansionismo japonés en Asia-Pacífico (Hane, 2003). Durante la Primera Guerra Mundial, la irrupción de la aviación y la potencia aumentada de las armas de fuego fue posible gracias a las Revoluciones Industriales que habían transformado Europa y el mundo. Desde el fin de la Segunda Guerra Mundial— y en especial las últimas décadas del siglo XX—, la proliferación nuclear, marcada por los efectos del nacimiento del campo de la física cuántica, ha creado un nuevo significado de disuasión (*deterrence)* y el ritmo de la política internacional.

La expansión de las tecnologías de la información y de la comunicación y su penetración en todos los estratos de la sociedad han hecho del ciberespacio— y por extensión del espacio exterior— dos nuevos campos estratégicos, sumándose a tierra, mar y aire. La preocupación por las comunicaciones ha conseguido desarrollar maneras cada vez más seguras de transferir información, entre ellas el desarrollo de criptosistemas, conjunto de secuencias para garantizar la seguridad de la información con el objetivo de asegurar la confidencialidad, integridad y autenticidad de los datos trasmitidos (O'Connor, Dukatz, DiValentin, & Farhady, 2018). El desarrollo tecnológico ha continuado por el camino de la digitalización y la computación. Los avances en física cuántica, y sobre todo en mecánica, y sus posibles aplicaciones en todo tipo de tecnologías constituyen desde principios de los 2000 lo que se ha bautizado como "segunda revolución cuántica" (Jaeger, 2018), un salto cualitativo y *capacitativo* en potencia e innovación basado en las aplicaciones de principios como el de superposición o el entrelazamiento, que— en el campo de la informática— afectarán a la ciberseguridad, a la capacidad de simulación, desarrollo de la inteligencia artificial, metrología y más. Además de las implicaciones en materia de seguridad, los avances cuánticos generan nuevas oportunidades para la economía nacional. Por ello, como escribió Cédric Villani en un informe para la Asamblea Nacional francesa (2019): "los gobiernos siguen estos desarrollos e invierten masivamente en el mercado a fin de afianzar su influencia en la escena internacional" (pág. 3).

Debido a sus consecuencias constructivas pero también destructivas, la inversión en tecnologías cuánticas ha entrado en el ámbito estratégico. En 2016. el lanzamiento de un satélite cuántico por parte de la República Popular China colocó a Pekín a la cabeza y abrió la puerta al establecimiento de comunicaciones cuánticas— seguras e indescifrables— a media y larga distancia vía satélite. El hito es parte del programa QUESS, establecido dentro del plan quinquenal 2015-2020 y se encuentra dentro de la visión Made in China 2025. Estados Unidos no se unió de manera pública a la carrera cuántica hasta 2018 con la publicación del Acta de Iniciativa Nacional Cuántica (*National Quantum Initiative Act*), aunque gigantes tecnológicos como Google, IBM o Microsoft ya desarrollaran proyectos de este tipo (Google, s.f; IBM, s.f.; Microsoft, s.f.). A pesar de la falta de un documento estratégico, instituciones públicas como el Instituto Nacional de Estándares y Tecnología (NIST) trabajan desde 2016 en el desarrollo de algoritmos post-cuánticos para asegurar los sistemas digitales (NIST, 2016). En la Unión Europea, esfuerzos nacionales pioneros como el de Portugal, Países Bajos o Reino Unido se complementan con el programa Buque Insignia Cuántico (*Quantum Flagship*) (European Commission, 2019), con el objetivo de crear una red de internet cuántico entre las principales ciudades de la Unión.

El presente artículo tiene el objetivo de dar una visión general de la cuestión desde el punto de vista competitivo. Para ello, dado que el objeto de referencia es la Unión Europea, se tomarán las iniciativas de Estados Unidos y la República Popular China como las otras dos unidades de análisis. Cabe destacar que, por motivos de simplificación del estudio, otros actores relevantes en la materia como Japón o Canadá han sido dejados fuera deliberadamente. La primera parte tratará de dar una introducción a las aplicaciones de la segunda revolución cuántica en el campo de la informática. Seguirá con una aclaración del término "autonomía estratégica" frente a "soberanía" y continuará con una descripción de las principales iniciativas cuánticas en China, Estados Unidos y la Unión Europea. Por último, concluirá que, aunque la UE no lidera en ninguna subsección medida por la Comisión Europea, el objetivo de establecer una red de Internet cuántico es ambicioso, pero puede lograrse. Además, la UE tiene la ventaja, frente a Estados Unidos y China, de poder promover redes más estrechas de cooperación que ayudan al intercambio de conocimiento y al avance tecnológico. Sin embargo, avisa, que no debe de perder de vista la dimensión de seguridad, de preparase para el salto cuántico y tratar de generar propuestas para mitigar sus consecuencias.

2. La computación cuántica frente a la computación tradicional

La física cuántica, a diferencia de la física tradicional, se ocupa de las unidades más pequeñas de la materia. Unidades *cuantificables*. En el mundo de la computación, son los principios de superposición, entrelazamiento y decoherencia de la mecánica cuántica los que sientan las bases de este salto. La información se almacena en forma de *bits*, clasificados en ceros y unos; la base del lenguaje binario de programación. Un *bit cuántico* o *qubit* es, de manera aproximada, tanto cero como uno a la vez (principio de superposición) y es *único*: no puede copiarse. Debido a la imposibilidad de copiar un qubit, se elimina la posibilidad de copiar la información para hacer un reenvío—un segundo intento—. Además, mantener la superposición cuántica necesita de procesadores con un avanzado sistema de refrigeración, cercano al 0 absoluto (-273ºC). Al ser 0 y 1, el qubit es por naturaleza más complejo y más seguro debido a que existe un mayor número de combinaciones. Un mayor número de combinaciones hace posible una mayor capacidad de computación y de simulación.

Un ejemplo de la aplicación práctica de la capacidad de potencia aumentada puede encontrarse en el dilema del laberinto. En el laberinto, el sujeto no tiene información previa sobre el camino y cuenta con altas dosis de incertidumbre (si toma una decisión incorrecta, se puede perder). Además, se trata de algo sumamente complejo que ciega los sentidos (es difícil retroceder sobre tus pasos para salir del laberinto) convirtiéndose, por lo tanto, en una metáfora del ingenio y del misterio. La humanidad ha desarrollado respuestas para resolver el dilema propuesto cada vez de manera más eficiente. Teseo llevó un ovillo de lana que le indicaba el camino para salir, girar siempre hacia el mismo lado nos garantiza encontrar la salida tarde o temprano, las sustancias quimio-atrayentes de un copo de avena puesto en el objetivo consigue que el plasmodio del *physarum polycephalum* encuentre a la primera el camino hacia el mismo (Adamatzky, 2012)… Todas ellas nos llevan al centro del laberinto o nos sacan de él, pero eficientes— en términos científicos de aprovechamiento de los recursos— no son. La simulación con tecnología cuántica ofrece la posibilidad de recorrer todos los caminos posibles a la vez para poder seleccionar *a posteriori* el mejor de todos ellos gracias a la naturaleza del bit cuántico. Ello se traduce en una mejora sustancial con respecto a la capacidad de computación tradicional y abre las puertas a la solución de problemas que un ordenador tradicional no puede o tardaría años en resolver (Caruso, Crespi, Ciriolo, Sciarrino, & Osellame, 2016).

Dos qubits pueden estar sincronizados o entrelazados (principio de entrelazamiento), de tal manera que se resuelvan del mismo modo aclarando— o "descifrando"— el contenido del mensaje. Este principio ofrece nuevas oportunidades en el campo de la ciberseguridad. Los dilemas criptográficos derivados de la literatura computacional tradicional que toma como ejemplo el axis Alice—Bob (*e.g.* Bernstein & Lange, 2017; Hayes, 2012; Boyer, Kenigsber & Mor, 2007), como la posibilidad de un tercer agente tratando de interceptar la comunicación cifrada se resuelven: cualquier disrupción en la línea de comunicación es más fácil de detectar (Mosca, 2018). Es por ello por lo que la comunicación cuántica es el método más seguro hasta el momento debido a la sensibilidad del sistema, reduciendo de manera drástica las posibilidades de espionaje (*eavesdropping*) y de un ataque *Man-in-the-Middle*.

Al igual que las comunicaciones cuánticas son más seguras, un ordenador cuántico vulnerabilizaría las actuales. Bernstein y Lange (2017), prueban que los algoritmos cuánticos de Shor y Grove son capaces de romper la mayoría de las claves utilizadas hoy en día en las comunicaciones —RSA, "Rivest, Shamir y Adleman" y ECC, "*Elliptic Curve Cryptography*" — y ofrecen cuatro sistemas derivados de ellos. La criptografía post-cuántica, un campo aún en su infancia, trata de resolver la pregunta de cómo codificar las comunicaciones cuando el actor que quiere penetrar en el sistema tiene un ordenador cuántico.

El ciclo de ciber resiliencia utilizado en empresas e instituciones consta, en términos generales, de los siguientes pasos: identificación, protección, detección, respuesta y recuperación (IBM, s.f. & Symantec, 2014). En él, dependiendo del tipo de *malware*, el actor que entre en nuestro sistema hará una cosa u otra. Descubierto el virus, éste es eliminado y el sistema parcheado y actualizado para evitar un nuevo ataque. Un ciberataque cuántico no solamente sería capaz de entrar en el sistema, sino de romper la criptografía haciendo más difícil la recuperación: la reescritura de un nuevo sistema criptográfico normalmente lleva años (Mosca, 2016).

Para el año 2026, cerca de un 14% de los instrumentos criptográficos actuales serán fáciles de romper. Este número será aún mayor—50%—para 2050 según el ritmo de innovación tecnológica actual (Mosca, 2016). La *datalización* de la actividad humana y la convergencia digital son tendencias constantes e imparables. El uso de la tecnología comprende el núcleo del comportamiento antropológico. Las telecomunicaciones se encuentran en el centro del funcionamiento gubernamental, personal y económico y forman parte, de hecho, de la infraestructura nacional crítica. El 5G,

el desarrollo del Internet de las Cosas y las ciudades inteligentes unirán a más personas con personas, cosas con cosas, y personas con cosas a través de señales de radio esencialmente (Khan, Abdullah, Khan, Julahi, & Tarmizi, 2017). Teniendo en cuenta que la posibilidad del desarrollo de un ordenador cuántico está aún lejos de nuestra realidad actual, cabe pensar estratégicamente a medio y largo plazo sin perder de vista la realidad que viene.

3. El concepto de "autonomía estratégica"

Académicos de las escuelas realistas y neo-realistas de las Relaciones Internacionales posicionan a los Estados como el objeto de referencia en el devenir político mundial, caracterizados por un comportamiento racional que los lleva a optimizar su posición mediante el intento de realización/fomento de sus intereses (*e.g.* Mearsheimer, 1990 & Waltz, 1979). De esta manera, los Estados son el núcleo de la seguridad internacional pues sólo ellos pueden crear políticas relacionadas con ello, debido a que ostentan el monopolio de la violencia legítima (Weber, 1919). De esta manera, ante las amenazas exteriores, los Estados se comportan de tres maneras siguiendo las teorías señaladas (Waltz, 1979): o buscan restaurar el equilibrio de poder, o buscan con oportunismo "subirse al carro" de la amenaza (*bandwagoning*), o buscan a un tercero para que proteja sus intereses mientras tratan de minimizar los daños manteniéndose, estratégicamente, al margen (*buck-passing*).

El concepto de autonomía estratégica se apoya sobre la definición de qué significa tener autonomía y cómo llegar a ella. En el contexto de la disciplina de seguridad, busca crear unas condiciones de ventaja mediante el fomento de parámetros de autosuficiencia en materias sensibles para el Estado. Una visión *estratégica* supone la necesidad de, por una parte, ver el desarrollo tecnológico y la autonomía digital como un valor a proteger (Baldwin, 1997), y por otra, de una vez llegado a este consenso, el compromiso de realizar esfuerzos dirigidos a este fin. Un valor *estratégico* en este ámbito es la suma importancia y prioridad de las telecomunicaciones como servicio y sus componentes como bien.

En el ámbito tecnológico, desde la Segunda Guerra Mundial, la concentración de innovación puntera digital se ha mantenido ajena al suelo europeo. Durante la Guerra Fría, una Europa descompuesta buscaba reponerse de los horrores de la guerra— material y psicológicamente— mientras el desarrollo tecnológico ocurría a su oriente y occidente, ejemplificada en la paradigmática carrera espacial. Asimismo, el colapso del bloque comunista en 1991 y las transformaciones que llevaban una década dándose en China dejaban de nuevo a Europa fuera de juego. El viejo continente, simplemente, vivía de las patentes que se originaban en gran medida en las universidades estadounidenses, aún a pesar de tener una alta densidad de graduados universitarios (OECD, 2018, pág. 50). Los grandes proyectos se elaboraban fuera, donde los mejores cerebros eran bienvenidos con financiación más generosa.

Autonomía digital y soberanía digital no son lo mismo. En términos de Jean Bodin, el concepto de soberanía tiene una dimensión absoluta y otra de perpetuidad (Abellán, 2014). La soberanía se centra en la cuestión de Estado, en la legitimidad, en el control y autoridad sobre un territorio (Timmers, 2019) y es por ello un concepto inherentemente limitado. El devenir de las relaciones internacionales se ha apartado de la concepción westfaliana del mundo y es habitual la cooperación interestatal y la fijación de estos de normas que limitan, en parte, su soberanía en ciertos asuntos.

El concepto de autonomía presupone la complejidad de las redes de relaciones del mundo digital y de las diferentes capas que se superponen a ella y busca, en todo momento proteger valores. En otras palabras, el concepto de autonomía digital busca incrementar la noción objetiva y psicológica de la seguridad por medio de la utilización de medios comprobados, registrados y examinados por autoridades competentes que trabajan con un mismo fin. La autonomía estratégica es considerada en ocasiones como el medio por el cual los Estados llegan a ser soberanos en una materia (Timmers, 2019) y, por ello, está estrechamente ligado con las doctrinas de seguridad y defensa. Con la excepción de la India, ningún estado ha hecho de la autonomía estratégica un fin en sí mismo.

La aparición del concepto de "autonomía estratégica" en la Unión Europea no es novedoso. En el intrincado menester de trabajar por una mayor integración en materia de seguridad y defensa, la UE avanza con el objetivo de conseguir un nivel "apropiado de ambición y autonomía estratégica" (EEAS, 2016). También en 2017, tras discrepancias con los Estados Unidos en materia de financiación de la OTAN, la canciller alemana Angela Merkel recalcó que "los europeos debemos tomar el destino en nuestras manos" (Carbajosa, 2017). A pesar de que ámbitos como la ciberseguridad se han incorporado recientemente a los documentos, la men-

ción de otras tecnologías sigue siendo marginal. La autonomía estratégica en el plano digital, también en materia de tecnologías cuánticas, busca, por lo tanto, 1) ampliar y defender las capacidades y competencias generales en el ámbito digital; 2) fomentar la investigación autóctona y la industria tecnológica europea; 3) reducir la dependencia exterior en materia tecnológica; 4) generar pautas de decisión comunes para la arquitectura cuántica europea de acuerdo a unos puntos consensuados en materia de ciberseguridad y privacidad; 5) proteger los valores de la Unión.

4. La estrategia cuántica de la República Popular China

La estrategia cuántica China se enmarca en el 13º Plan Quinquenal, inaugurado en 2016 con validez hasta 2021. En él, el objetivo principal es la transición desde el crecimiento por capital acumulado al crecimiento por innovación, es decir, de ser un país que manufactura y ensambla los componentes del mundo al ser el país que los diseña (Alietta & Bai, 2016). Además del plano económico, el giro tecnológico de la República Popular China se sustenta en una visión de seguridad. Así, en 2016, Xi Jinping declaraba que el hecho de que la tecnología estuviera controlada por otros era un peligro escondido (Lewis, 2019, pág. 25) para la seguridad nacional china.

El Plan dotaba de financiación extra y encaje estratégico a los planes tecnológicos dibujados en la estrategia "Made in China 2025", desvelada un año antes, 2015, mediante la cual China busca la equiparación tecnológica con los gigantes tecnológicos occidentales. De hecho, fue en 2016 cuando por primera vez se unió al club de los 25 países más innovadores según la Organización Mundial de la Propiedad Intelectual (Jung, 2016). Esta estrategia se encuentra superpuesta al plan de desarrollo para ciencia y tecnología que el país tenía presente desde el año 2006 (Gobierno de China, 2006) con el objetivo de ampliar el impacto de la innovación en la economía y de generar la infraestructura necesaria para dar el paso Made in China 2025.

En el plano de la tecnología cuántica, China lanzó al espacio el primer satélite cuántico en 2016, *Micius*, como parte del programa QUESS, capaz de mantener comunicaciones encriptadas con la superficie terrestre, desmontando la barrera de la distancia para las comunicaciones cuánticas—limitada de manera segura a día de hoy a un centenar de kilómetros (Wehner, 2018)— y abriendo paso a futuras comunicaciones intercontinentales (Ju, Liu, & Hu, 2018). *Micius* fue capaz de comunicar a China con Austria. Además, con la ayuda de BeiDou, el Ejército Chino está trabajando para desarrollar una brújula cuántica que dotaría de independencia de los sistemas de geolocalización espaciales a los sistemas de navegación militares (Kania, 2018), lo cual en la práctica reduciría las posibilidades de aislamiento, interrupción e intercepción de las comunicaciones así como de la geolocalización de un vehículo por el enemigo en un escenario de conflicto. Una brújula cuántica es una realidad que Reino Unido ya ha desarrollado (Murgia, 2018).

La pronta apuesta por las tecnologías cuánticas y su formulación estratégica en planes a corto, medio y largo plazo, dan a China una ventaja sobre sus competidores. Además, acostumbrada a actuar paralelamente en el ámbito de las TICs, el lanzamiento de *Micius* ha avanzado en las posibilidades de desarrollar un Internet cuántico con características chinas.

5. La estrategia cuántica de Estados Unidos

Estados Unidos basa su investigación en iniciativas privadas que tienen lugar en sus *hubs* tecnológicos y sólo se ha incorporado de manera estratégica y pública a la carrera cuántica a partir de 2018. La investigación estadounidense se basa en el desarrollo de componentes y de criptografía post-cuántica. El primer supuesto se concentra en la región de Silicon Valley, en universidades y empresas privadas. De entre éstas últimas destacan Microsoft— con su primera publicación en 1993— con un total de 259 publicaciones hasta julio de 2019 (Microsoft, s.f.), IBM, con su ordenador comercial de 20-qubits (IBM, 2019) y Google con un procesador de 72-qubits (Google AI, 2018). En el segundo, ligado al Departamento de Comercio estadounidense, sobresale NIST.

NIST es uno de los laboratorios de física más antiguos de EE. UU. Se fundó en 1901 con la misión de mejorar la competitividad del país respecto a los gigantes industriales de la época como Alemania o Reino Unido. El Instituto ha dado cuatro premios Nobel de física y uno de química, el último en 2012— Dave Wineland— por su investigación en la "medida y manipulación de sistemas cuánticos individuales" (NIST, s.f.). De entre los 88 proyectos activos del Instituto, destaca aquél para estandarizar uno o más algoritmos criptográficos resistentes a los avances en tecnología cuántica. La primera ronda del concurso finalizó a finales de

2017. Desde entonces hay 26 algoritmos que siguen en revisión (NIST, 2019).

La Visión Estratégica Nacional Cuántica (2018) añade la visión de seguridad y defensa. Tiene como objetivo mejorar la comunicación entre actores privados y públicos, fomentar la investigación en ciencia y tecnología cuánticas y establecier programas especiales en universidades. En el ámbito de la seguridad nacional y la competición exterior, Estados Unidos, de manera poco precisa, establece la meta de crear mecanismos de comunicación interdepartamentales para calcular y analizar los riesgos y oportunidades en materia de economía, seguridad y defensa.

Asimismo, establece parámetros de cooperación internacional, aunque solamente con "industrias y gobiernos afines" (in. *like-minded*) (US Subcommittee on Quantum Information Science, 2018, pág. 12). La estrategia está complementada con el Acta de Iniciativa Nacional Cuántica cuyo propósito explícito es "asegurar el liderazgo continuado de los Estados Unidos en la ciencia de la información cuántica y sus aplicaciones tecnológicas" (US Congress, 2018, pág. 2).

En definitiva, de todas las aplicaciones posibles de las tecnologías cuánticas, Estados Unidos se centra en el ámbito de la computación invirtiendo con menos intensidad en otros aspectos igualmente importantes para el avance tecnológico. Esto es debido a una clara mentalidad de seguridad y defensa (US Congress, 2018), para asegurar las comunicaciones, y en consecuencia se centra en la carrera para desarrollar el primer ordenador cuántico. A nivel público, sobre todo en criptología post-cuántica. A nivel privado, en el desarrollo de *hardware* y *software*. A pesar de ello, su tardía incorporación a nivel público a la carrera cuántica hace que China se encuentre por delante en ámbitos muy relevantes y prioritarios para EE. UU. como en distribución de clave cuántica (QKD), o, según la tendencia actual, pronto en investigación relativa al principio de entrelazamiento (Travagnin, 2019); clave para el desarrollo de sistemas de navegación autónomos, o sincronización.

6. La estrategia cuántica de la Unión Europea

A las escasas iniciativas nacionales europeas (Portugal, Reino Unido, Países Bajos) se ha sumado dentro del continente la estrategia Buque Insignia Cuántica (*Quantum Flagship*, BIC de aquí en adelante). La estrategia tiene como base el Manifiesto publicado en mayo de 2016 por el cual la UE decidía implicarse en el desarrollo de estas tecnologías con el objetivo de "liderar la segunda revolución cuántica" (European Union, 2016, pág. 7).

El Manifiesto establecía un periodo de 20 años (2015-2035) como el tiempo en el que la humanidad tardaría en construir el primer ordenador cuántico funcional. Para ello, dividía la estrategia en prioridades cronológicas como pasos para llegar a construir ese ordenador: dominio en la comunicación cuántica, después en simulación, sensores y por último ordenadores. Comunicación y simulación en el periodo 2015-2020, simulación y sensores en el periodo 2020-2025 y sensores y ordenadores en el periodo restante con el añadido de crear una red de internet cuántica que conectara las grandes ciudades europeas (European Union, 2016).

El BIC fue inaugurado en octubre de 2018 y tiene una financiación de 1.000 millones de euros a lo largo de los 10 años de la estrategia, parte de los cuales vienen de la iniciativa europea Horizonte 2020, con un presupuesto de cerca de 80.000 millones de euros para el periodo 2014-2020 (European Commission, s.f.). Complementario a los fondos de Horizonte 2020, BIC también bebe de la iniciativa QuantERA, la cual se financia tanto por la Unión Europea como por agencias nacionales (Quantera, s.f.). Las inversiones están divididas en las siguientes categorías o subprogramas: simulación, metrología y sensores, computación, comunicación y ciencia.

El objetivo a largo plazo de la iniciativa cuántica europea, dibujada ya en el Manifiesto, es la creación de un Internet cuántico dentro de la Unión. Paradójicamente, salvo *Micius*, las comunicaciones terrestres son, de momento, posibles a corta distancia (Wehner, 2018), por lo que crear una red multidireccional cuántica de larga distancia es aún una tarea imposible.

A pesar de ello, la empresa neerlandesa QuTech llevará a cabo en 2020 el primer experimento de internet cuántico en Países Bajos, Estado geográficamente ideal debido a que tiene núcleos medianos de población relativamente uniformes separados por pocos kilómetros (TUDelft, 2018). El objetivo es tener una red de internet cuántico entre las ciudades de Ámsterdam, Leiden, La Haya y Delft para el año 2022 (QuTech, 2019, pág. 15) y desde Países Bajos extenderlo al resto de Europa.

7. Conclusiones

En número de patentes relacionadas con las tecnologías cuánticas, la Unión Europea no lidera en ninguna de las categorías que establece la Comisión Europea: computación, distribución de clave cuántica (información cuántica, incluyendo criptografía), entrelazamiento e interferometría atómica fría (Travagnin, 2019). China y Estados Unidos lideran estos sectores con un ratio de 2-2, a pesar de que el impulso de la investigación pública en China hace que las previsiones de crecimiento del país asiático sean mayores que las estadounidenses, pudiendo traspasar pronto su capacidad de investigación e innovación en el plano de las tecnologías cuánticas sobre todo tras el lanzamiento de Huawei a la carrera (HUAWEI, 2018).

A pesar de la ambiciosa estrategia del Buque Insignia Cuántico de la Unión Europea, en comparación con las iniciativas chinas y estadounidenses—a nivel privado— sigue por detrás. La iniciativa de una primera red cuántica europea en funcionamiento desde 2022 desde Países Bajos sería un hito prodigioso, pero aún así no sería único. Iniciativas similares ya están en prueba en Japón y China, en este último con una red de cerca de 2.000 km. de largo, entre Pekín y Shanghái (QuTech, 2019, pág. 19). Estados Unidos, a pesar de haberse incorporado con una estrategia pública en 2018, el último de entre estos casos-sujetos, sigue liderando los desarrollos en el campo de la computación cuántica a través de sus empresas tecnológicas, pero no termina de hacerlo en otros subsectores.

No obstante, hay un punto en la estrategia nacional cuántica estadounidense que es a la vez una gran ventaja para la Unión Europea. La cooperación con entidades "afines" (US Subcommittee on Quantum Information Science, 2018) es un hecho dentro de la UE, donde el nivel de confianza en las instituciones europeas es lo suficientemente alto como para sacar adelante iniciativas comunes tales como BIC que unan a los sectores públicos y privados en el triángulo empresas-gobiernos-Unión Europea. La concepción neorrealista de la competición tecnológica por parte de EE. UU. tal y como se extrae de los documentos públicos disponibles contrasta con la visión de la UE, favoreciendo, en el caso del segundo actor, el reparto de proyectos y subvenciones y facilitando el intercambio de conocimiento.

De esta manera, se abre un nuevo escenario de oportunidades para el desarrollo de la tecnología europea con el objetivo de rebajar la dependencia exterior, en especial de China y Estados Unidos. Con una concepción más integradora y de bloque, la UE se distancia de la competición realista de EE. UU. aunque ello puede hacer que pierda de vista la dimensión estratégica de la cuestión al centrarse en la dimensión de mercado. Mediante el BIC, la Unión amplía sus capacidades digitales y fomenta la industria e investigación europea, pero no le dedica suficientes esfuerzos a las labores defensivas y de mitigación de riesgos como lo hace Estados Unidos.

A pesar de que un entorno de autonomía estratégica digital total es difícil de concebir, la motivación por el desarrollo de soluciones cuánticas está en plena efervescencia. Los riesgos para la seguridad nacional las han colocado alto en la pirámide de prioridades de los Estados. Sus oportunidades de mercado hacen que nos encontremos, otra vez, en una carrera por el desarrollo y el control de nuevas tecnologías. Ahora, como antes con la primera revolución cuántica, tampoco tenemos claras las consecuencias.

8. Referencias

Aaronson, S. (2018). What Quantum Computing Isn't. *TEDx Dresden*. Dresden, Alemania. Retrieved from https://www.youtube.com/watch?v=JvIbrDR1G_c

Abellán, J. (2014). *Estado y soberanía.* Madrid: Alianza Editorial.

Adamatzky, A. (2012, febrero). Slime Mold Solves Maze in One Pass, Assisted by Gradient of Chemo-Attractants. *IEEE Transactions on Nanobioscience, 11*(2).

Alietta, M., & Bai, G. (2016, septiembre). China's 13th Five-Year Plan. In Pursuit of a "Moderately Prosperous Society". *CEPII*(12).

Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies, 23*, 5-26.

Ball, J. (2018). Quantum computing is the future...eventually. *TEDxOIST*. Retrieved from https://www.youtube.com/watch?v=7hg5eaGpjDg

Bernstein, D. J., & Lange, T. (2017, Septiembre 14). Post-quantum cryptography. *Nature, 549*, 188-194.

Bouwmeester, D., & Zeilinger, A. (2000). The Physics of Quantum Information: Basic Concepts. In D.

Bouwmeester, A. Ekert, & A. Zeilinger (Eds.), *The Physics of Quantum Information*. Berlin: Springer.

Boyer, M., Kenigsber, D., & Mor, T. (2007). Quantum Key Distribution with Classical Bob. *First International*.

Carbajosa, A. (2017, mayo 29). Merkel: "Los europeos tenemos que tomar el destino en nuestras manos". *El País*. Retrieved from https://elpais.com/internacional/2017/05/28/actualidad/1495991847_111089.html

Caruso, F., Crespi, A., Ciriolo, A. G., Sciarrino, F., & Osellame, R. (2016). Fast escape of a quantum walker from an integrated photonic maze. *Nature Communications*.

EEAS. (2016). *Shared Vision, Common Action: A Stronger Europe: A Global Strategy for the European Union's Foreign and Security Policy*. Retrieved from http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

European Commission. (2019). *Quantum Flagship: A Major Boost for European Quantum Research*. Retrieved from Digital Single Market: https://ec.europa.eu/digital-single-market/en/news/quantum-flagship-major-boost-european-quantum-research

European Commission. (n.d.). *What is Horizon 2020?* Retrieved from Horizon 2020: https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020

European Union. (2016, mayo). *Quantum Manifesto: A New Era of Technology*. Retrieved from https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf

Gobierno de China. (2006, febrero 09). *China to strengthen basic research*. Retrieved from Gov.cn: http://www.gov.cn/english/2006-02/09/content_183726.htm

Google AI. (2018, marzo 5). *A Preview of Bristlecone, Google's New Quantum Processor*. Retrieved from Google AI Blog: https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html

Google. (n.d.). *Quantum*. Retrieved from Google AI: https://ai.google/research/teams/applied-science/quantum-ai/

Hane, M. (2003). *Breve historia de Japón*. Madrid: Alianza Editorial.

Hayes, B. (2012, septiembre-octubre). Alice and Bob in Cipherspace. *American Scientist, 100*, 362-367.

House, J. (2018). *Fundamentals of Quantum Mechanics* (3 ed.). Londres: Academic Press.

Howorth, J. (2019). Differentiation in security and defence policy. *Comparative European Politics, 17*, 261-277.

HUAWEI. (2018, octubre 12). *Huawei Unveils Quantum Computing Simulation HiQ Cloud Service Platform*. Retrieved from Press & Events: https://www.huawei.com/en/press-events/news/2018/10/huawei-hiq-cloud-service-platform

IBM. (2019, enero 8). *IBM Unveils World's First Integrated Quantum Computing System for Commercial Use*. Retrieved from IBM News Room: https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use

IBM. (n.d.). *Cyber resilience lifecycle*. Retrieved from IBM: https://www.ibm.com/services/business-continuity/cyber-resilience

IBM. (n.d.). *IBM Q*. Retrieved from IBM: https://www.research.ibm.com/ibm-q/

Jaeger, L. (2018). *The Second Quantum Revolution: from Entanglement to Quantum Computing and Other Super-Technologies*. Cham: Springer.

Ju, S., Liu, Y., & Hu, T. (2018). QUESS Operations at Chinese Space Science Mission Centre. *2018 SpaceOps Conference*. doi:10.2514/6.2018-2329

Jung, J. (2016, diciembre 15). *China's Innovation-Driven Development Strategy and Prospects*. Retrieved from Korea Institute for International Economic Policy: file:///C:/Users/AndreaRodriguez/Downloads/KIEP%20opinions_no98%20(1).pdf

Kania, E. B. (2018, September 26). China's Quantum Future. *Foreign Affairs*.

Khan, A., Abdullah, J., Khan, N., Julahi, A., & Tarmizi, S. (2017, Mayo). Quantum-Elliptic curve Cryptography for Multihop Communication in 5G Networks. *International Journal of Computer Science and Network Security, 17*(5).

Kuhn, T. S. (1971, primavera). The Relations between History and History of Science. *Daedalus, 100*(2), 271-304.

Lewis, J. A. (2019). *Learning the Superior Techniques of the Barbarians: China's Pursuit of Semiconductor Independence*. CSIS Technology Program. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190115_Lewis_Semiconductor_v6.pdf

Mearsheimer, J. (1990). Back to the Future: Instability in Europe after the Cold War. *International Security, 15*(1), 5-56.

Miakisz, K., Piotrowski, E. W., & Sladkowski, J. (2006). Quantization of games: Towards quantum artificial intelligence. *Theoretical Computer Science, 358*, 15-22.

Microsoft. (n.d.). *Quantum Computing.* Retrieved from Research: https://www.microsoft.com/en-us/research/research-area/quantum/

Mosca, M. (2016). *A Quantum of Prevention for our Cybersecurity*. Retrieved from Global Risk Institute: https://globalriskinstitute.org/research/cyber-security-fraud/

Mosca, M. (2018, Septiembre/Octubre). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy, 16*(5).

Murgia, M. (2018, noviembre 9). UK scientists build world's first quantum compass. *Financial Times*. Retrieved from https://www.ft.com/content/e90f902a-e441-11e8-a6e5-792428919cee

Nijssen, S. R., Schaap, G., & Verheijen, G. P. (2018). Has your smartphone replaced your brain? Construction and validation of the Extended Mind Questionnaire (XMQ). *Plos One, 13*(8).

NIST. (2016). *Post-Quantum Cryptography*. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

NIST. (2019). *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process.* Gaithersburg: National Institute of Standards and Technology.

NIST. (n.d.). *Dave Wineland.* Retrieved from NIST and the Nobel: https://www.nist.gov/content/nist-and-nobel/dave-wineland

O'Connor, L., Dukatz, C., DiValentin, L., & Farhady, N. (2018). *Cryptography in a Post-Quantum World: Preparing intelligent enterprises now for a secure future.* Accenture.

OECD. (2018). *Education at a Glance.* Paris: OECD Publishing. Retrieved from https://www.oecd-ilibrary.org/docserver/eag-2018-en.pdf?expires=1563372620&id=id&accname=guest&checksum=095151395C9CA58852036540AA470295

Orange, E., Weiner, J., The Future Hunters, & Ranasinghe, E. (2019, March 12). *The Quantum Race.* Retrieved from Medium: https://medium.com/positive-returns/the-quantum-race-5e30f76ff59

Quantera. (n.d.). *QuantERA ERA-NET Cofund in Quantum Technologies*. Retrieved from About: https://www.quantera.eu/about

QuTech. (2019). *Quantum Internet.* Delft, Netherlands: Technological University of Delft. Retrieved from https://issuu.com/tudelft-mediasolutions/docs/quantum_magazine_june_2019

Rosenberg, S. (2017, Septiembre 27). *Firewalls Don't Stop Hackers. AI Might.* Retrieved from WIRED: http://www.wired.com/story/firewalls-dont-stop-hackers-ai-might/

Schmidt, M. S., Bradsher, K., & Hauser, C. (2012, octubre 8). U.S. Panel Cites Risks in Chinese Equipment. *The New York Times.*

Symantec. (2014). *The Cyber Resilience Blueprint: A New Perspective on Security.* Mountain View CA.

The White House. (2019, Mayo 15). *Executive Order on Securitng the Information and Communications Technology and Services Supply Chain.* Retrieved from https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

Timmers, P. (2019, mayo 10). *Strategic Autonomy and Cybersecurity*. Retrieved from EU Cyber Direct: https://eucyberdirect.eu/content_research/strategic-autonomy-and-cybersecurity/

Travagnin, M. (2019). *Patent Analysis of Selected Quantum Technologies.* Luxembourg: Publications Office of the European Union. Retrieved from http://publications.jrc.ec.europa.eu/repository/bitstream/JRC115251/patent_analysis_of_selected_quantum_technologies_1.pdf

TUDelft. (2018, junio 13). *Delft scientists make first 'on demand' entanglement link*. Retrieved from Delft University of Technology: https://www.tudelft.nl/en/2018/tu-delft/delft-scientists-make-first-on-demand-entanglement-link/

US Congress. (2018, enero 3). National Quantum Initiative Act. Washington DC, District of Columbia, United States of America. Retrieved from https://www.congress.gov/115/bills/hr6227/BILLS-115hr6227enr.pdf

US Subcommittee on Quantum Information Science. (2018). *National Strategic Overview for Quantum Information Science.* National Science & Technology Council, Committee on Science. Retrieved from

https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf

Villani, C. (2019). *Les technologies quantiques: introduction et enjeux*. Asemblée Nationale, Office Parlementaire D'Évaluation des Choix Scientifiques et Technologiques. Paris: Assemblée Nationale. Retrieved from http://www2.assemblee-nationale.fr/content/download/79022/810034/version/2/file/Note_TechnologiesQuantiques_Introduction_versionFinale.pdf

Waltz, K. (1979). *Theory of International Politics*. Addison-Wesley: Reading.

Weber, M. (1919). La política como vocación. *Conferencia de la Asociación Libres de Estudiantes de Munich*.

Wehner, S. (2018). The Quantum Internet. *TEDx Vienna*. Viena, Austria. Retrieved from https://www.youtube.com/watch?v=XzPi29O6DAc

.