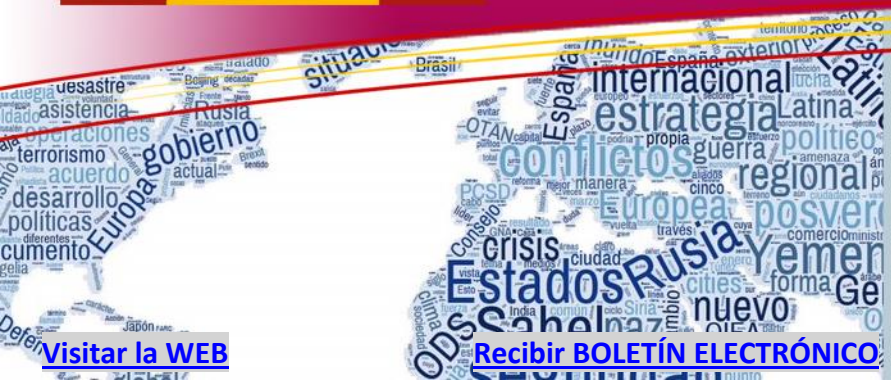
Documento
Opinión

34/2024 4 de abril de 2024

Elisa M. Darias, Sonia Ramos, Beatriz Gómez, F. Javier Marcos, Enrique Belda, Dionís Oña *

Las tecnologías cuánticas en la cuarta revolución industrial



Las tecnologías cuánticas en la cuarta revolución industrial

Resumen:

La cuarta revolución industrial engloba la transformación tecnológica producida desde los años ochenta del siglo XX, que afecta a la producción industrial y a múltiples aspectos de la vida cotidiana. Se caracteriza principalmente por iniciar un proceso de transición hacia nuevos sistemas sustentados en la digitalización.

La revolución digital se basa en muy diversas tecnologías que derivan en multitud de aplicaciones, aquí se enmarcan las tecnologías cuánticas que son un conjunto heterogéneo de equipos y técnicas aplicables a muy distintos usos, de entre los cuales podemos destacar algunos que afectan a cuestiones de seguridad y defensa. Por ello, resulta un objetivo estratégico fundamental promover el desarrollo de la investigación cuántica, impulsando para ello la colaboración con la industria, la Universidad y los centros de investigación especializados, así como el acuerdo con instituciones internacionales. Las iniciativas que está desarrollando España muestran la apuesta nacional por impulsar su presencia en este ámbito y por potenciar la soberanía europea en la computación cuántica mediante la cooperación internacional.

Palabras clave:

Cuarta revolución industrial, tecnologías cuánticas, cúbits, criptografía, EDT.

Cómo citar este documento:

Varios Autores. *Las tecnologías cuánticas en la cuarta revolución industrial*. Documento de Opinión IEEE 34/2024.
https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO34_2024_VVAA_Tecnologias.pdf y/o enlace bie[3] (consultado día/mes/año)

*__NOTA:__ Las ideas contenidas en los ***Documentos de Opinión*** son responsabilidad de sus autores, sin que reflejen necesariamente el pensamiento del IEEE o del Ministerio de Defensa.

Cualquier revolución, de la índole que sea, conlleva ventajas y desventajas, retos y oportunidades, incertidumbres y certezas. A lo largo de la historia del ser humano se han venido produciendo cambios en la forma de pensar, vivir y relacionarse, es lo que comúnmente se conoce como revolución industrial.

Este trabajo tiene por objeto mostrar una visión generalista de lo que hoy se conoce como la cuarta revolución industrial para, posteriormente, hacer una descripción más detallada de las tecnológicas disruptivas emergentes asociadas a ella, poniendo el foco en las tecnologías cuánticas y lo que estas suponen para la Seguridad y Defensa de Europa y España.

Revoluciones industriales: revisión histórica

Las revoluciones industriales son procesos de transformación económica, tecnológica y social que, en un intervalo de tiempo relativamente breve, producen un verdadero cambio de paradigma a nivel mundial, lo que hace que sea necesario revisar constantemente las reglas de convivencia para adecuarlas a los cambios. Para propiciar una revolución de esta magnitud deben confluir múltiples factores y la innovación tecnológica es uno de los más determinantes y que mejor caracterizan cada una de las sucesivas revoluciones experimentadas por la humanidad.

Se considera que actualmente estamos inmersos en la cuarta revolución industrial. Para ponerla en contexto conviene hacer un breve repaso por las anteriores.

La primera revolución industrial comenzó a mediados del siglo XVIII en Gran Bretaña y se extendió hasta la primera mitad del siglo XIX. El hito tecnológico que la propició fue la máquina de vapor, patentada por James Watt en 1769, junto con la construcción del ferrocarril y el uso del carbón como principal fuente de energía. Los cambios económicos y sociales supusieron una gran transformación de la humanidad en menos de un siglo. Así, la economía mundial rural, basada hasta entonces en un predominio casi absoluto de la agricultura y la ganadería, la artesanía y el comercio, evoluciona a una economía industrial, mecanizada y de carácter urbano. En el ámbito político, es el momento del Estado de Derecho, el reconocimiento de la soberanía popular y de los derechos individuales (vida, libertad, seguridad, propiedad privada y resistencia frente al autoritarismo).

La segunda revolución industrial se inició en 1870 y se extendió hasta el estallido de la I Guerra Mundial. Vino impulsado por nuevas fuentes de energía: petróleo, gas electricidad, y porque se hizo posible la producción en masa, fomentada por la cadena de montaje. Esta revolución trajo aparejada una globalización en la que las comunicaciones jugaron un papel crucial: por un lado, las redes de comunicaciones físicas con el perfeccionamiento de la navegación marítima y del ferrocarril, la invención del motor de combustión interna y la aparición de nuevos medios como el avión o el automóvil y, por otro lado, las telecomunicaciones, con la invención de la radio y del teléfono. Es el momento en que se desarrollan los partidos políticos de masas, los movimientos sindicales y se reconocen los derechos de participación política, que incluyen el sufragio censitario y universal (femenino a partir del siglo XX).

Tras las dos grandes guerras mundiales, comenzó la tercera revolución industrial, o revolución digital. La caracteriza el desarrollo de la electrónica digital, los ordenadores, la informática y las telecomunicaciones, así como la invención del transistor en 1947 y el desarrollo exponencial de los semiconductores. Las primeras computadoras y redes de ordenadores, como ARPANET[1] fueron precursoras del gran desarrollo del hardware, software y redes de telecomunicaciones actuales. En el ámbito político, comienza a desarrollarse el Estado del Bienestar con el reconocimiento de los derechos sociales o prestacionales y derechos colectivos en el trabajo (negociación colectiva y huelga) y la creación de la ONU.

Por último, el término cuarta revolución industrial engloba la transformación tecnológica producida desde los años ochenta del siglo XX, que afecta a la producción industrial y a múltiples aspectos de la vida cotidiana. No se caracteriza sólo por el descubrimiento de un conjunto de tecnologías emergentes, sino por iniciar un proceso de transición hacia nuevos sistemas sustentados en la digitalización. Es el paso a una era de tecnologías conectadas y conocimientos basados en el análisis de datos.

En el ámbito político se reconocen los derechos relacionados con las tecnologías de la información y comunicaciones, y comienza el desarrollo de nuevas formas de gestión pública en las que la ciudadanía pasa a ser copartícipe del poder político. Aparecen nuevos actores, como las compañías tecnológicas, que desde su posición de control de

[1] Academia de las ciencias y las artes militares. Primer enlace de ARPANET. - 21 DE NOVIEMBRE DE 1969Primer enlace de ARPANET - Acami.

la información a la que se accede, o el desarrollo de nuevas herramientas como los teléfonos móviles inteligentes o la inteligencia artificial, pueden contribuir a desdibujar aún más las reglas clásicas del desarrollo de políticas (derechos, libertades, democracia, etc.). Y también amenazar derechos tanto colectivos (empresas, patentes, ventas, compras, etc.) como personales especialmente protegidos por la LOPD (Ley Orgánica de Protección de Datos)[2], que son susceptibles de ser conseguidos por medios que se han considerado ilícitos y puestos a la venta de forma ilícita en el mercado.

Hay grandes diferencias entre esta revolución industrial y las tres anteriores:

- El desarrollo del cambio productivo se apoya en un ecosistema de PYMES altamente innovadoras, startups y no en grandes entidades que aglutinen todo el conocimiento.
- No se basa en una única innovación disruptiva como la máquina de vapor.
- Tiene un carácter transversal, que afecta a sectores más allá de la industria (sanidad, financiero, logístico, etc.), y también colaborativo, porque necesita la cooperación de los distintos elementos del ecosistema para generar productos y servicios capaces de transformar los procesos. Lo que la hace más sensible a accesos y comercio ilícito de los datos que se generan.
- Las nuevas tecnologías, denominadas tecnologías disruptivas, han cambiado la tradicional forma de trabajar, comprar o relacionarse de las personas.

Tecnologías de la revolución digital en la cuarta revolución industrial. tecnologías cuánticas

Como hemos visto, la revolución digital se basa en muy diversas tecnologías que derivan en multitud de aplicaciones que forman un ecosistema que está cambiando la forma de vivir y trabajar de las personas y cuyo uso debe ser regulado y especialmente incentivado. Estas tecnologías interactúan entre sí y los productos actuales suelen incorporar varias de ellas.

[2] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Dentro de esta familia están las tecnologías cuánticas, estas se basan su funcionamiento en la física cuántica, cuyos inicios se remontan a la primera mitad del siglo XX, con los trabajos de científicos como Planck, Schrödinger o Heisenberg.

Algunas tecnologías, como los relojes atómicos (1949) o los láseres (1960) tienen una base cuántica, pero fue el físico teórico estadounidense Richard Feynman[3] el primero en relacionar la física cuántica con la teoría de la información, abriendo el camino a la computación y a las comunicaciones cuánticas. Estas tecnologías están llamadas a jugar un papel disruptivo en los próximos años por su impacto en muchas áreas y, especialmente, en la capacidad de cálculo masivo y en las comunicaciones seguras, campos en los que se prevé que marcarán una nueva época, lo que obligará a hacer una revisión de los sistemas de seguridad.

Actualmente, son cuatro las principales tecnologías existentes en este ámbito:

- Los sensores cuánticos se basan en la gran respuesta a los cambios físicos que experimentan los sistemas cuánticos, haciéndolos idóneos para medir variables físicas como el tiempo, la gravedad, el campo magnético, etc.
- La simulación cuántica con aplicaciones muy prometedoras en el desarrollo de nuevos materiales, nuevos medicamentos o en las previsiones del comportamiento de la naturaleza. Los simuladores cuánticos se componen de los mismos elementos que la realidad a simular, por lo que su simulación es mucho más natural que la de los ordenadores clásicos.
- Las comunicaciones cuánticas ofrecen mayor seguridad por la propia naturaleza cuántica y el efecto de no clonación: cuando se intenta extraer información de un sistema cuántico, este se perturba, por lo que es posible detectar un ataque o interferencia en las comunicaciones.
- La computación cuántica es la tecnología que se espera que suponga una mayor revolución, por lo que conviene detenerse en ella.

Tras la exposición de Feynman de los primeros principios de la teoría de la computación cuántica en 1981 durante una conferencia organizada por IBM y el Instituto de Tecnología de Massachusetts (MIT), en los años 90 del siglo XX se comienzan a diseñar

[3] Feynman, R.P., “Simulating Physics with Computers”, International Journal of Theoretical Physics, vol. 21, pp. 467-488, 1982

los primeros algoritmos cuánticos, como el de Shor[4], sobre la factorización de números primos, crucial en criptografía. También se empiezan a definir las primeras aplicaciones de la computación cuántica y a realizar los primeros experimentos que implican cúbits, los bits cuánticos.

En la década del 2000 se desarrollan los primeros ordenadores cuánticos capaces de ejecutar algoritmos como el de Shor. Progresivamente, se desarrollan diferentes ordenadores de 8 y 12 cúbits y las primeras memorias cuánticas. Posteriormente, la primera computadora cuántica comercial la produciría la empresa D-Wave Systems en 2011. IBM se suma a la carrera en 2016 con un ordenador cuántico de 17 cúbits y alcanza los 20 cúbits en 2019 con su IBM Q SystemOne. En la década actual, se habla de cientos o incluso de miles de cúbits.

La capacidad de procesamiento de los ordenadores cuánticos crece de manera exponencial con el número de cúbits. La computación cuántica está hoy en día en sus inicios, y ni siquiera ha llegado a desarrollarse un modelo físico de ordenador cuántico cuyas ventajas lo hagan prevalecer sobre los demás. Conviven hoy en día ordenadores cuánticos y propuestas para futuros prototipos de diferente naturaleza: adiabáticos, orientados a puertas y topológicos, con grandes empresas detrás de estos desarrollos (D-Wave Systems, IBM, Microsoft, Google, etc.).

Computación cuántica para seguridad y defensa

La noticia de octubre del 2019 en la que Google afirmaba haber conseguido la supremacía cuántica, supuso un origen de preocupación para los expertos y responsables de ciberseguridad y ciberdefensa acerca de las posibles implicaciones de seguridad que podía conllevar este desarrollo. Teóricamente, un ordenador cuántico dispone de capacidades de resolución de problemas matemáticos tan superiores a la de un ordenador convencional que podría dejar fuera de juego algunos de los sistemas de criptografía en los que hoy basamos la protección de la información y las comunicaciones digitales.

[4] Shor, Peter W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput., 26(5), 1997, 1484–1509.

Pese a ser aún una tecnología poco madura que además requiere de una gran inversión para su desarrollo, la computación cuántica tiene el potencial de transformar la tecnología y las capacidades en el ámbito de la defensa. Estados Unidos, China, Europa, Japón, Canadá, Corea del Sur o Rusia están invirtiendo muchos recursos en los ordenadores cuánticos. En España, se están haciendo grandes avances gracias a grupos de investigación integrados en instituciones como el CSIC y en empresas como IBM, Google o Intel.

Sin embargo, también plantea desafíos, como la necesidad de desarrollar medidas contra posibles amenazas cuánticas. Cabe citar aquí la Recomendación sobre ámbitos tecnológicos críticos para la seguridad económica de la UE[5], realizada el pasado 3 de octubre de 2023 y que deriva de la Comunicación conjunta sobre una Estrategia Europea de Seguridad Económica[6]. En ella se recomienda llevar a cabo evaluaciones de riesgos en cuatro ámbitos tecnológicos críticos, incluyendo entre ellos el cuántico. Por lo tanto, es fundamental que las instituciones de Defensa y Seguridad Nacional estén al tanto de los avances en esta tecnología y trabajen en su integración de manera estratégica para mantener la ventaja en un entorno geopolítico en constante evolución. Pudiera ser demasiado tarde si se espera hasta que la tecnología esté disponible para realizar cambios en las políticas y normas de ciberseguridad.

En este punto, conviene recordar la definición de ciberamenazas incluida en la Estrategia Nacional de Ciberseguridad 2019[7], según la cual, “son todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos”, añadiendo que se caracterizan por su diversidad, en cuanto a capacidades y motivaciones, por no distinguir fronteras y porque afectan a la práctica totalidad de los ámbitos de la Seguridad Nacional, como son la Defensa Nacional, la seguridad económica o la protección de las infraestructuras críticas.

Las tecnologías cuánticas son, por tanto, un conjunto heterogéneo de equipos y técnicas aplicables a muy distintos usos, de entre los cuales podemos destacar algunos que afectan a cuestiones de seguridad y defensa.

[5] Commission Recommendation of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States. 3 de Octubre 2023.

[6] Comunicación conjunta al parlamento europeo, al consejo europeo y al consejo. Bruselas, 20.6.2023 eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52023JC0020

[7] Orden PCI/487/2019, de 26 de abril, Estrategia Nacional de Ciberseguridad 2019 | DSN

Los sistemas de criptografía actuales están amenazados por la computación cuántica, especialmente por la capacidad del algoritmo de Shor para romper los sistemas de cifrado actuales, como el ampliamente utilizado RSA[8].

Se está trabajando en sistemas y algoritmos de criptografía que, basados en la computación convencional, sean capaces de resistir ataques cuánticos, es decir, que sean robustos ante ataques basados en algoritmos cuánticos actuales como el de Shor o el de Grover. Esta criptografía llamada "post-quantum", puede ofrecer soluciones temporales relativamente fáciles de implementar, pero sigue teniendo la debilidad de utilizar computación convencional, por lo que se mantiene el riesgo de que se desarrolle en algún momento un nuevo algoritmo cuántico eficiente contra su sistema de encriptado.

Además de las amenazas relacionadas con la criptografía, los avances en sensórica (que permitirán, por ejemplo, que los sensores puedan detectar amenazas de forma más precisa y difícilmente perceptible o disponer de sistemas de navegación con menor riesgo de interferencia que el GPS), optimización (realizar operaciones de forma más rápida que los ordenadores actuales, con aplicaciones por ejemplo en logística) o simulación (para comprender el funcionamiento de sistemas complejos mediante el análisis de sistemas cuánticos modelo y que podrían permitir el desarrollo de nuevos materiales y fármacos, por ejemplo, frente a la guerra química) pueden ser aplicables al sector de la defensa. Un ejemplo de ello es la actividad de la empresa aeroespacial, de armamento y sistemas de defensa Lockheed Martin, que adquirió un ordenador cuántico D-Wave y cuenta con el centro de investigación USC-Lockheed Martin Quantum Computing Center (QCC) en colaboración con la Universidad del Sur de California.

Precisamente por sus implicaciones en seguridad y defensa, las tecnologías cuánticas se consideran estratégicas por los Estados. Los diferentes países llevan tiempo realizando grandes esfuerzos de inversión en I+D+i para su evolución. Aunque es complejo determinar el alcance de esta inversión, según el informe de McKingsey & Company de finales de 2021[9] sobre computación cuántica, el esfuerzo de financiación público a nivel mundial alcanza los 30.000 millones de dólares, con China y la Unión Europea a la cabeza. Sin embargo, este informe contempla solo la financiación pública,

[8] En criptografía, RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1979, que utiliza factorización de números enteros. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente).

[9] McKinsey: Lo último en tendencias tecnológicas: perspectivas para el 2023. | LinkedIn

por lo que a estas cifras habría que sumar el esfuerzo del sector privado, la industria que, en países como Estados Unidos, es muy relevante.

Hay un hilo conductor común a los ámbitos de seguridad y de defensa. Lo podemos ver claro con un ejemplo: una persona hostil armada con una pistola supone un problema de seguridad civil. Diez mil personas hostiles armadas, sin embargo, son un problema de defensa. La escala es, por lo tanto, uno de los factores que determinan el alcance de una amenaza y el ámbito de actuación de la respuesta requerida. Actualmente, la computación cuántica opera principalmente a escala de grandes corporaciones, gobiernos y bloques geopolíticos. Por lo tanto, la seguridad cuántica se plantea en esos mismos términos. A medida que estas tecnologías evolucionen y sean accesibles a un mayor espectro de la sociedad, es previsible que otro tipo de organizaciones e incluso individuos puedan hacer uso de ella con fines delictivos. Por ello es también primordial ir adecuando la legislación punitiva y ampliar la clasificación de delitos relacionados con estas tecnologías para establecer unos mecanismos de defensa a todos los niveles ante cualquier acción o actuación que se pueda considerar ilícita.

Actividades e iniciativas cuánticas de los ministerios del interior y defensa. Anillo cuántico y enlace con Europa

La Unión Europea, tras el Manifiesto Cuántico publicado en 2016 (x), ha lanzado la iniciativa de investigación e innovación a largo plazo, Quantum Technologies Flagship, cuyo objetivo es poner a Europa a la vanguardia de la llamada segunda revolución cuántica mediante el apoyo a la investigación en un plazo 10 años (2018-2028), con un presupuesto previsto de 1.000 millones de euros. Si bien su objetivo no está centrado en la defensa, sí es una acción europea destinada a afianzar una cierta soberanía tecnológica, que supone financiación adicional vinculada a las tecnologías cuánticas para el desarrollo y el refuerzo de las capacidades digitales estratégicas de Europa.

En España, como proyecto complementario con la iniciativa anterior, el Ministerio de Asuntos Económicos y Transformación Digital ha impulsado desde 2021 la creación del primer ecosistema de computación cuántica del sur de Europa con el Proyecto Quantum Spain. El Consejo de Ministros del pasado 28 de octubre de 2021 aprobó para este proyecto una subvención de 22 millones de euros.

Entrando en materia de seguridad y defensa, una tecnología tan crítica que requiere de tiempo, de un gran esfuerzo en inversión e investigación y que además debe permitir la interoperabilidad entre sistemas distintos, tendrá más probabilidades de éxito si su desarrollo en el ámbito de la defensa se acomete con la máxima colaboración no solo con el sector privado, sino también entre los países que componen el bloque occidental. Además, debe compaginar la investigación del desarrollo de su potencial con el análisis de los mecanismos de defensa ante su posible uso por los adversarios.

Por eso, la OTAN aprobó en 2021 la estrategia "Promover y Proteger: Estrategia Común OTAN sobre Tecnologías Emergentes y Disruptivas (EDT)". La estrategia tiene dos dimensiones: por una parte, la promoción del desarrollo de las EDT y de las tecnologías de uso dual para multiplicar y aprovechar plenamente su potencial y, por otra, la necesidad de crear un foro de debate sobre protección contra amenazas relacionadas con el uso que pueden hacer de ellas competidores y adversarios. Entre las siete áreas clave de la Estrategia se encuentran las tecnologías cuánticas. Asimismo, la Agenda 2030 de la OTAN establece como uno de sus cinco pilares la Preservación de la vanguardia tecnológica, que contiene iniciativas como un Acelerador OTAN de empresas de nueva creación (start-ups) de innovación (DIANA)[10] y un Fondo OTAN de innovación.

En Europa destaca la creación del Fondo Europeo de Defensa para complementar los esfuerzos de colaboración de los Estados miembro para desarrollar capacidades tecnológicas e industriales en defensa. Además, la Agencia Europea de Defensa, en 2022, lanzó un Hub de Innovación en Defensa de la UE (HEDI).

Asimismo, el Ministerio de Defensa publicó en 2021 la actualización de la Estrategia de Tecnología e Innovación en Defensa que, dentro del pilar de Objetivos Tecnológicos, incluye el Seguimiento de tecnologías emergentes con potencial aplicación futura a defensa, donde se ubica la tarea de vigilancia tecnológica en torno a un conjunto de EDT que incluye, entre otras muchas cuestiones, la computación cuántica; la comunicación e información cuántica; y los sensores y metrología cuántica, incluyendo el campo de la fotónica o la simulación cuántica.

[10] Aceleradora de Innovación en Defensa del Atlántico Norte (DIANA). https://www.tecnologiaeinnovacion.defensa.gob.es/es -es/Contenido/Paginas/detalleiniciativa.aspx?iniciativaID=466

Teniendo en cuenta la evidente relación entre defensa y seguridad, también es fundamental desarrollar la ciberseguridad para impedir que acciones externas (ciberataques) puedan desestabilizar los sistemas estatales. Las amenazas híbridas, que atacan vulnerabilidades sistémicas, tienen entre sus objetivos más patentes los relacionados con el ciberespacio.

Con el fin de impulsar la ciencia y la innovación, en áreas estratégicas como la comunicación cuántica, el Gobierno de España ha puesto en marcha planes complementarios de I+D+i, programas en colaboración con las comunidades autónomas. Destaca el Plan de Comunicación Cuántica que tiene como objetivos crear una infraestructura de comunicaciones de alta seguridad en España; apoyar la industria cuántica europea e impulsar un nuevo sector industrial con nuevas empresas en el ámbito digital y de la ciberseguridad. El programa cuenta con la participación de las Comunidades de Madrid, Cataluña, País Vasco, Galicia y Castilla y León, así como del CSIC.

La línea principal de actuación de este programa es desarrollar una red de comunicaciones de alta seguridad (anillo cuántico), resistente a cualquier ataque computacional, ya sea por medios clásicos o cuánticos, primero para sistemas en fibra y, más adelante, en otras redes más amplias, incluyendo los satélites, que constituye el segmento espacial de la EuroQCI (European Quantum Communication Infrastructure) para las comunicaciones a muy larga distancia, y, también, comunicaciones con vehículo aéreo no tripulado. En esta misma línea se desarrollará tecnología basada en entrelazamiento, incluyendo repetidores cuánticos para CC a largas distancias (>300 km) sobre fibras ópticas.

La Infraestructura desplegada de Comunicaciones Cuánticas de Madrid, es actualmente uno de los nodos del proyecto OpenQKD que puede verse, desde la perspectiva del programa principal, como un plan complementario de Comunicaciones Cuánticas, como el embrión de la Infraestructura Cuántica Europea, una infraestructura de comunicaciones cuánticas paneuropea que conecta toda Europa, que tendrá una parte terrestre basada en fibra óptica y un segmento espacial basado en satélite. Estas redes promoverán la interoperabilidad y la cooperación entre los países de la UE, colocando a Europa en una posición privilegiada en términos de investigación, innovación y seguridad con España a la cabeza.

Conclusiones

La revolución digital ofrece ahora una oportunidad de crecimiento en todos los sectores económicos y sociales, pero estos precisan de una verdadera transformación para integrarla en sus procesos y generar el beneficio productivo, social y medioambiental que exige la nueva economía. Los gobiernos y las instituciones públicas tienen un papel crucial en esta transformación, pero también, la sociedad y los ciudadanos deben abrazar la innovación tecnológica y conocer sus riesgos para que sea verdaderamente un factor crucial de progreso.

A lo largo de las últimas décadas se ha hecho cada vez más estrecha la relación entre el desarrollo tecnológico, científico y de la innovación, por un lado, y el desarrollo económico por el otro. Junto a ello, se ha ido haciendo cada vez más evidente que no es posible asegurar la defensa y la seguridad nacionales si no se invierte en un desarrollo tecnológico y en una innovación militar y de seguridad que permitan a España, a Europa y a los países que integran la OTAN, hacer frente a unas amenazas emergentes que evolucionan muy rápidamente y que, tal y como hemos visto, podrían ser masivas y a gran escala si se benefician del uso de la computación cuántica.

La computación cuántica y las tecnologías con ella relacionadas pueden ser críticas y suponer un cambio de paradigma sin precedentes en todos los ámbitos y también en el de la Defensa. Por ello, resulta un objetivo estratégico fundamental promover el desarrollo de la investigación cuántica, impulsando para ello la colaboración con la industria, la Universidad y los centros de investigación especializados, así como el acuerdo con instituciones internacionales. Las iniciativas que está desarrollando España muestran la apuesta nacional por impulsar su presencia en este ámbito y por potenciar la soberanía europea en la computación cuántica mediante la cooperación internacional. La exigencia económica y técnica que implica el desarrollo de estas tecnologías y el salto cualitativo que podría suponer su implantación en cuanto a capacidades defensivas, hacen fundamental no quedarse atrás y generar las sinergias necesarias para que nuestros bloques geopolíticos mantengan el grado de superioridad necesario en la esfera internacional.

En definitiva, si bien la investigación en materia de computación cuántica se encuentra en estado de desarrollo, nadie duda de que tendrá un impacto significativo en la Seguridad Nacional. No obstante, nadie puede asegurar hoy cómo ni cuándo este

entorno cuántico será realidad, ni en qué medida afectará –no sólo a la Seguridad Nacional- sino a la vida diaria.

Estas afirmaciones, unidas al hecho cierto de que la mayoría de los Gobiernos, de las entidades públicas y privadas, junto a la mayor parte de sus líderes y, sobre todo, la mayoría de la sociedad no están preparados para el entorno cuántico que se aproxima, exigen la adopción de decisiones y medidas concretas.

Parece necesario desarrollar una estrategia nacional que aúne todas las iniciativas y las aglutine en torno a la seguridad, enfocada no solo a las prioridades de seguridad nacional, las infraestructuras críticas, la Administración y los sectores estratégicos, sino que cubra también la seguridad económica y social. Esta estrategia, además, debe enfocarse con una actitud proactiva, de modo que incentive el liderazgo tecnológico y en la innovación para mitigar la dependencia de las grandes potencias industriales y estatales.

Una adecuada combinación de educación, divulgación y preparación básica pueden convertir a cualquier organización o empresa –independientemente de su tamaño o naturaleza- en una organización o empresa cuántica y, de este modo, mitigar los efectos de un impacto brusco en la seguridad y bienestar de los ciudadanos.