

Tecnologie quantistiche: profili tecnologici, scenari geopolitici e prospettive per l'Italia

di Giovanni Trotta

Abstract

Le tecnologie quantistiche stanno progressivamente emergendo come una delle frontiere più rilevanti dell'innovazione contemporanea, per le loro potenziali implicazioni nei campi del calcolo, delle comunicazioni sicure e della sensoristica avanzata. Questo contributo propone una ricognizione introduttiva delle tre principali traiettorie del settore, *quantum computing*, *quantum communication* e *quantum sensing*, con l'obiettivo di chiarirne i fondamenti tecnico-funzionali, i principali ambiti applicativi e il diverso grado di maturità industriale. Il *quantum computing* viene analizzato come paradigma computazionale specializzato, destinato ad affiancare il calcolo classico nella soluzione di problemi ad alta complessità; la *quantum communication* come insieme di soluzioni orientate a rafforzare la sicurezza delle reti e delle comunicazioni; il *quantum sensing* come nuova generazione di tecnologie metrologiche ad altissima precisione, già vicine a diversi impieghi applicativi concreti. Su questa base, l'analisi colloca lo sviluppo delle tecnologie quantistiche entro il quadro della competizione internazionale, mettendo a confronto il modello statunitense, quello cinese e quello europeo. In tale contesto, l'Italia emerge come un ecosistema di scala intermedia ma strategicamente rilevante, caratterizzato da una crescente integrazione tra ricerca, infrastrutture, politiche pubbliche e iniziative imprenditoriali, con specializzazioni particolarmente visibili nella comunicazione quantistica, nella metrologia, nella fotonica e nell'integrazione tra *high-performance computing* e sistemi quantistici.

Quantum technologies are increasingly emerging as one of the most relevant frontiers of contemporary innovation, given their potential implications for computation, secure communications, and advanced sensing. This contribution provides an introductory overview of the three main technological trajectories in the field, *quantum computing*, *quantum communication*, and *quantum sensing*, with the aim of clarifying their underlying principles, key application domains, and differing levels of industrial maturity. *Quantum computing* is examined as a specialized computational paradigm designed to complement classical systems in addressing highly complex problems; *quantum communication* as a set of solutions aimed at strengthening the security of networks and data transmission; and *quantum sensing* as a new generation of high-precision metrological technologies, already approaching concrete applications in several domains. Building on this framework, the analysis situates the

development of quantum technologies within the broader landscape of international competition, comparing the United States, China, and Europe. In this context, Italy emerges as an intermediate but strategically relevant ecosystem, characterized by a growing integration of research, infrastructures, public policies, and entrepreneurial initiatives, with particular strengths in quantum communication, metrology, photonics, and the integration of *high-performance computing* and quantum systems.

Introduzione

Le tecnologie quantistiche occupano oggi una posizione paradossale nel dibattito sull'innovazione contemporanea. Da un lato, si tratta di un dominio in cui la base scientifica è straordinariamente solida: i fenomeni fisici che ne costituiscono il fondamento sono noti e validati sperimentalmente da quasi un secolo, le piattaforme tecnologiche sono molteplici e in costante evoluzione, e la produzione scientifica internazionale cresce a ritmi sostenuti. Dall'altro lato, la traduzione di questo patrimonio scientifico in capacità industriale stabile, in catene di fornitura mature e in mercati di sbocco riconoscibili procede a una velocità sensibilmente inferiore, e con modalità profondamente diverse a seconda dei contesti nazionali. Tra ciò che la fisica quantistica già consente di fare in laboratorio e ciò che le imprese, le pubbliche amministrazioni e le infrastrutture critiche sono effettivamente in grado di adottare, esiste una distanza che resta in larga misura il vero terreno della competizione internazionale.

È proprio questa tensione – tra maturità scientifica e maturità industriale – ad attraversare in filigrana la traiettoria delle tecnologie quantistiche e a costituire il filo conduttore di questo contributo. Il *quantum computing*, pur sostenuto da investimenti pubblici e privati di scala crescente, fatica ancora a esprimere applicazioni *general-purpose* economicamente sostenibili al di fuori di domini computazionali molto specifici. La *quantum communication* mostra un livello di prossimità al mercato più avanzato, soprattutto nelle applicazioni di sicurezza, ma deve confrontarsi con il problema dell'integrazione nelle infrastrutture di rete esistenti e con la coesistenza, in parte cooperativa e in parte competitiva, con la crittografia *post-quantum*. Il *quantum sensing*, infine, è la traiettoria in cui il passaggio dalla prestazione di laboratorio alla diffusione industriale appare oggi più avanzato, pur in presenza di limiti significativi sul fronte della miniaturizzazione e della standardizzazione.

Su queste premesse, il contributo si propone di offrire una mappa di orientamento per un lettore non specialista, articolata su due livelli di analisi tra loro complementari. Un primo livello, di carattere tecnico-funzionale, ricostruisce i fondamenti e gli ambiti applicativi delle tre principali traiettorie del settore. Un secondo livello, di carattere geopolitico, colloca queste traiettorie nel quadro della competizione tra Stati Uniti, Cina ed Europa, leggendole come declinazioni diverse di una stessa difficoltà di fondo: trasformare il sapere in capacità industriale. È in questo secondo livello che il caso italiano trova la propria collocazione specifica, come ecosistema di scala intermedia che ha cominciato a strutturare la propria filiera quantistica proprio attorno al nodo critico della valorizzazione industriale della ricerca. Resta consapevolmente fuori dal perimetro del contributo, invece, l'analisi tecnica dettagliata degli algoritmi quantistici, lo studio degli ecosistemi nazionali minori e la valutazione comparativa delle singole soluzioni proprietarie.

Capitolo 1 – Le diverse tecnologie quantistiche: una rassegna preliminare

Quantum computing

Definizione

Il paradigma del *quantum computing* si fonda sull'integrazione dei principi della meccanica quantistica per superare le barriere computazionali intrinseche alle architetture tradizionali, le quali risultano spesso inadeguate di fronte a carichi di lavoro eccessivi in termini di tempo, memoria e risorse energetiche. Piuttosto che proporsi come un sostituto universale del calcolo classico, questa tecnologia mira a introdurre architetture specializzate per la risoluzione di specifiche classi di problemi ad alta complessità. L'efficacia di tale approccio si manifesta con particolare evidenza nella simulazione di sistemi fisico-chimici, nell'ottimizzazione combinatoria e nelle analisi di natura probabilistica. In ultima analisi, il valore aggiunto del calcolo quantistico risiede proprio nella capacità di intervenire laddove i metodi convenzionali – pur supportati da sistemi di *High-Performance Computing* (HPC) – mostrano limiti strutturali di scalabilità o costi computazionali proibitivi.

La differenza rispetto all'informatica tradizionale riguarda in primo luogo l'unità minima di informazione. Nei sistemi classici l'elaborazione si basa sul bit, che assume valori discreti e mutuamente esclusivi, 0 oppure 1. Nel calcolo quantistico si impiega

invece il *quantum bit* (qubit), un'unità informativa che può essere realizzata fisicamente secondo tecnologie differenti e che possiede proprietà non equivalenti a quelle dei bit classici. È però importante chiarire che tali proprietà non generano automaticamente un vantaggio in ogni scenario: il beneficio computazionale si manifesta solo quando le risorse quantistiche sono incorporate in architetture e algoritmi in grado di tradurle in un incremento di efficienza, accuratezza o capacità risolutiva rispetto alle migliori alternative classiche disponibili.

Le principali proprietà che rendono i qubit potenzialmente abilitanti sono tre. La prima è la sovrapposizione, per cui un qubit può essere preparato in una combinazione degli stati di base e quindi rappresentare, durante l'evoluzione del calcolo, più configurazioni possibili del problema. La seconda è l'entanglement, cioè una forma di correlazione quantistica per cui lo stato complessivo di più qubit non può essere descritto come semplice somma di stati indipendenti: una parte dell'informazione risiede nelle relazioni tra i qubit stessi. La terza è l'interferenza, che consente di progettare l'evoluzione del sistema in modo da amplificare la probabilità degli esiti desiderati e sopprimere quella degli esiti non desiderati. In termini intuitivi, ciò non significa che il computer quantistico “provi tutto contemporaneamente”, ma che manipola una distribuzione di possibilità con modalità che, in alcuni problemi, possono risultare più efficienti del calcolo convenzionale.

Principali piattaforme tecnologiche

Dal punto di vista ingegneristico, il *quantum computing* non coincide con una sola tecnologia, ma con una famiglia di piattaforme diverse, ciascuna caratterizzata da specifici vantaggi e limiti. I qubit superconduttivi sono realizzati tramite circuiti superconduttori che operano a temperature prossime allo zero assoluto e rappresentano oggi una delle piattaforme più adottate in ambito industriale e sono al centro delle iniziative di attori come IBM, Google, Amazon, D-Wave, Rigetti e IQM. Gli ioni intrappolati si basano invece su atomi ionizzati confinati in trappole elettromagnetiche e controllati con impulsi laser; sono spesso associati a elevata coerenza e robustezza operativa e vengono perseguiti, tra gli altri, da Quantinuum e IonQ. I qubit fotonici utilizzano fotoni come portatori di informazione: offrono buona resistenza al rumore e particolare idoneità alle comunicazioni su lunga distanza, motivo per cui sono sviluppati da imprese come PsiQuantum e Xanadu.

Accanto a queste piattaforme, stanno emergendo ulteriori approcci. I qubit ad atomi neutri sono realizzati con atomi non ionizzati, raffreddati e controllati otticamente, e vengono spesso considerati un buon compromesso tra scalabilità e coerenza; tra i principali attori figurano QuEra, Pasqal, Atom Computing e Infleqtion. I qubit a spin in silicio utilizzano lo *spin* di elettroni intrappolati in strutture semiconduttrici e presentano il vantaggio di potersi sviluppare in continuità con la filiera industriale del silicio già esistente; tra gli attori maggiormente impegnati in questa direzione figura Intel. I qubit topologici si fondano su quasiparticelle esotiche e mirano a ottenere una tolleranza intrinseca agli errori; Microsoft è il principale sostenitore di questo approccio, che però resta ancora in una fase relativamente più esplorativa. Infine, i Nitrogen-Vacancy Center sfruttano difetti puntuali nel reticolo cristallino del diamante: hanno il vantaggio di poter operare anche a temperatura ambiente, ma pongono sfide di scalabilità industriale legate alla complessità dei materiali impiegati. Questo approccio è sviluppato, tra gli altri, da Quantum Brilliance e SaxonQ, anche in ottica di acceleratori compatti integrabili nei *data center*.

Metriche di maturità e principali trade-off

Il confronto tra queste piattaforme non può essere ridotto al semplice numero di qubit. La maturità di una tecnologia quantistica dipende infatti da un insieme di metriche che devono essere considerate congiuntamente. La prima è la scalabilità, cioè la capacità di aumentare il numero di qubit senza compromettere stabilità e prestazioni complessive. La seconda è la velocità di esecuzione, intesa come numero di operazioni quantistiche realizzabili nell'unità di tempo. La terza è il tempo di coerenza, ossia l'intervallo durante il quale uno stato quantistico mantiene le proprie proprietà prima che la decoerenza ne degradi l'informazione. A queste dimensioni si aggiunge la fedeltà delle operazioni, cioè l'accuratezza con cui il sistema implementa porte logiche e misure.

La sfida industriale consiste nel far crescere simultaneamente queste metriche, poiché l'incremento di una dimensione può compromettere le altre. Aumentare il numero di qubit, ad esempio, può rendere più difficile preservare coerenza e fedeltà; incrementare la velocità può accentuare problemi di rumore; aumentare la complessità dell'architettura può ridurre l'affidabilità complessiva. Per cui, il problema non è solo "quanti qubit" si possiedono, ma quanto tali qubit siano controllabili, accurati e utili su scala reale.

L'attuale fase di sviluppo del *quantum computing* è quindi caratterizzata da un forte orientamento verso modelli ibridi, nei quali sistemi classici e quantistici lavorano in sinergia. In molti casi, il processore quantistico non sostituisce il calcolo convenzionale, ma opera come acceleratore specializzato per sotto-problemi particolarmente difficili, mentre il resto del flusso computazionale resta affidato a infrastrutture classiche o a sistemi HPC. Questa logica ibrida riflette il fatto che il vantaggio quantistico, quando emerge, tende a manifestarsi in compiti mirati più che in applicazioni *general-purpose*.

Ambiti applicativi

Le applicazioni industriali oggi considerate più promettenti si concentrano nei domini ad alta complessità. In ambito farmaceutico, chimico e dei materiali, il *quantum computing* è ritenuto particolarmente interessante per la simulazione di molecole, la scoperta di nuovi farmaci, lo sviluppo di nuovi materiali e la modellazione di interazioni tra proteine e composti chimici. Il potenziale riguarda anche la creazione di *digital twins* di sistemi biologici complessi, il *protein folding*, l'analisi di dati biomedici e l'ottimizzazione di *trial* clinici, benché tali applicazioni richiedano ancora notevoli progressi tecnologici e organizzativi.

Altri settori promettenti sono la logistica, i trasporti, l'energia e la finanza. Nella logistica il *quantum computing* viene studiato per problemi di *routing*, pianificazione delle consegne, allocazione di risorse e gestione dinamica dei flussi, soprattutto quando la variabilità del contesto rende poco efficaci gli approcci euristici tradizionali. Nel settore energetico, l'interesse riguarda l'ottimizzazione delle *smart grids*, la riconfigurazione delle reti e la soluzione di problemi complessi come lo *Unit Commitment Problem* (UCP), cioè la scelta ottimale di quali impianti attivare in funzione del carico di rete. In finanza, il potenziale si concentra su simulazioni stocastiche, analisi del rischio, ottimizzazione di portafoglio e gestione di grandi quantità di dati. In parallelo, si osserva crescente attenzione per l'interazione tra *quantum computing* e intelligenza artificiale soprattutto per applicazioni di *machine learning* avanzato, modellazione complessa e analisi di grandi basi di dati.

Nel complesso, il *quantum computing* va interpretato non come una tecnologia destinata a rimpiazzare il calcolo classico, ma come una frontiera computazionale specializzata, il cui valore dipende dalla capacità di applicarla a problemi in cui la struttura matematica del compito è realmente compatibile con le risorse quantistiche

disponibili. La sua traiettoria di sviluppo è ancora segnata da limiti importanti, ma il numero crescente di investimenti, piattaforme, collaborazioni industriali e casi d'uso suggerisce che il settore stia progressivamente passando da una fase prevalentemente sperimentale a una fase di più chiara articolazione industriale.

Quantum communication

Definizione

La *quantum communication* identifica un insieme di tecnologie di telecomunicazione che impiegano proprietà della meccanica quantistica, in particolare la sovrapposizione e l'*entanglement*, per realizzare canali di trasmissione con caratteristiche di sicurezza fisica intrinseca e, in alcuni casi, con potenziali vantaggi di efficienza rispetto ai sistemi convenzionali. L'interesse per queste soluzioni cresce in parallelo con l'aumento delle interdipendenze digitali, della superficie di attacco delle reti e della prospettiva che futuri computer quantistici possano compromettere parte della crittografia classica oggi impiegata. In questo contesto, la comunicazione quantistica si configura come una frontiera rilevante per la protezione delle informazioni sensibili e per l'evoluzione delle infrastrutture di rete sicure.

L'elemento distintivo rispetto alle comunicazioni classiche è che la sicurezza non viene affidata esclusivamente a protocolli crittografici basati su difficoltà computazionali, ma anche alle proprietà fisiche del canale trasmissivo. Nelle reti tradizionali, i dati vengono trasmessi sotto forma di impulsi binari lungo rame, fibra ottica o collegamenti radio, e la loro protezione dipende principalmente da algoritmi e protocolli *software*. Nella comunicazione quantistica, invece, si impiegano fotoni come portatori di informazione, sfruttando il fatto che i loro stati quantistici possono essere preparati, manipolati e misurati in modi che rendono rilevabile un'eventuale intercettazione. In termini operativi, ciò significa che un tentativo di accesso non autorizzato tende a lasciare una traccia fisica nella trasmissione stessa, alterando lo stato quantistico utilizzato per lo scambio.

È importante chiarire che questo non rende automaticamente inviolabile ogni comunicazione. Più precisamente, la comunicazione quantistica consente di rafforzare alcune funzioni critiche della sicurezza, in particolare la distribuzione delle chiavi crittografiche, facendo leva su meccanismi fisici che non dipendono soltanto dalla robustezza di un algoritmo. Per questa ragione il suo interesse è particolarmente elevato

nei contesti in cui la riservatezza del dato, la tempestiva rilevazione di intrusioni e la resilienza a minacce future costituiscono requisiti strutturali.

La Quantum Key Distribution

L'applicazione oggi più matura della *quantum communication* è la *Quantum Key Distribution* (QKD). La QKD non serve a trasmettere direttamente il contenuto dei messaggi, ma a permettere a due interlocutori, convenzionalmente denominati Alice e Bob, di condividere una chiave segreta in modo tale che eventuali tentativi di intercettazione risultino rilevabili. In questo senso, la QKD affronta uno dei punti più delicati di molte architetture crittografiche: lo scambio iniziale delle chiavi.

Il primo protocollo elaborato a questo scopo è il BB84, proposto nel 1984 da Bennett e Brassard. Il suo principio fondamentale è che la misura di uno stato quantistico ne modifica il contenuto: se un attaccante tenta di osservare la chiave durante la trasmissione, altera inevitabilmente gli stati quantistici impiegati per codificarla. Di conseguenza, l'informazione intercettata non è pienamente affidabile e, allo stesso tempo, i due interlocutori possono rilevare l'intrusione e scartare la chiave compromessa. In questo modo, una parte della sicurezza si sposta dal livello puramente matematico a quello fisico del canale.

Accanto al BB84 si collocano protocolli successivi, come quello di Ekert, e schemi più avanzati che sfruttano il *Quantum Teleportation* e forme più sofisticate di *entanglement* tra fotoni. Il punto essenziale, anche in questi casi, è che la correlazione quantistica può essere utilizzata per costruire protocolli di sicurezza più robusti. Tuttavia, la QKD non sostituisce né elimina i canali tradizionali: le chiavi vengono distribuite tramite il canale quantistico, ma i dati continuano a essere trasmessi su reti classiche. La comunicazione quantistica va quindi interpretata come una componente di architetture ibride, non come un'alternativa integrale alle telecomunicazioni convenzionali.

Questa logica è già stata sperimentata sia su reti terrestri in fibra ottica sia tramite collegamenti satellitari, aprendo la strada a reti quantistiche distribuite e alla prospettiva, ancora in evoluzione, di una futura *Quantum Internet*. In questa prospettiva, una delle sfide tecnologiche più ambiziose riguarda lo sviluppo dei *quantum repeaters*, dispositivi pensati per estendere la portata delle comunicazioni quantistiche su distanze molto superiori a quelle oggi gestibili con collegamenti diretti in fibra. A differenza dei ripetitori classici, che amplificano semplicemente il segnale, i *quantum repeaters* devono preservare le proprietà quantistiche dell'informazione

trasmessa, in particolare l'*entanglement*, senza distruggerne il contenuto fisico. Si tratta di un obiettivo particolarmente complesso, perché richiede il coordinamento di memorie quantistiche, protocolli di scambio dell'*entanglement* e meccanismi di correzione o mitigazione delle perdite lungo il canale. Proprio per questo, i *quantum repeaters* sono considerati una tecnologia abilitante cruciale per passare da collegamenti punto-punto o metropolitani a reti quantistiche su scala nazionale, continentale e, in prospettiva, globale. La *Quantum Internet* non va quindi intesa come una semplice estensione di Internet in chiave più sicura, ma come una possibile futura infrastruttura di rete capace di connettere nodi quantistici remoti.

Efficienza trasmissiva

Sebbene la sicurezza sia l'aspetto più noto, la *quantum communication* non si esaurisce nella QKD. Una tecnica rilevante è il *Superdense Coding*, che mostra come l'*entanglement* possa essere sfruttato anche per aumentare l'efficienza della trasmissione. In una comunicazione classica, un bit trasporta al massimo un'informazione binaria; nel *Superdense Coding*, invece, è possibile trasmettere due bit classici utilizzando un solo fotone, a condizione che esso sia *entangled* con un secondo fotone già detenuto dal destinatario. Questo non significa che ogni rete quantistica raddoppierà automaticamente la propria capacità, ma evidenzia come le correlazioni quantistiche possano essere usate non solo per proteggere l'informazione, ma anche per ottimizzarne il trasferimento.

Accanto ai protocolli, assumono un ruolo importante alcune componenti abilitanti. Tra queste vi sono i *Quantum Random Number Generator* (QRNG), che sfruttano i meccanismi probabilistici della meccanica quantistica per generare sequenze di numeri realmente casuali, utili sia nella QKD sia in molte altre applicazioni di sicurezza. A differenza dei *Pseudo Random Number Generator* (PRNG), i QRNG non si basano su processi deterministici e risultano quindi particolarmente interessanti nei contesti in cui la casualità costituisce una risorsa critica. Un'altra componente chiave è rappresentata dai *Single-Photon Detectors* (SPDs), dispositivi essenziali per rilevare segnali ottici estremamente deboli e quindi centrali nel funzionamento delle reti quantistiche e di molte applicazioni di ottica avanzata. Questo mostra come la comunicazione quantistica non coincida soltanto con il canale o con il protocollo, ma coinvolga anche una filiera di dispositivi, componenti e *software* necessari per rendere operative queste tecnologie in ambienti reali.

Ambiti applicativi

Dal punto di vista applicativo, la *quantum communication* è considerata una delle tecnologie quantistiche più vicine a impieghi concreti nel breve periodo. I contesti di maggiore interesse sono quelli in cui la protezione delle comunicazioni è un requisito strutturale, come difesa e sicurezza, servizi finanziari, telecomunicazioni, *healthcare*, ambienti *cloud* e *data center*.

Anche sul piano industriale sta emergendo una filiera specializzata, composta da imprese che sviluppano protocolli QKD, QRNG, SPD e soluzioni di integrazione nelle reti esistenti. Tra gli attori più rilevanti figurano ID Quantique, EvolutionQ, QuSecure e, nel contesto italiano, Quantum Telecommunications Italy (QTI), insieme ad altre realtà attive nello sviluppo di sistemi QKD, generatori quantistici di numeri casuali e soluzioni per reti in fibra o *free-space*. Nel complesso, si tratta di un ecosistema ancora in evoluzione, ma già sufficientemente maturo da mostrare una traiettoria industriale più vicina all'adozione rispetto ad altre tecnologie quantistiche.

Quantum sensing*Definizione*

Il *quantum sensing* è l'ambito delle tecnologie quantistiche dedicato alla realizzazione di sensori ultrasensibili, progettati per rilevare variazioni estremamente piccole di grandezze fisiche come tempo, gravità, campi magnetici, campi elettrici, accelerazione e temperatura. Il suo tratto distintivo non consiste soltanto in un miglioramento rispetto alla sensoristica convenzionale, ma nella possibilità di spingersi verso regimi di misura in cui la sensibilità diventa un fattore realmente abilitante per nuove applicazioni e, in alcuni casi, per l'osservazione di fenomeni che con la strumentazione tradizionale risultano difficili o impossibili da rilevare.

Da un punto di vista metrologico, il vantaggio del *quantum sensing* è duplice. Da un lato, consente di misurare meglio grandezze già rilevabili con sensori classici, aumentando precisione, stabilità, risoluzione e affidabilità. Dall'altro, permette di accedere a segnali estremamente deboli o a variazioni minime che diventano informative proprio grazie alla sensibilità del sensore. In questo senso, la novità non riguarda solo la qualità della misura, ma anche la possibilità di ampliare lo spazio dei fenomeni osservabili. Ciò è particolarmente rilevante in contesti nei quali la qualità del

dato misurato condiziona direttamente la capacità di prendere decisioni, monitorare sistemi complessi o abilitare nuovi servizi.

Questa capacità si traduce in alcune proprietà generali che spiegano il crescente interesse industriale per la sensoristica quantistica: maggiore sensibilità ai segnali deboli, precisione superiore rispetto ai limiti classici, velocità di rilevazione e, in alcuni casi, anche migliori condizioni operative rispetto a sensori tradizionali comparabili. Per questo il *quantum sensing* può essere interpretato come una nuova generazione di tecnologie metrologiche, in grado di intervenire a monte della catena del valore informativa: se il dato è più preciso, stabile e tempestivo, migliorano di conseguenza anche osservazione, navigazione, controllo e monitoraggio.

Principali traiettorie tecnologiche

Il *quantum sensing* non coincide con un'unica classe di dispositivi, ma comprende diverse famiglie di sensori, ciascuna ottimizzata per specifiche grandezze fisiche e contesti applicativi. Una prima categoria è costituita dagli orologi atomici, che rappresentano una delle forme più mature di sensoristica quantistica. Il loro valore risiede nell'estrema accuratezza con cui consentono di misurare tempo e frequenza, rendendoli centrali in applicazioni quali navigazione, telecomunicazioni e finanza, dove sincronizzazione e *timestamping* sono funzioni critiche. La loro rilevanza è particolarmente evidente nei sistemi di posizionamento satellitare: scarti temporali dell'ordine di pochi nanosecondi possono tradursi in errori di localizzazione al suolo di diversi metri.

Una seconda traiettoria tecnologica è quella degli interferometri atomici, progettati per sfruttare il comportamento ondulatorio della materia. Questi sensori, spesso basati su atomi ultra-freddi posti in uno stato di sovrapposizione quantistica, oppure su configurazioni ottiche, risultano particolarmente interessanti perché possono operare con elevata stabilità nel tempo, senza richiedere continua calibrazione e mantenendo buone prestazioni anche in ambienti difficili o per lunghi periodi di funzionamento. In forma di accelerometri, giroscopi e gravimetri quantistici, trovano applicazione nella navigazione inerziale, nelle ricerche geofisiche, nel monitoraggio infrastrutturale e in varie applicazioni dei trasporti e della logistica. Tra questi, i gravimetri quantistici emergono per la capacità di rilevare strutture sotterranee, falde acquifere o giacimenti senza ricorrere a lunghe e costose attività di scavo, e hanno già trovato impiego anche nella caratterizzazione del sottosuolo di aree vulcaniche.

Un'altra famiglia importante è quella dei magnetometri atomici, utilizzati per rilevare campi magnetici estremamente deboli. Questi dispositivi possono essere basati su atomi in fase gassosa, come rubidio o cesio, oppure su difetti atomici in materiali solidi, come i *Nitrogen-Vacancy Center* nel diamante. Un vantaggio rilevante di questa tecnologia è la possibilità, in molti casi, di operare a temperatura ambiente pur mantenendo livelli di sensibilità molto elevati, con benefici in termini di portabilità, consumo energetico e riduzione della complessità criogenica. Questo li rende particolarmente promettenti in applicazioni come l'*imaging* cerebrale, il monitoraggio avanzato e il controllo non distruttivo.

Accanto a queste traiettorie si collocano anche sensori atomici di campo elettrico e sensori ottici quantistici. I primi risultano interessanti in ambito diagnostico ed elettronico per il rilevamento di variazioni locali e il monitoraggio di componenti; i secondi, che utilizzano stati quantistici della luce e dei fotoni, comprendono interferometri ottici e altre architetture adatte a misure ottiche ultra-precise, *quantum imaging* e *sensing* ottico.

Ambiti applicativi

Sul piano applicativo, il *quantum sensing* è spesso considerato una delle tecnologie quantistiche più vicine a una fase quasi produttiva, proprio perché molte delle sue applicazioni non richiedono necessariamente grandi infrastrutture di rete o di calcolo, ma possono tradursi in dispositivi specialistici ad alto valore aggiunto. I settori di maggiore interesse comprendono *healthcare*, geologia, monitoraggio ambientale, difesa, manifattura di precisione, aerospazio, logistica e navigazione. In ambito sanitario, i sensori quantistici sono promettenti per scansioni neurologiche non invasive e per il monitoraggio precoce di parametri fisiologici; in geofisica e vulcanologia, per la rilevazione di strutture sotterranee, risorse naturali e variazioni gravitazionali; nella difesa e nella sicurezza, per sistemi radar avanzati, navigazione di precisione e capacità operative in ambienti complessi; nei trasporti e nella mobilità autonoma, per funzioni di orientamento, *backup* ai sistemi *Global Navigation Satellite System* (GNSS) e navigazione inerziale.

Anche sul piano industriale sta emergendo una filiera specializzata, composta da imprese attive nello sviluppo di sensori geofisici, biomagnetici, sistemi di controllo quantistico e piattaforme per applicazioni metrologiche avanzate. La traiettoria del settore appare già sostenuta da applicazioni reali e da una domanda crescente nei

comparti che richiedono dati ultra-precisi per abilitare nuovi servizi. Restano tuttavia alcune sfide rilevanti, in particolare quelle legate a miniaturizzazione, standardizzazione e integrazione con sensoristica e infrastrutture esistenti. Per questa ragione, il *quantum sensing* può essere considerato una tecnologia con forte potenziale industriale nel breve e medio periodo, ma ancora impegnata in un passaggio delicato dalla prestazione sperimentale alla diffusione su scala più ampia.

Nel complesso, il *quantum sensing* rappresenta quindi una frontiera della misura più che del calcolo o della trasmissione: il suo valore strategico dipende dalla capacità di generare dati migliori, più stabili e più informativi, in contesti nei quali la qualità della misura condiziona direttamente la qualità del servizio, della decisione o dell'intervento operativo. Proprio per questo, tra le principali famiglie delle tecnologie quantistiche, è una di quelle che più chiaramente mostrano come i principi della fisica quantistica possano tradursi in vantaggi industriali concreti già nel presente.

Capitolo 2 – Il panorama delle tecnologie quantistiche: quadro internazionale

2.1-II panorama delle tecnologie quantistiche negli Stati Uniti

Gli Stati Uniti rappresentano oggi l'ecosistema quantistico più completo dal punto di vista della catena del valore. Il tratto distintivo del modello statunitense è la compresenza, nello stesso spazio nazionale, di tutti gli attori chiave: settore pubblico, apparato militare, università, laboratori federali, grandi piattaforme tecnologiche, *startup* e partnership pubblico-private. Questo assetto consente agli Stati Uniti di presidiare non solo la ricerca di frontiera, ma anche le fasi di *testing*, trasferimento tecnologico, standardizzazione e primi percorsi di industrializzazione, configurando un ecosistema in cui scienza, politica industriale e mercato risultano fortemente integrati.

Questa traiettoria è stata formalizzata con la *National Quantum Initiative* (NQI) del 2018, pensata per consolidare la *leadership* statunitense nelle scienze e nelle applicazioni quantistiche. L'impostazione è ampia e sistemica: le priorità riguardano ricerca scientifica, formazione della forza lavoro, industria, infrastrutture, sicurezza economica e cooperazione internazionale. In questo quadro, il *quantum* non è considerato soltanto una tecnologia emergente, ma una capacità critica per la

competitività industriale, la sicurezza nazionale e le applicazioni *dual-use*, con il coinvolgimento diretto di attori come il *Department of Defense*, il *Department of Homeland Security* e la *Defense Advanced Research Projects Agency* (DARPA). Anche sul piano finanziario gli Stati Uniti mantengono un ruolo centrale: gli investimenti pubblici cumulati sono stimati in circa 6 miliardi di dollari¹, ai quali si affiancano iniziative statali di rilievo, come 500 milioni di dollari in Illinois² e un piano da 1 miliardo di dollari nel Maryland³ per infrastrutture quantistiche. A questa base pubblica si somma una forte capacità di attrarre capitale privato: nel 2024 i finanziamenti di *venture capital* destinati a *startup* e *scale-up* quantistiche hanno raggiunto a livello globale circa 2 miliardi di dollari, con una crescita del 50% sull'anno precedente⁴.

Il cuore del vantaggio competitivo statunitense risiede tuttavia nella capacità di far interagire grandi piattaforme tecnologiche e imprenditorialità *deep tech*. IBM, Google, Amazon e Microsoft investono miliardi di dollari in ricerca, collaborazioni accademiche, sviluppo di *hardware* e *software* e integrazione con infrastrutture digitali, agendo da catalizzatori per l'intero ecosistema. La loro presenza facilita la nascita di *startup* fornitrici di componenti, *software* e servizi e accelera il passaggio dalla sperimentazione alla costruzione di offerte accessibili al mercato. In questo gruppo, IBM continua a occupare una posizione di primo piano sia come attore *full-stack* sia per la sua roadmap verso sistemi *fault-tolerant*⁵, che include Starling come primo sistema previsto per il 2029 e una successiva espansione verso macchine con migliaia di qubit logici; Google resta uno degli attori simbolicamente più rilevanti per il lavoro sulla riduzione degli errori e per i progressi mostrati con Willow; Amazon Web Services ha rafforzato la propria presenza anche sul versante dei processori con Ocelot, un *chip* che utilizza i "*cat qubits*", una tecnologia specifica che garantisce una maggiore stabilità e resiste intrinsecamente ad alcuni tipi di errori; Microsoft, infine, presidia una traiettoria più sperimentale con i qubit topologici e il chip Majorana 1.

¹ McKinsey Digital, *Quantum Technology Monitor* (giugno 2025)

² <https://dceo.illinois.gov/expandrelocate/incentives/quantum-enterprise-zone-program.html>

³ <https://governor.maryland.gov/news/press/pages/governor-moore-announces-1-billion-capital-of-quantum-initiative.aspx>

⁴ McKinsey Digital, *Quantum Technology Monitor* (giugno 2025)

⁵ Per *fault-tolerant* si intende un sistema quantistico progettato per continuare a eseguire calcoli in modo affidabile anche in presenza di errori fisici dei *qubit*, grazie all'impiego di tecniche di correzione degli errori che distribuiscono l'informazione logica su più *qubit* fisici.

Un ulteriore elemento decisivo del modello statunitense è anche il *Quantum Computing as a Service* (QCaaS) che riduce le barriere alla sperimentazione e trasforma il mercato in una vera infrastruttura di sviluppo. In questo ambito un ruolo centrale è svolto dai grandi operatori *cloud*: IBM con *IBM Quantum Platform*, Google attraverso *Google Cloud*, Amazon Web Services con *Amazon Braket* e Microsoft con *Azure Quantum*. Queste piattaforme consentono ad aziende, università e centri di ricerca di accedere a macchine quantistiche reali o simulatori da remoto, testare algoritmi e confrontare *hardware* diversi senza sostenere i costi di possesso dell'infrastruttura fisica, facendo diventare il *cloud* il collante infrastrutturale del settore e uno dei principali acceleratori della sua adozione.

A queste si affianca una costellazione di imprese specializzate già ben finanziate, e in alcuni casi quotate, come IonQ e Rigetti. Quest'ultima rappresenta un caso emblematico di integrazione *full-stack*, combinando *chip*, *software* e *cloud* proprietario; nel 2024 ha commercializzato la *Quantum Processing Unit* (QPU)⁶ Novera a 9 *qubit* e presentato il processore Ankaa-3 a 82 *qubit*. Accanto alle architetture superconduttive, gli Stati Uniti presidiano anche traiettorie alternative: Atom Computing lavora su sistemi ad atomi neutri e ha dimostrato con Microsoft la gestione di 24 *qubit* logici *entangled*; Infleqtion sviluppa *hardware* ad atomi neutri e collabora con NVIDIA per simulazioni quantistiche sui materiali; SeeQC punta su sistemi *system-on-a-chip*⁷ quantistici per ridurre complessità criogenica, costi e consumi. Il quadro è ulteriormente rafforzato dai cluster territoriali come *Chicago Quantum Exchange*, che mette in rete la *University of Chicago*, l'*Argonne National Laboratory* e il *Fermi National Accelerator Laboratory*, con l'obiettivo di integrare ricerca, test, formazione e trasferimento tecnologico. La logica di cluster è cruciale nel modello statunitense: la prossimità tra università, laboratori, manifattura avanzata e

⁶ La QPU è la componente centrale di un computer quantistico, analogo, per funzione generale, al processore nei sistemi classici: ospita i qubit fisici e le strutture necessarie per manipolarli ed eseguirne le operazioni. In senso più ampio, il termine può includere anche l'elettronica di controllo e l'hardware classico di supporto necessari per l'input, l'output e il funzionamento del sistema.

⁷ Il *system-on-a-chip* è un'architettura in cui diverse funzioni di elaborazione e controllo, che altrimenti sarebbero distribuite su più componenti separati, vengono integrate in un unico chip. Nel caso del *quantum computing*, questo approccio mira a combinare su scala di chip componenti classiche e quantistiche, riducendo complessità hardware, consumi energetici e requisiti del sistema complessivo.

imprese innovative accelera infatti la trasformazione della ricerca in prodotti e capacità industriali.

Nel panorama globale delle tecnologie quantistiche, gli Stati Uniti si distinguono quindi non solo per la qualità della ricerca o per il volume degli investimenti, ma soprattutto per la capacità di integrare politica industriale, capitale privato, grandi imprese tecnologiche e infrastrutture digitali in un ecosistema coerente. Il vero vantaggio competitivo statunitense risiede nella presenza simultanea di tutti i nodi della catena del valore e nella rapidità con cui tali nodi interagiscono. Rispetto all'Europa, il modello statunitense appare meno centrato sulla sola eccellenza scientifica e più orientato alla messa a mercato delle tecnologie, alla costruzione di piattaforme abilitanti e alla crescita di campioni industriali. La sfida principale, per gli Stati Uniti, non è tanto avviare l'ecosistema quanto mantenere il vantaggio in un contesto sempre più competitivo; ma allo stato attuale il Paese resta il riferimento principale per densità imprenditoriale, integrazione tra *computing* e *cloud* e capacità di tradurre il *quantum* in una frontiera concreta della politica tecnologica e industriale.

2.2-II panorama delle tecnologie quantistiche in Cina

La Cina adotta nelle tecnologie quantistiche un modello profondamente diverso rispetto a Stati Uniti ed Europa. Il tratto distintivo è il carattere centralizzato, pianificato e direttamente guidato dal governo, in cui quasi tutte le attività rilevanti sono inserite in una strategia pubblica di lungo periodo. L'obiettivo immediato è costruire sovranità tecnologica, riducendo la dipendenza da fornitori esteri; nel medio-lungo periodo, invece, il Paese mira a diventare esportatore di prodotti e servizi basati sul *quantum*.

Questa impostazione è stata incorporata nel 14° Piano Quinquennale (2021–2025), che ha previsto investimenti, misure normative e semplificazioni per sostenere la crescita digitale del Paese, includendo esplicitamente, accanto al *supercomputing* classico, anche le tecnologie quantistiche. Il piano si inserisce però in un disegno ancora più ampio: entro il 2035, la Cina punta infatti a raggiungere l'indipendenza nella produzione e nella gestione delle tecnologie digitali e informatiche di frontiera. Il *quantum* rientra quindi in una strategia industriale e geopolitica di lungo periodo, nella quale dimensione commerciale, sicurezza e applicazioni *dual-use* risultano strettamente intrecciate.

Sul piano delle risorse mobilitate, la Cina rappresenta oggi il principale investitore pubblico mondiale nelle tecnologie quantistiche. Fino ad aprile 2025, i fondi pubblici cumulati destinati al settore raggiungono 15,3 miliardi di dollari, pari a oltre il 40% dei fondi pubblici globali complessivamente allocati⁸. Questo dato colloca la Cina davanti a UE e Stati Uniti e segnala la volontà di presidiare il settore non solo sul piano scientifico, ma anche su quello industriale e strategico. Alla *leadership* negli investimenti pubblici si accompagna una forte capacità di produzione scientifica e di accumulazione di proprietà intellettuale. La Cina detiene infatti il primato mondiale per numero di pubblicazioni in fisica quantistica, con circa il 42% delle pubblicazioni globali nel 2024, e per domande di brevetto nel *quantum computing*, con circa il 32% del totale, superando gli Stati Uniti⁹. Questo elemento è particolarmente rilevante perché suggerisce che la strategia cinese non si limita al finanziamento pubblico, ma sta producendo anche una base scientifica e tecnologica ampia, funzionale a rafforzare la capacità nazionale di presidiare i segmenti più promettenti della futura *value chain* quantistica.

Anche sul fronte privato il sistema cinese mostra una crescita significativa, pur restando meno aperto e meno orientato al *venture capital* rispetto a quello statunitense. Nel 2023 la Cina ha rappresentato circa il 10% degli investimenti privati globali nel *quantum*¹⁰. Il dato resta inferiore a quello degli Stati Uniti, ma conferma che il comparto sta attirando un interesse crescente anche da parte del capitale privato e che il rafforzamento dell'ecosistema non dipende esclusivamente dall'intervento statale. Tuttavia, a differenza del modello statunitense, in cui il capitale privato svolge una funzione trainante nella nascita e nello *scale-up* delle imprese, in Cina esso si inserisce ancora dentro un quadro complessivamente dominato dalla regia pubblica.

La visione strategica del modello cinese si è tradotta negli ultimi anni in una rapida costruzione di laboratori e infrastrutture scientifiche di altissimo livello nelle principali città universitarie del Paese. Ne emerge un ecosistema in cui ricerca pubblica, priorità industriali e obiettivi strategici nazionali convergono in modo sistematico, con una forte capacità di coordinamento centrale. Dal punto di vista geografico, gli ecosistemi cinesi del *quantum* si concentrano soprattutto nelle grandi aree urbane di Shanghai, Pechino e Hefei, dove si trovano istituti pubblici di ricerca e grandi aziende. Questi poli urbani rappresentano i principali nodi della filiera nazionale e riflettono una logica

⁸ McKinsey Digital, *Quantum Technology Monitor* (giugno 2025).

⁹ Ibidem.

¹⁰ Ibidem.

di sviluppo per *cluster*, ma in una forma diversa da quella occidentale: non tanto ecosistemi spontanei trainati dal *venture capital*, quanto piuttosto piattaforme territoriali fortemente sostenute dalla pianificazione pubblica e dall'integrazione tra apparato scientifico, industria e obiettivi strategici dello Stato.

La Cina può inoltre contare su una platea molto estesa di grandi gruppi industriali e grandi imprese tecnologiche nazionali interessati all'uso delle tecnologie quantistiche. Questo è un aspetto importante perché mostra come il *quantum*, in Cina, non sia confinato alla sola dimensione accademica o sperimentale, ma venga considerato un ambito di interesse anche per attori industriali già consolidati. Al tempo stesso, però, il quadro disponibile resta più sintetico rispetto a quello di Stati Uniti ed Europa: emerge con chiarezza la presenza di una base industriale ampia e di ecosistemi urbani specializzati, mentre risultano meno dettagliati i singoli progetti aziendali o i nomi delle imprese rispetto ai casi occidentali. Questa minore trasparenza rende più difficile valutare con precisione il grado di maturità commerciale dell'ecosistema, ma non ne riduce la rilevanza strategica.

Nel panorama globale delle tecnologie quantistiche, la Cina si distingue dunque soprattutto per scala degli investimenti pubblici, capacità di pianificazione strategica e intensità della produzione scientifica e brevettuale. Il suo vantaggio non risiede tanto in un modello di mercato aperto o in una particolare visibilità internazionale delle singole *startup*, quanto nella capacità di mobilitare risorse, orientare la ricerca e costruire infrastrutture e poli territoriali coerenti con una strategia nazionale di lungo periodo. Rispetto agli Stati Uniti, che appaiono più forti nella mobilitazione del capitale privato e nella messa a mercato delle tecnologie, e rispetto all'Europa, che mostra una forte base scientifica ma una maggiore frammentazione industriale, la Cina presenta un modello più integrato tra politica industriale, sicurezza nazionale e costruzione di autonomia tecnologica. Proprio la combinazione di investimenti pubblici, centralizzazione decisionale, accumulazione di brevetti e costruzione di *cluster* urbani rende oggi la Cina uno degli attori centrali della competizione quantistica internazionale.

2.3-II panorama in Europa ed in Italia

L'Europa si è affermata come uno dei principali poli globali delle tecnologie quantistiche per intensità del sostegno pubblico e qualità della base scientifica. Il suo

posizionamento deriva da una costruzione multilivello, nella quale le strategie dell'Unione si intrecciano con le politiche dei singoli Stati membri, dando forma a un ecosistema articolato che combina ricerca, infrastrutture e primi percorsi di industrializzazione. Tra le iniziative più rilevanti si colloca la *Quantum Flagship*, che con un investimento superiore a 1 miliardo di euro ha rappresentato uno dei principali strumenti di consolidamento del settore, sostenendo ricerca, innovazione e sviluppo industriale lungo l'intera catena del valore. A essa si affiancano programmi infrastrutturali come il *European High Performance Computing Joint Undertaking* (EuroHPC JU), orientato all'integrazione tra *supercomputing* e *quantum computing*, ed *European Quantum Communication Infrastructure* (EuroQCI)¹¹, finalizzato alla realizzazione entro il 2027 di una rete europea di comunicazione quantistica sicura.

Su questa base, la strategia europea più recente ha ulteriormente rafforzato il riconoscimento del *quantum* come tecnologia critica per la competitività, la sicurezza e la sovranità dell'Unione. L'obiettivo non è più soltanto preservare l'eccellenza scientifica europea, ma favorire il passaggio dal laboratorio alla fabbrica, dall'invenzione all'adozione, agendo contemporaneamente sul rafforzamento della ricerca, sullo sviluppo di infrastrutture quantistiche, sul consolidamento dell'ecosistema industriale, sull'integrazione con le strategie di spazio, sicurezza e difesa e sulla formazione di competenze specialistiche. In questo senso, il *quantum* si sta progressivamente configurando come uno dei terreni in cui l'Europa cerca di tradurre il proprio patrimonio scientifico in autonomia tecnologica e capacità industriale.

Nonostante questi progressi, il quadro europeo resta segnato da una criticità strutturale. L'ecosistema è dinamico e in espansione – a settembre 2025 si contano oltre 100 *startup* quantistiche attive nel continente, concentrate soprattutto in Germania, Francia, Paesi Bassi, Finlandia, Italia e Spagna – ma continua a mostrare fragilità nella raccolta di capitale privato e nella crescita d'impresa. Tra il 2015 e il 2023, infatti, l'Europa ha attratto circa il 16% del *venture capital* globale, pari a circa un sesto di quelli degli Stati Uniti. Ne emerge un sistema forte nella ricerca, nelle partnership pubblico-private e nella costruzione di programmi istituzionali, ma ancora meno efficace nella fase di *scale-up*, nel consolidamento industriale e nella creazione di campioni globali. In altri termini, l'Europa dispone di ottimi presupposti scientifici e tecnologici, ma deve

¹¹ <https://digital-strategy.ec.europa.eu/it/policies/european-quantum-communication-infrastructure-euroqci>

ancora rafforzare i meccanismi che consentono di trasformare tale patrimonio in imprese di grande scala e in un più solido presidio della *value chain*.

All'interno di questo quadro, alcuni Paesi stanno assumendo un ruolo particolarmente rilevante. La Germania rappresenta oggi il sistema più solido in termini di dimensioni e capacità industriale, grazie a un tessuto scientifico avanzato, a consistenti investimenti pubblici e a una struttura industriale capace di accompagnare lo sviluppo delle tecnologie emergenti.

La Francia, invece, si distingue per una strategia nazionale chiara e per una geografia dell'innovazione già fortemente specializzata: l'area di Parigi e dell'Île-de-France concentra università, centri di ricerca e attività focalizzate su fotonica, macchine e chip quantistici; Grenoble è specializzata nella *quantum communication* e nei circuiti quantistici; Tolosa, anche attraverso l'Aerospace Valley, sviluppa competenze nel *quantum sensing*, con particolare attenzione a gravimetri e orologi atomici per applicazioni aeronautiche e aerospaziali. In questo ecosistema si collocano anche *startup* di primo piano come Pasqal e Alice & Bob, tra gli attori più visibili del panorama europeo.

Uno degli ambiti in cui questa traiettoria appare più avanzata è quello della *quantum communication*, in particolare per quanto riguarda la QKD e più in generale le applicazioni per la sicurezza delle comunicazioni. Si tratta di un orientamento coerente con la crescente centralità della protezione dei dati, delle infrastrutture critiche e delle comunicazioni governative, finanziarie e industriali. In questo campo l'Europa sta costruendo sia una rete infrastrutturale comune sia un ecosistema di imprese specializzate. EuroQCI, come anticipato, punta a realizzare una rete in fibra ottica con componente spaziale integrata, mentre *Open Quantum Key Distribution (OpenQKD)*¹² favorisce la sperimentazione sul campo attraverso siti di test aperti e collaborazioni tra università, industria e *startup* in più Paesi europei, inclusa l'Italia. Accanto a queste iniziative si collocano imprese emblematiche come la svizzera ID Quantique, pioniera nella commercializzazione di soluzioni QKD, QRNG e SPD per telecomunicazioni, *cloud*, settore bancario e comunicazioni governative. La sua acquisizione da parte di IonQ nel 2025, pur con mantenimento dell'autonomia operativa, riflette bene la rilevanza strategica assunta da questi asset nel quadro competitivo internazionale.

¹² <https://cordis.europa.eu/project/id/857156>

È in questo contesto che si colloca il caso italiano. Pur non occupando ancora una posizione di *leadership* dimensionale paragonabile a quella di Germania o Francia, l'Italia sta rafforzando il proprio posizionamento attraverso la progressiva costruzione di una filiera quantistica nazionale capace di integrare ricerca scientifica, sviluppo tecnologico, infrastrutture e applicazioni industriali. Più che su una singola eccellenza isolata, l'evoluzione italiana si fonda sull'emersione di un ecosistema distribuito che mette in connessione università, centri di ricerca, infrastrutture di *high-performance computing* e *startup deep tech*. A guidare questa traiettoria sono soprattutto due iniziative. La prima è l'Istituto Nazionale per le Scienze e le Tecnologie Quantistiche (*National Quantum Science and Technology Institute*, NQSTI), consorzio nazionale istituito nel 2022 e composto da 20 enti tra università e centri di ricerca pubblici distribuiti sul territorio. La seconda è il Centro Nazionale *High Performance Computing, Big Data e Quantum Computing* (ICSC)¹³, che ospita uno spoke interamente dedicato al *quantum* e svolge un ruolo importante nel trasferimento tecnologico e nella gestione di infrastrutture computazionali ibride classico-quantistiche.

Il progetto NQSTI, finanziato dal PNRR con una dotazione complessiva di 115,9 milioni di euro, è particolarmente rilevante perché copre l'intera catena dell'innovazione: rafforzamento della ricerca di base, sperimentazione applicata, sostegno alla nascita di *startup* e *spin-off*, valorizzazione territoriale e sviluppo di applicazioni concrete tanto nel *quantum computing* quanto nella comunicazione quantistica sicura. Questa impostazione riflette bene l'approccio italiano, che tende a svilupparsi non solo attraverso singoli progetti di ricerca, ma anche tramite la costruzione progressiva di un'infrastruttura nazionale capace di connettere competenze, piattaforme sperimentali e domanda applicativa.

Questa traiettoria è stata accompagnata da una più esplicita assunzione di iniziativa da parte del Governo italiano, che ha progressivamente collocato le tecnologie quantistiche tra le leve della politica industriale, della sicurezza nazionale e della sovranità tecnologica. Il passaggio più rilevante in questa direzione è stato la presentazione in Consiglio dei ministri, il 5 settembre 2025, della *Strategia Italiana per le Tecnologie Quantistiche*, promossa dal Sottosegretario alla Presidenza del Consiglio con delega all'innovazione tecnologica Alessio Butti insieme ai ministeri competenti. La Strategia individua quattro direttrici principali – rafforzamento della

¹³ <https://www.supercomputing-icsc.it>

ricerca e delle infrastrutture, accelerazione della transizione industriale, sviluppo di nuove competenze e tutela della sicurezza nazionale anche attraverso la migrazione verso crittografie *post-quantum* – e mira a trasformare il vantaggio scientifico accumulato dal Paese in capacità tecnologica, applicativa e produttiva. Nella versione pubblicata dal MIMIT, il documento dettaglia infatti azioni per potenziare ricerca e innovazione, migliorare l'accesso alle infrastrutture, stimolare gli investimenti privati e rafforzare le reti di collaborazione tra soggetti pubblici e privati. A questa cornice strategica si sono aggiunti, nel corso del 2025, momenti di raccordo istituzionale e di consolidamento della filiera, come gli Stati Generali del Quantum¹⁴ del dicembre 2025, presentati dal Governo come sede di confronto operativo tra istituzioni, università, imprese e pubblica amministrazione, e orientati anche alla costruzione di un polo nazionale di ricerca. Nel complesso, l'azione governativa appare quindi orientata a dare continuità e riconoscibilità strategica a una filiera che fino a pochi anni fa si presentava soprattutto come somma di iniziative scientifiche e progettuali, e che oggi viene invece sempre più letta come infrastruttura critica per la competitività industriale, la resilienza digitale e il posizionamento internazionale del Paese.

Proprio la dimensione infrastrutturale rappresenta uno degli elementi più significativi della traiettoria italiana. Il CINECA, già nodo strategico del *supercomputing* nazionale ed europeo, sta assumendo un ruolo di primo piano anche nello sviluppo del *quantum computing*, con un approccio esplicitamente orientato all'integrazione tra sistemi classici e quantistici. In particolare, CINECA collabora con la finlandese IQM per l'installazione di un sistema quantistico da 54 *qubit*, previsto all'inizio del 2026, da integrare con il *supercomputer* Leonardo presso la sede di Bologna¹⁵. Parallelamente, la francese Pasqal fornirà il sistema EuroQCS-Italy, un computer quantistico analogico da 140 *qubit*, progettato per essere aggiornabile nel tempo e pienamente operativo entro il 2027, anch'esso integrato con Leonardo nell'ambito di EuroHPC e cofinanziato dal Ministero dell'Università e della Ricerca (MUR)¹⁶. Il significato di queste iniziative va oltre il dato tecnologico puntuale: l'integrazione tra *supercomputing* e *quantum computing* prefigura infatti modelli ibridi di *high-performance computing* e *quantum* (HPC-quantum) destinati a diventare una componente strutturale delle future

¹⁴ <https://www.mimit.gov.it/it/eventi/stati-general-quantum-attuazione-della-strategia-nazionale-per-le-tecnologie-quantistiche>

¹⁵ https://www.lastampa.it/economia/2025/03/17/news/cineca_bologna_computer_quantistico_iqm-15056081/

¹⁶ <https://www.supercomputing-icsc.it/2025/03/27/euroqcs-italy-firmato-lacquistato-del-nuovo-calcolatore-quantistico-italiano-dellinfrastruttura-europea/>

infrastrutture computazionali per ricerca, industria e pubblica amministrazione. In questa prospettiva, CINECA non agisce soltanto come centro di calcolo, ma come piattaforma nazionale di attrazione per competenze, progetti e sperimentazioni applicative.

Accanto a Bologna stanno emergendo altri poli territoriali rilevanti. Torino occupa una posizione centrale soprattutto nella metrologia e nella comunicazione quantistica, grazie al ruolo dell'Istituto Nazionale di Ricerca Metrologica (INRiM) e al coordinamento del progetto *Quantum Italy Deployment* (QUID). Napoli rappresenta un altro polo in crescita, trainato dalle attività della Federico II e dalle sperimentazioni su *hardware* quantistico superconduttivo. Presso l'Università Federico II è stato assemblato già nel 2023 un primo prototipo di elaboratore per attività di ricerca, mentre nel 2024 è stato inaugurato Partenope, descritto come il primo computer quantistico italiano a tecnologia superconduttiva aperto al pubblico per attività di ricerca e anche per utilizzo da parte di soggetti privati. Dotato di un processore a 24 *qubit*, e recentemente potenziato tramite l'installazione di un nuovo processore a 64 *qubit*¹⁷, il sistema costituisce un passaggio importante per la crescita del *quantum computing* sperimentale in Italia. Nel complesso, il quadro che emerge è quello di un ecosistema nazionale ancora in consolidamento, ma sempre più capace di articolarsi in poli complementari, ciascuno con una propria specializzazione funzionale.

Se nel *quantum computing* l'Italia sta costruendo progressivamente capacità infrastrutturali, nella comunicazione quantistica il suo posizionamento appare già più definito. Il progetto QUID, coordinato dall'INRiM di Torino, costituisce la declinazione italiana di EuroQCI e punta allo sviluppo di nodi metropolitani di comunicazione quantistica collegati tramite l'*Italian Quantum Backbone*¹⁸, infrastruttura basata su fibre ottiche commerciali e concepita per distribuire segnali di tempo e frequenza campione su scala nazionale. Un obiettivo strategico del progetto è inoltre il collegamento tra rete terrestre in fibra e segmento spaziale europeo, rafforzando l'integrazione dell'Italia nella futura architettura continentale della comunicazione quantistica sicura. Anche su questo fronte, dunque, il caso italiano appare coerente con le priorità europee, ma al tempo stesso caratterizzato da una specializzazione nazionale ben riconoscibile.

¹⁷ <https://www.unina.it/it/w/con-il-nuovo-processore-a-64-qubit-del-computer-della-federico-ii-partenope-?redirect=%2Fit%2Fpersonale-home>

¹⁸ <https://www.ilnuovosaggiatore.sif.it/article/200>

Questa specializzazione trova riscontro anche nel tessuto imprenditoriale, ancora contenuto nelle dimensioni ma coerente con alcuni punti di forza nazionali. Tra le realtà più significative emerge Quantum Telecommunications Italy (QTI), *spin-off* del Consiglio Nazionale delle Ricerche, Istituto Nazionale di Ottica (CNR-INO), nato nel 2020 e attivo nella progettazione di soluzioni QKD. L'azienda si è distinta per aver realizzato nel 2021, durante il G20 Scienza di Trieste, una comunicazione quantistica sicura intergovernativa tra Italia, Slovenia e Croazia¹⁹; la sua traiettoria industriale si è poi rafforzata con l'ingresso di Telsy nel 2021 e con una *proof of concept* sviluppata nel 2024 insieme a Sparkle per la trasmissione ad alta velocità di dati protetti da QKD su una rete esistente tra due *data center* ad Atene²⁰. Accanto a QTI si colloca ThinkQuantum, *spin-off* dell'Università di Padova specializzato in dispositivi *Discrete Variable Quantum Key Distribution* (DV-QKD) e in moduli *Quantum Random Number Generator* (QRNG) per la generazione di numeri realmente casuali, con una forte enfasi sull'integrazione nelle reti in fibra ottica metropolitane e regionali e su una *value chain* europea. Un'altra realtà interessante è levelQuantum, che ha sviluppato una soluzione proprietaria di QKD evoluta, progettata per rafforzare la sicurezza delle informazioni anche in scenari in cui singole componenti *hardware* possano essere compromesse, e adattabile sia a reti in fibra sia ad architetture *free-space* o satellitari.

Su questo stesso versante della sicurezza quantistica si colloca in modo particolarmente rilevante Telsy, che occupa una posizione centrale nel punto di intersezione tra *quantum communication*, *cybersecurity* e integrazione industriale delle soluzioni di sicurezza nelle infrastrutture di rete esistenti. Società del Gruppo TIM e centro di competenza del gruppo per la sicurezza delle comunicazioni, Telsy ha consolidato il proprio posizionamento nel *quantum* attraverso un duplice percorso: da un lato, il rafforzamento della filiera nazionale della QKD tramite l'ingresso nel capitale di QTI nel 2021 e il successivo passaggio al controllo dell'80% nel 2024²¹; dall'altro, lo sviluppo di un presidio più ampio sulla sicurezza *quantum-safe*, che affianca alle soluzioni QKD anche attività su *Post-Quantum Cryptography* (PQC) e *secure hardware*. Il profilo distintivo di Telsy risiede soprattutto nella capacità di trasformare la sicurezza quantistica da ambito sperimentale a soluzione integrabile in contesti operativi reali. In questa direzione si collocano sia Quell-X, sistema QKD sviluppato nell'orbita Telsy-QTI per la generazione e distribuzione di chiavi quantistiche tramite

¹⁹ <https://www.qticompany.com/quantum-network/>

²⁰ <https://www.gruppotim.it/it/archivio-stampa/sparkle/2024/CS-QKD-PoC-Grecia.html>

²¹ <https://www.gruppotim.it/en/press-archive/corporate/2025/PR-BOD-1Q-12-02-2025.html>

fotoni tra nodi fidati, sia la collaborazione con Fortinet, annunciata nel 2025²², per integrare Quell-X con i *Next-Generation Firewalls* FortiGate e realizzare *virtual private network* (VPN) *quantum-safe* basate su chiavi distribuite via QKD secondo interfacce standard ETSI. Lo stesso orientamento all'integrazione emerge anche nelle sperimentazioni su reti esistenti: nel 2024 Telsy, insieme a QTI e all'operatore portoghese MEO²³, ha implementato nell'area metropolitana di Lisbona un collegamento protetto con QKD su una rete combinata terrestre e sottomarina, dimostrando la possibilità di estendere la sicurezza quantistica a infrastrutture di telecomunicazione già operative. A rafforzare ulteriormente questo posizionamento contribuiscono il lavoro sui *Trusted Node* sviluppato con l'INRiM, per estendere la portata della crittografia quantistica oltre le distanze tipiche delle tratte in fibra, e il progetto Telsy Secure Microchip, nato per realizzare un microcontrollore italiano per applicazioni di sicurezza e poi evoluto verso una micro-piattaforma programmabile *secure-by-design* basata su algoritmi PQC. Nel complesso, Telsy si distingue quindi non solo come utilizzatore di tecnologie quantistiche, ma come attore di industrializzazione capace di connettere ricerca, *telecommunications*, crittografia avanzata e domanda di sicurezza in settori civili, industriali e istituzionali.

Un ruolo differente ma altrettanto significativo è assunto da Al maviva, che presidia soprattutto il versante dell'integrazione sistemica del *quantum* nelle comunicazioni sicure, nella *cybersecurity* avanzata e nelle infrastrutture critiche, con una particolare attenzione al dominio della difesa. Questo posizionamento si è reso particolarmente visibile con *Quantum Agile and Resilient Military Communications* (Q-ARM), progetto coordinato da Al maviva e selezionato nell'*European Defence Fund 2024* tra le iniziative europee dedicate alle tecnologie quantistiche dirompenti. Q-ARM, che ha una durata di 36 mesi e un budget di circa 5 milioni di euro, punta a sviluppare un sistema di comunicazione *crypto-agile*, *quantum-secure* e di gestione decentralizzata dell'identità per contesti di difesa e infrastrutture critiche, combinando PQC, QKD, *blockchain* per l'identità digitale decentralizzata e infrastrutture ibride in fibra e satellite. Il progetto include inoltre la realizzazione di un simulatore *end-to-end* per modellare la comunicazione quantistica tra satellite e stazione di terra e stimarne le prestazioni. Più che sviluppare una singola piattaforma quantistica, Al maviva opera quindi come integratore e coordinatore industriale, capace di mettere insieme

²² <https://www.gruppotim.it/en/press-archive/corporate/2025/PR-Telsy-Fortinet-19-November-2025.html>

²³ https://www.gruppotim.it/it/archivio-stampa/mercato/2024/CS_Telsy_QTI_e_MEO_QKD_Lisbona.html

componenti crittografiche, reti di telecomunicazione, simulazione, identità digitale e requisiti di interoperabilità, trasferendo verso il *quantum* competenze già maturate in intelligenza artificiale, *cloud*, *data analytics* e *cybersecurity* verso casi d'uso ad alta criticità istituzionale. Anche la composizione del consorzio Q-ARM conferma questa vocazione: Al maviva guida, infatti, una rete di 10 partner di 7 Paesi europei, che include università, centri di ricerca, piccole e medie imprese e aziende specializzate, con l'obiettivo di costruire una soluzione compatibile con le future architetture digitali della difesa europea. In questo senso, il contributo di Al maviva alla filiera italiana riguarda soprattutto la traduzione delle tecnologie quantistiche in architetture applicative per comunicazioni sicure e resilienti, rafforzando il posizionamento nazionale nei temi della sovranità tecnologica europea.

Su un piano ancora diverso si colloca Rotonium, che rappresenta un caso peculiare perché presidia una traiettoria tecnologica distinta da quella dei grandi sistemi criogenici. L'azienda, fondata nel 2022 in Friuli-Venezia Giulia e incubata a Padova, sviluppa infatti processori quantistici fotonici pensati per essere compatti, a basso consumo e operativi a temperatura ambiente, con un orientamento esplicito verso applicazioni *edge* e contesti operativi mobili o spaziali. Il nucleo della sua proposta è l'impiego dell'*Orbital Angular Momentum* (OAM), dei fotoni per costruire architetture fotoniche più scalabili e sostenibili, capaci di ridurre complessità circuitale, dimensioni e requisiti energetici rispetto ad altre soluzioni quantistiche. In questa prospettiva, Rotonium non punta tanto a replicare i modelli dominanti del *quantum computing*, quanto a proporre acceleratori quantistici modulari e integrabili in ambienti dove peso, ingombro, consumo e robustezza costituiscono vincoli decisivi, come satelliti, piattaforme aerospaziali e sistemi distribuiti. Anche il percorso industriale dell'azienda va in questa direzione: nel 2024 ha raccolto un investimento *seed* da 1 milione di euro²⁴ per accelerare la ricerca industriale sul proprio processore quantistico fotonico e sviluppare ulteriormente i componenti necessari alla verifica dell'architettura. Nello stesso percorso rientrano sia la roadmap presentata sull'uso di *qudit* fotonici basati su OAM e processi semiconduttori standard, sia l'annuncio del primo processore RP000, descritto come un dispositivo fotonico a 4 qubit operante a temperatura ambiente. Il ruolo di Rotonium nel panorama italiano appare dunque significativo perché contribuisce a diversificare la filiera nazionale oltre il binomio tradizionale tra calcolo

²⁴ <https://www.rotonium.com/post/revolutionizing-quantum-computing-rotonium-s-light-based-technology>

criogenico e comunicazione quantistica, aprendo una traiettoria verso soluzioni fotoniche leggere, modulari e a basso assorbimento energetico.

Infine, IonQ Italia assume rilievo non solo per il profilo internazionale della casa madre, ma anche perché il suo insediamento si colloca in una fase di rafforzamento della proiezione italiana nel settore, nella quale il Paese sta cercando di tradurre la propria base scientifica in una più stabile capacità industriale, applicativa e infrastrutturale. Nel novembre 2025 IonQ ha nominato Marco Pistoia *Chief Executive Officer* della controllata italiana, affidandogli il compito di ampliare l'accesso ai sistemi quantistici dell'azienda per imprese, istituzioni di ricerca e partner pubblici italiani. Secondo l'impostazione data alla nuova sede, IonQ Italia lavorerà su applicazioni in settori come finanza, energia, aerospazio, difesa, farmaceutica e manifattura avanzata, e porterà in Italia non solo *quantum computing*, ma anche *quantum networking*, *quantum security* e *quantum sensing*. Lo stesso Pistoia continuerà inoltre a guidare a livello globale il gruppo *Special Projects* di IonQ, attivo su sistemi finanziari quantistici, comunicazioni *quantum-safe* e integrazione tra QKD, crittografia *post-quantum* e nuove tecnologie satellitari e di rete. Il profilo concreto dell'iniziativa italiana emerge dal fatto che Roma è stata concepita non come semplice presidio commerciale, ma come vero *hub* tecnologico europeo della società. In interviste successive all'annuncio, Pistoia ha descritto IonQ Italia come una controllata destinata a sviluppare *hardware*, algoritmi, applicazioni, *quantum networking*, crittografia *quantum-safe* e *quantum sensing*, con un piano iniziale di almeno 100²⁵ assunzioni tra ricercatori, ingegneri e sviluppatori. La scelta di Roma è stata presentata come strategica anche per la volontà di fare dell'Italia la base europea e mediterranea delle future attività del gruppo, con una forte enfasi sul rientro dei talenti italiani e sulla costruzione di una filiera industriale nazionale capace non solo di usare, ma anche di progettare e sviluppare tecnologie quantistiche. A rafforzare ulteriormente questo posizionamento contribuisce la partecipazione di IonQ a Q-Alliance²⁶, iniziativa annunciata nell'ottobre 2025 in Lombardia e presentata come parte della strategia italiana per le tecnologie digitali e quantistiche. In questo progetto IonQ figura tra i fondatori dell'*hub* quantistico insieme a D-Wave, con l'obiettivo di creare in Italia un

²⁵ https://www.repubblica.it/tecnologia/2025/11/22/news/il_colosso_del_quantum_computing_ionq_aprira_una_sede_a_roma_1_ad_pistoia_subito_100_assunzioni-424996299/#:~:text=L'Ad%20Pistoia%3A%20%22Subito%20100%20assunzioni%20di%20Arcangelo%20Rociola&text=IonQ%20sbarca%20in%20Italia%20e,primo%20livello%20in%20questa%20tecnologia.

²⁶ <https://nqsti.it/news/q-alliance-nqsti-pronto-fare-la-propria-parte>

centro di eccellenza aperto a ricerca, industria e formazione, capace di sostenere borse di studio, tirocini e programmi di sviluppo delle competenze. In questo senso, il ruolo di IonQ Italia non si limita alla fornitura di capacità computazionale, ma riguarda la costruzione di un presidio industriale e scientifico stabile, collegato sia alla strategia nazionale sia a una più ampia ambizione di posizionare l'Italia come nodo europeo del cosiddetto “Rinascimento quantistico”.

Nel complesso, il panorama europeo delle tecnologie quantistiche appare oggi ben posizionato sul versante della ricerca, del coordinamento istituzionale e delle infrastrutture, ma continua a misurarsi con una sfida decisiva: trasformare il vantaggio scientifico in capacità industriale, valorizzazione economica e controllo della catena del valore. In questo contesto, l'Italia mostra come anche un ecosistema di scala intermedia possa ritagliarsi un ruolo strategico, non tanto attraverso la presenza di un singolo campione nazionale, quanto mediante la progressiva emersione di una filiera articolata in cui convergono programmi pubblici, centri di eccellenza, infrastrutture di ricerca, collaborazioni europee, *startup* ad alta specializzazione e attori industriali capaci di presidiare segmenti diversi ma complementari, dalla comunicazione sicura all'integrazione infrastrutturale, fino allo sviluppo di nuove piattaforme applicative e fotoniche. Proprio la capacità di specializzarsi in segmenti ad alta intensità di conoscenza – come *quantum communication*, metrologia, fotonica e integrazione *HPC-quantum* – e di inserirsi coerentemente nelle architetture europee di lungo periodo costituisce oggi il principale punto di forza della traiettoria italiana.

Conclusioni

La rassegna proposta consente di tornare, in chiusura, alla tensione da cui ha preso le mosse: la distanza tra ciò che la scienza quantistica già consente e ciò che i sistemi industriali e istituzionali riescono effettivamente ad assorbire. I tre piani di analisi attraversati nel contributo possono essere rilette, in fondo, come tre diverse risposte a questo medesimo problema.

Sul piano tecnologico, tale distanza non è uniforme, ma si distribuisce in modo diseguale lungo le tre traiettorie: massima nel calcolo quantistico, dove il divario tra dimostrazione di laboratorio e utilità economica resta ampio; più contenuta nella comunicazione quantistica, la cui prossimità al mercato dipende però dalla capacità di innestarsi su reti e standard preesistenti; quasi colmata nel *sensing*, dove il vincolo si è ormai spostato dalla prestazione fisica all'industrializzazione su scala. Ne deriva che

parlare di "maturità quantistica" in termini unitari risulta fuorviante: ciascuna traiettoria si trova in un punto diverso del proprio percorso di traduzione industriale.

Sul piano geopolitico, appaiono altrettante strategie per ridurre quella stessa distanza, ciascuna con un punto di leva differente: il capitale privato e le piattaforme *cloud* negli Stati Uniti, la pianificazione centralizzata e la mobilitazione di risorse pubbliche in Cina, il coordinamento istituzionale e infrastrutturale in Europa. Non si tratta quindi di modelli più o meno avanzati lungo un'unica scala, ma di architetture che presidiano in modo diverso il passaggio dalla ricerca alla capacità industriale, ed è proprio su quel passaggio che si gioca il rispettivo vantaggio competitivo di lungo periodo.

È su questo sfondo che il caso italiano acquista il proprio significato più preciso. Più che per la dimensione assoluta del proprio sistema, l'Italia rileva per il modo in cui sta affrontando il nodo della traduzione industriale: non attraverso la scommessa su un'unica tecnologia o su un singolo campione, ma costruendo le condizioni – infrastrutturali, imprenditoriali e di *governance* – che rendono quella traduzione possibile. È un percorso ancora aperto, il cui esito dipenderà meno dalla qualità della ricerca, che resta un punto di forza ormai acquisito, e più dalla continuità delle politiche pubbliche, dalla disponibilità di capitale paziente e dalla capacità di trattenere competenze. In questo senso, la traiettoria quantistica italiana si configura oggi soprattutto come una scommessa sulle proprie condizioni abilitanti, prima ancora che sui singoli risultati.

Appendice: tabella riassuntiva delle sigle utilizzate

<i>Sigla</i>	<i>Definizione</i>
BB84	Bennett-Brassard 1984 (protocollo di Quantum Key Distribution)
DV-QKD	Discrete Variable Quantum Key Distribution
GNSS	Global Navigation Satellite System
HPC	High-Performance Computing
OAM	Orbital Angular Momentum
PQC	Post-Quantum Cryptography
PRNG	Pseudo Random Number Generator
QCaaS	Quantum Computing as a Service
QKD	Quantum Key Distribution
QPU	Quantum Processing Unit
QRNG	Quantum Random Number Generator
SPD	Single-Photon Detector
UCP	Unit Commitment Problem
VPN	Virtual Private Network

Bibliografia

- Central Committee of the Communist Party of China, *The Outline of the 14th Five-Year Plan for Economic and Social Development and Long-Range Objectives Through the Year 2035 of the People's Republic of China*, Pechino, 2021.
- Commissione europea, *Communication from the Commission to the European Parliament and the Council – Quantum Europe Strategy: Quantum Europe in a Changing World*, COM(2025) 363 final, Bruxelles, 2 luglio 2025.
- Commissione europea, *The future is quantum: EU countries plan ultra-secure communication network*, comunicato stampa, Digital Assembly, Bucarest, 13 giugno 2019.
- Consiglio dell'Unione europea, *Regolamento (UE) 2021/1173 del Consiglio del 13 luglio 2021 relativo all'istituzione dell'impresa comune per il calcolo ad alte prestazioni europeo e che abroga il regolamento (UE) 2018/1488*, in *Gazzetta Ufficiale dell'Unione Europea*, L 256, 19 luglio 2021, pp. 3–51.
- ENISA – European Union Agency for Cybersecurity, *Post-Quantum Cryptography – Integration Study*, ENISA Publications, ottobre 2022, ISBN 978-92-9204-590-6, DOI 10.2824/151162.
- ENISA – European Union Agency for Cybersecurity, *Post-Quantum Cryptography: Current State and Quantum Mitigation*, ENISA Publications, maggio 2021, ISBN 978-92-9204-468-8, DOI 10.2824/92307.
- ETSI – European Telecommunications Standards Institute, ISG QKD, *Quantum Key Distribution (QKD); Protocol and Data Format of REST-based Key Delivery API*, ETSI GS QKD 014 V1.1.1, Sophia Antipolis, febbraio 2019.
- European Quantum Flagship – Strategic Advisory Board, *Strategic Research and Industry Agenda 2030: Roadmap and Quantum Ambitions over this Decade (SRIA 2030)*, Bruxelles, 14 febbraio 2024.
- Ministero dell'Università e della Ricerca, Ministero delle Imprese e del Made in Italy, Comitato Interministeriale per la Transizione Digitale, *Strategia Italiana per le Tecnologie Quantistiche*, Roma, 5 settembre 2025.
- National Institute of Standards and Technology (NIST), *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, Federal Information Processing Standards Publication FIPS 203, U.S. Department of Commerce, Gaithersburg (MD), 13 agosto 2024, DOI 10.6028/NIST.FIPS.203.

- National Quantum Coordination Office, Executive Office of the President of the United States, *National Quantum Initiative: Fact Sheet*, Washington (DC), aprile 2022.
- NQSTI – Istituto Nazionale di Scienze e Tecnologie Quantistiche, *Quantum for Italy*, a cura di G. R. Greco, Edizioni Saletta dell'Uva, Caserta, 202