

*Quantum Computing e Sicurezza:
una (complessa) opportunità.*



Pensare fuori dagli schemi. Come ogni buona teoria che si rispetti, il punto di partenza è sempre un limite da superare.

"La natura non è classica, diamine, e se vuoi fare una simulazione della natura, faresti meglio a renderla quantistica"

Questa frase fu pronunciata da Richard Feynman durante una conferenza intitolata "The Physics of Computation" tenutasi al Massachusetts Institute of Technology (1981), e pose le basi dell'informatica quantistica, suggerendo l'idea che le simulazioni di sistemi quantistici richiedessero calcolatori basati sui principi della meccanica quantistica stessa.

Realizzare questa visione è una delle grandi sfide che scienza e tecnologia devono affrontare.

Affermare che la natura non sia affatto classica, significa allontanarsi un po' dal concetto che la prevedibilità del macroscopico a cui siamo abituati sia un porto sicuro ed accogliere le leggi, spesso controintuitive, che regolano il microscopico.

Com'è noto, l'informatica classica e quella quantistica differiscono fundamentalmente nell'unità di base dell'informazione e nei principi fisici su cui si fondano i loro calcoli: la tecnologia classica che oggi utilizziamo gestisce l'informazione attraverso il bit (che può avere solo i due stati 0 o 1 mutuamente esclusivi), esegue le operazioni in modo sequenziale ed ogni calcolo segue un percorso logico ben definito.

L'informatica quantistica, d'altro canto, processa le informazioni in modo completamente diverso, utilizzando il qbit e grazie ai principi di sovrapposizione ed entanglement, può esistere contemporaneamente in uno stato che è una combinazione di 0 e 1, essendo così in grado di esplorare molteplici soluzioni simultaneamente ad una velocità che oggi definiremmo surreale.

Si può ben immaginare come il calcolo quantistico possa dunque essere rivoluzionario in tutti gli ambiti in cui ci sia necessario processare una grande mole di dati, come ad esempio nell'implementazione delle analisi finanziarie, della ricerca scientifica a tutto tondo e dell'intelligenza artificiale. A tal proposito ricordiamo che la IA è affamata di dati, per imparare, migliorare, prendere decisioni, ha bisogno di elaborare enormi quantità di informazioni. Questo processo richiede tempo e potenza di calcolo, più un algoritmo è sofisticato, più è difficile addestrarlo, testarlo, perfezionarlo. E qui entra in gioco il quantum computing.

Tuttavia, non sono trascurabili le minacce a cui siamo potenzialmente esposti nel campo della sicurezza informatica e delle comunicazioni: un computer quantistico sarebbe in grado scardinare gli attuali protocolli crittografici nel giro di qualche ora, con impatti devastanti sulla riservatezza, l'integrità e la disponibilità delle informazioni: i gruppi criminali potrebbero intercettare e registrare oggi dati sensibili criptati per decifrarli in un secondo momento, quando la tecnologia quantistica sarà matura (i cosiddetti attacchi "Harvest Now, Decrypt Later")

Sebbene i computer quantistici non siano ancora disponibili sul mercato, per mitigare i rischi relativi alle vulnerabilità degli algoritmi e salvaguardare l'integrità delle infrastrutture digitali (per come le intendiamo oggi), la comunità scientifica sta guidando lo sviluppo di nuove soluzioni di sicurezza

“quantum-safe” come, ad esempio, la crittografia post-quantistica (PQC) e la Quantum Key Distribution (QKD).

Non è difficile, pertanto, comprendere la corsa allo sviluppo di tecnologie legate al quantum computing, rappresenti oggi una delle maggiori aree di investimento da parte delle grandi Big Tech che, disponendo di ingenti capitali e collaborando con centri di ricerca specializzati, hanno la possibilità di tracciare la rotta di questo sviluppo.

Ad oggi, gli aspetti più sfidanti sono relativi all'hardware necessario per supportare la tecnologia quantistica: i qbit sono estremamente fragili e altamente sensibili alle più piccole vibrazioni o variazioni di temperatura che, a questi ordini di grandezza, causerebbero la perdita della preziosa sovrapposizione, rendendo vana la capacità di calcolo simultaneo tanto ambito. La soluzione risiede nel garantire a tali macchine una temperatura estremamente bassa, con condizioni di esercizio prossime allo zero assoluto e con immaginabili costi di realizzazione importanti.

Nonostante i numerosi ostacoli tecnologici e con tutte le incertezze del caso, gli investimenti nel quantum computing stanno crescendo esponenzialmente e i dati ufficiali indicano un valore di circa 17,7 miliardi nel 2024 (a livello mondiale) con previsioni di crescita degli investimenti nel 20% nel 2025.

Anche l'Italia si sta muovendo in tale direzione e, per dare concretezza agli obiettivi strategici assunti a livello internazionale con la firma della European Declaration on Quantum Technologies nel 2023, ha comunicato nel mese di luglio, l'adozione di una Strategia Italiana per le Tecnologie Quantistiche.

È interessante notare che uno dei primi aspetti sottolineati in tale documento è il riconoscimento delle tecnologie quantistiche come leva strategica per la competitività, la sovranità tecnologica e la sicurezza nazionale, mettendo a sistema le risorse disponibili per valorizzare i risultati emersi e continuare a investire sui punti di forza identificati, così da capitalizzare le opportunità e rafforzare il ruolo dell'Italia nel contesto europeo ed internazionale.

La Strategia identifica le azioni da mettere in pratica e gli obiettivi da perseguire per rendere l'Italia più competitiva, andando ad individuare le direzioni di sviluppo scientifico e redigendo le raccomandazioni strategiche in ambito, basandosi principalmente su quattro pilastri: lo sviluppo scientifico e industriale, la costruzione di un ecosistema nazionale integrato, l'internazionalizzazione e la sicurezza, e – non per ultime – la governance e misurabilità.

Ci sono stati anche nel dicembre 2025 a Roma gli Stati generali del Quantum che hanno riunito i rappresentanti delle istituzioni, del mondo della ricerca e dell'industria per fare il punto sulla Strategia nazionale per le tecnologie quantistiche e sulle sue implicazioni per sicurezza, innovazione e competitività. L'iniziativa, promossa dal Dipartimento per la Trasformazione digitale presso la presidenza del Consiglio ha posto al centro il ruolo del quantum come infrastruttura trasversale per il Paese. Gli interventi istituzionali hanno fatto emergere la necessità per il Paese di non disperdere gli investimenti e di concentrare gli sforzi in ottica sistemica. Da qui l'appello per la creazione di un Polo nazionale per le tecnologie quantistiche. Per quanto riguarda la Sicurezza nazionale e la competizione strategica, il ministro della Difesa, Guido Crosetto, ha chiarito che il quantum non può più essere considerato un ambito confinato alla ricerca avanzata, ma rappresenta già oggi “una leva specifica di sicurezza nazionale”, perché incide “sulla protezione delle informazioni, sulla resilienza delle infrastrutture critiche, sulla capacità di deterrenza e, in ultima analisi, sulla sovranità tecnologica

di una nazione”. “Quando un attore acquisisce capacità quantistiche mature – ha spiegato – non solo cambia il mondo in cui protegge i propri sistemi e il modo in cui può mettere a rischio quelli altrui, ma anche il proprio vantaggio competitivo in tutti i settori a più alto contenuto tecnologico”. In questo quadro, il rischio post-quantum e la vulnerabilità degli attuali sistemi crittografici impongono scelte rapide.

In questo contesto, Crosetto ha indicato quattro ambiti chiave – calcolo, sensing, simulazione e comunicazione – nei quali il quantum è destinato a produrre effetti immediati. Il computing quantistico, in particolare, introduce una nuova forma di superiorità computazionale, mentre il sensing consente capacità di misurazione e rilevamento senza precedenti.

Il Ministro ha quindi rilanciato l’idea di un Polo Nazionale Quantistico come infrastruttura unificante, capace di mettere insieme ricerca, industria e istituzioni. “Siamo troppo piccoli per permetterci compartimenti stagni e troppo piccoli per non mettere in sinergia tutte le nostre risorse”, ha osservato. Il modello indicato dal ministro è la Darpa statunitense, divisione del Dipartimento della Difesa in cui le tecnologie vengono ideate, testate e prototipate in modo rapido. “Questo dovrebbe essere il ruolo di un Polo Nazionale Quantum: evitare dispersioni e trasformare conoscenza e tecnologia in sicurezza concreta”.

Governance e coordinamento nazionale.

Accanto al profilo della sicurezza, durante gli Stati generali è emersa con forza l’esigenza di una governance pubblica e un coordinamento nazionale capaci di evitare le frammentazioni.

E’ merso inoltre che “il Quantum non è più una semplice promessa scientifica né una nicchia, ma una leva strategica che determinerà velocemente la competitività economica, la sicurezza nazionale e la capacità di innovazione dei singoli Paesi”.

Inoltre “il quantum non è un settore verticale ma un’infrastruttura che tocca ambiti nevralgici come la difesa, la sanità e l’industria, mettendo in gioco la competitività dell’intero sistema”. Da qui il ruolo dello Stato, chiamato a creare le condizioni per uno sviluppo ordinato e coordinato.

Sul versante della ricerca e dell’università, è essenziale la necessità di leggere il quantum come parte integrante della storia scientifica italiana e come leva per rafforzare la competitività del Paese. “Il quantum nasce dalla grande storia scientifica dell’Italia”, si sottolinea come, a differenza di altri ambiti – come l’IA –, l’Italia abbia radici profonde e riconosciute a livello internazionale nell’ambito quantistico.

Si è inoltre sottolineato il binomio tra capitale umano e capitale tecnologico, “due gemelli inscindibili che devono sempre stare molto vicini”. In questa prospettiva si collocano gli investimenti in infrastrutture di supercalcolo e tecnologie quantistiche, che hanno consentito di rafforzare l’Hpc nazionale e di avviare progetti come Partenope e Colossus. “Il quantum si sviluppa in maniera orizzontale, non solo producendo infrastrutture, ma collaborando con l’intelligenza artificiale”.

Un altro asse centrale è quello dell’ecosistema; il quantum impone un approccio non frammentato e fortemente interdisciplinare. La competitività, ha aggiunto, passa dalla capacità di creare “una massa critica” e di favorire la contaminazione tra discipline, dalla fisica al diritto, dall’ingegneria all’etica. In

questo quadro rientra anche il tema della sicurezza delle comunicazioni e dei dati. “Non esiste ricerca libera senza sicurezza: la ricerca può essere libera solo se sicura, e non c’è sicurezza senza difesa”, ha sottolineato il ministro, collegando il rafforzamento dell’ecosistema scientifico alla protezione delle infrastrutture e delle informazioni sensibili.

Emergono altresì chiaramente, alcuni punti di debolezza del nostro Paese: ritardo nello sviluppo di hardware quantistico nazionale competitivo (con conseguente necessità di grandi capitali di investimento), la poca consapevolezza in merito al potenziale di tali tecnologie, e la mancanza di linee guida su quantum e post-quantum security.

In questo senso, vi è la necessità di cogliere quanto prima le opportunità di sviluppo derivanti da questa analisi, puntando sulla formazione, l’adeguamento infrastrutturale e il rafforzamento della partecipazione italiana a tavoli di coordinamento tra filiera industriale, ricerca e istituzioni a livello europeo e internazionale.

Il Quantum Computing non è banale evoluzione tecnologica, ma una vera e propria rivoluzione in grado di trasformare il nostro approccio alla gestione dei problemi, della ricerca scientifica e anche al modo in cui saremo chiamati a proteggere le informazioni digitali.

Per questo motivo è importante non farsi trovare impreparati e mettere in moto sforzi sinergici per mettere in evidenza, ancora una volta, il grande bagaglio culturale e tecnologico che da sempre distingue la nostra Nazione.