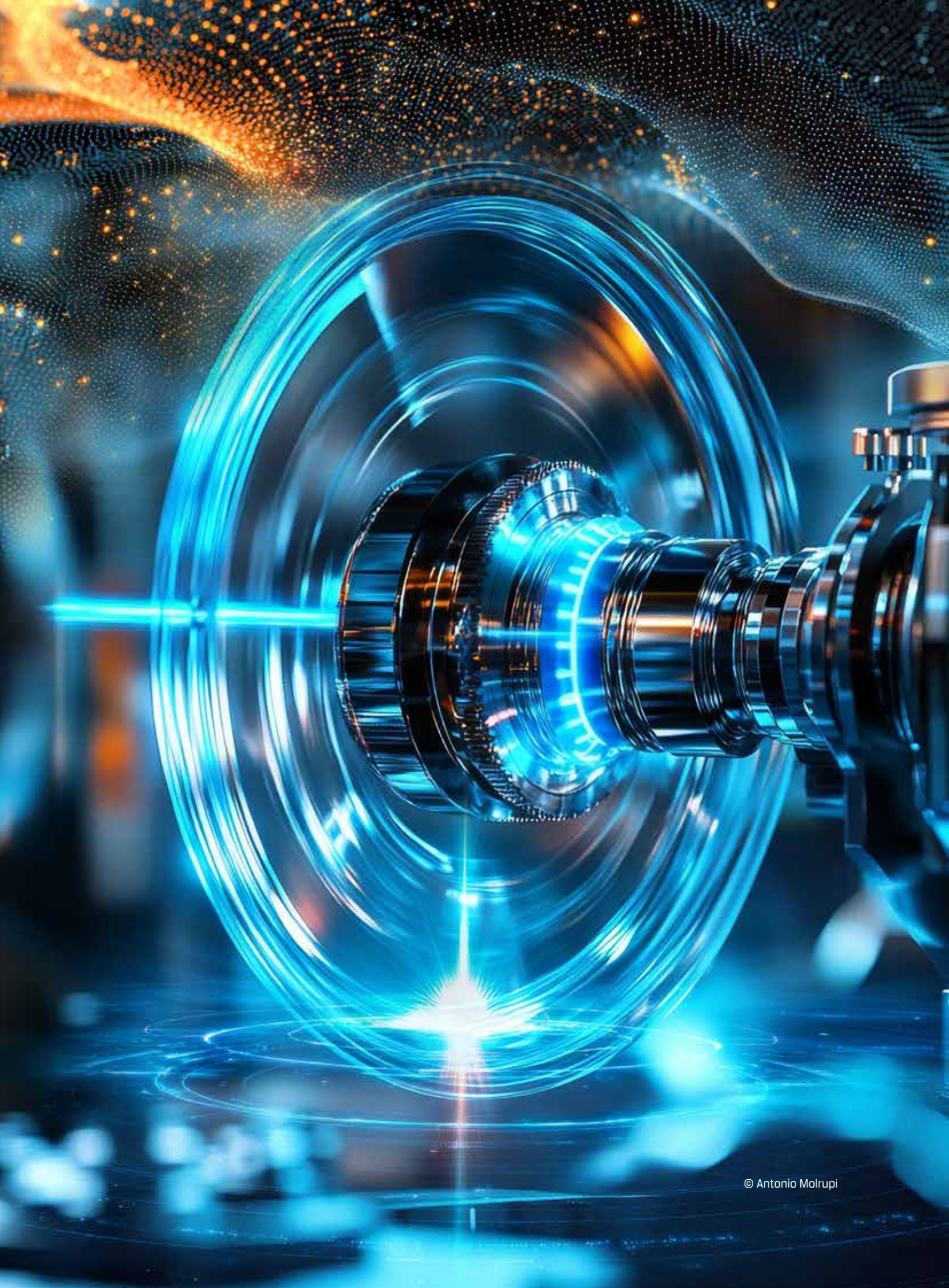

© Antonio Molrupi

ALESSANDRO GRASSANO - VINCENZO PULLEZ

ESPERTI TECNOLOGIE EMERGENTI*

TECNOLOGIE QUANTISTICHE

Un'opportunità strategica per lo sviluppo capacitivo della Difesa e il rafforzamento del sistema di ricerca e innovazione nazionale

La cosiddetta "seconda rivoluzione quantistica" rappresenta una delle trasformazioni più profonde nel rapporto tra ricerca scientifica avanzata, sicurezza, collaborazione e competizione geopolitica

*Gen. Div. Alessandro Grassano
Capo Ufficio Generale Strategia Militare e Innovazione dello Stato Maggiore della Difesa.

C.V. Vincenzo Pullez
Capo Ufficio Studi Strategici e Innovazione Tecnologica del Ministero della Difesa.

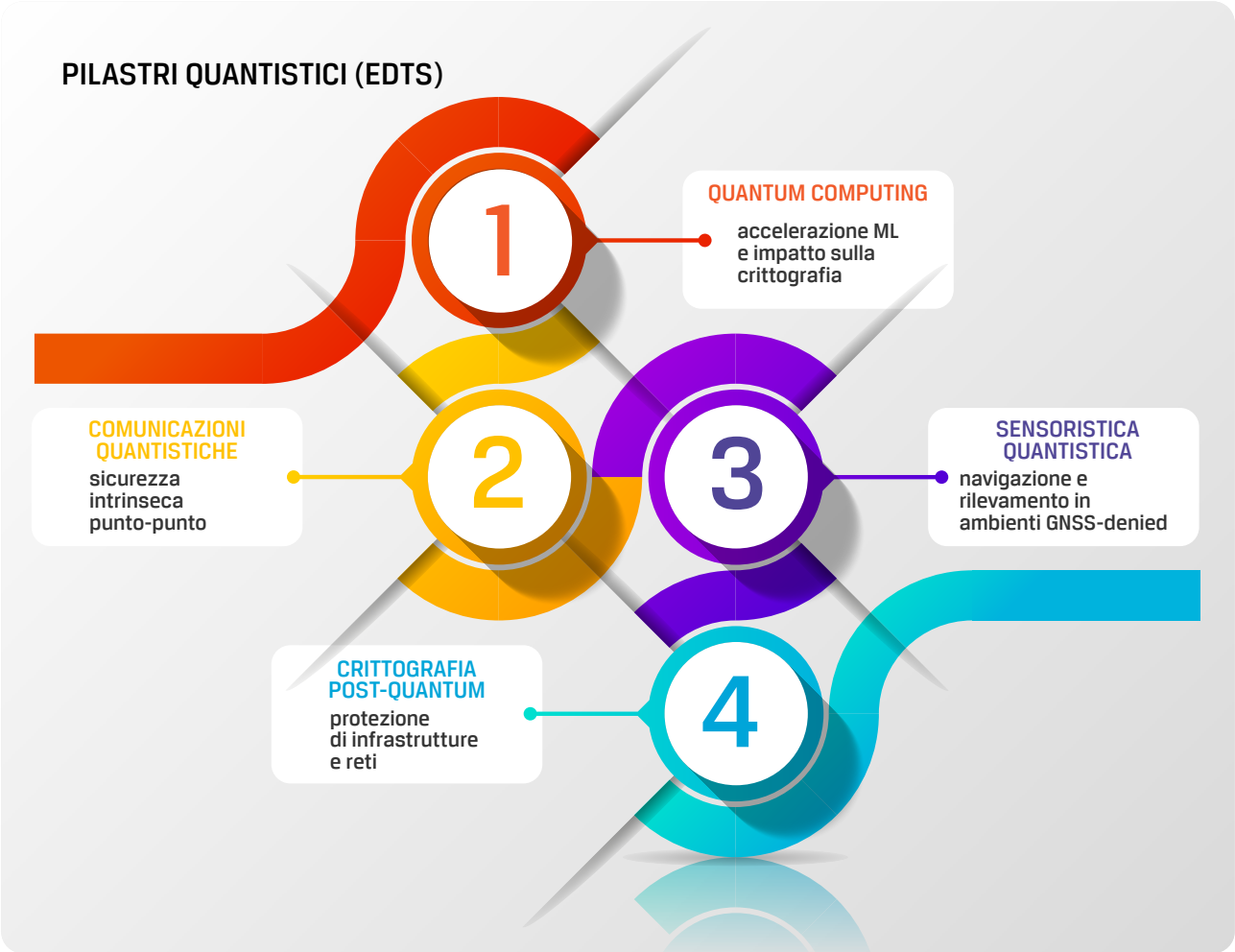


Audible sintesi articolo

Dopo la prima rivoluzione quantistica del XX secolo – che ha reso possibili tecnologie come i semiconduttori, il laser e il GPS – questa nuova fase è caratterizzata dalla capacità di controllare e sfruttare direttamente i fenomeni quantistici, aprendo nuovi scenari tecnologici.

Tra le Emerging and Disruptive Technologies (EDTs), le tecnologie quantistiche – quantum computing, sensoristica quantistica, comunicazioni quantistiche e crittografia post-quantum – stanno progressivamente ridefinendo gli equilibri globali. Il quantum computing, in prospettiva, potrebbe alterare i paradigmi della superiorità computazionale e della sicurezza crittografica; la sensoristica quantistica promette capacità di rilevamento e navigazione estremamente precise anche in ambienti Global Navigation Satellite System (GNSS) - denied; le comunicazioni quantistiche introducono nuovi modelli di sicurezza delle informazioni; mentre la crittografia post-quantum diventa una priorità per la protezione delle infrastrutture digitali e dei sistemi militari. In parallelo, la crescente integrazione tra quantum computing e intelligenza artificiale (IA) – sia nell'uso dell'IA per progettare e controllare sistemi quantistici sia nell'impiego di risorse quantistiche per accelerare specifici compiti di machine learning – sta emergendo come uno dei principali driver della prossima generazione di tecnologie digitali avanzate.

In questo contesto, la competizione tecnologica tra grandi potenze si estende sempre più al dominio quantistico, rendendo tali tecnologie un elemento chiave della sovranità e del vantaggio tecnologico, della resilienza delle infrastrutture digitali e della superiorità informativa. Per l'Europa, e per l'Italia in particolare, la sfida consiste nel trasformare l'eccellenza scientifica in capacità industriali, applicazioni dual-use e vantaggio strategico, evitando nuove forme di dipendenza tecnologica.



In ambito Difesa, le tecnologie quantistiche si configurano come un potenziale moltiplicatore di potenza informativa e operativa, destinato a incidere in modo significativo sull'evoluzione delle capacità militari. In particolare, la sensoristica quantistica promette avanzamenti rilevanti nella navigazione inerziale, nel rilevamento subacqueo e nella condotta di operazioni multidominio, mentre le comunicazioni quantistiche aprono prospettive di sicurezza intrinseca delle trasmissioni. Tali sviluppi si inseriscono nella più ampia trasformazione dei teatri operativi verso modelli di integrazione tra domini fisici, informativi e cognitivi, contribuendo alla progressiva configurazione di un "quantum-enabled battlefield".

Queste evoluzioni tecnologiche si collocano all'interno di una trasformazione più ampia dei conflitti del XXI secolo, caratterizzata da una crescente competizione tra grandi potenze e da cicli di innovazione militare più rapidi. In tale contesto, il quantum assume una valenza strategica non solo sul piano militare, ma anche su quello industriale e geopolitico, poiché il controllo delle tecnologie abilitanti contribuisce a definire standard tecnologici, catene del valore e architetture di cooperazione internazionale. Inoltre, la convergenza tra IA e quantum computing, già visibile nello sviluppo di algoritmi quantistici ottimizzati tramite machine learning e nei modelli di quantum-enhanced AI, è destinata a diventare un fattore abilitante della superiorità tecnologica e dell'innovazione deep-tech nel medio-lungo periodo.

Accanto alle opportunità capacitive, il quantum introduce tuttavia anche una nuova dimensione di rischio strategico, legata alla possibile vulnerabilità delle infrastrutture crittografiche su cui si fonda l'ecosistema digitale globale. L'attuale sicurezza delle comunicazioni digitali, delle transazioni finanziarie, delle identità elettroniche e delle reti governative e militari dipende infatti in larga misura dalla crittografia a chiave pubblica, fondata su problemi matematici computazionalmente proibitivi per i computer classici. Lo sviluppo di computer quantistici

Roadmap di migrazione Post-Quantum Cryptography (PQC)

Fasi prioritarie per infrastrutture digitali quantum-safe:
dalla mappatura degli asset alla gestione operativa e agli aggiornamenti continui.

Fase	Obiettivo	Output chiave
1. Inventario	Mappare asset e dipendenze crittografiche	Baseline e rischi HNDL
2. Priorizzazione	Classificare per valore e ciclo di vita	Lista MIgrazione
3. Migrazione	Integrare algoritmi NIST PQC	Prototipi e piani rollout
4. Validazione	Test di conformità e resilienza	Certifiche e hardening
5. Operazioni	Monitoraggio e gestione chiavi	Gestione incidenti e update



crittograficamente rilevanti, grazie ad algoritmi come quello di Shor, potrebbe mettere in discussione tali presupposti.

Il concetto di "Q-day", ossia la soglia tecnologica oltre la quale la crittografia a chiave pubblica diventa vulnerabile, è ormai entrato stabilmente nel dibattito strategico internazionale. Le stime disponibili indicano che questa soglia potrebbe essere raggiunta entro le prossime due decadi, con impatti economici, tecnologici e geopolitici potenzialmente sistemici. Un elemento particolarmente critico è rappresentato dal fenomeno noto come "harvest now, decrypt later", attraverso il quale attori statali o non statali possono intercettare e archiviare dati cifrati oggi per decifrarli in futuro, quando capacità quantistiche adeguate saranno disponibili. Il rischio riguarda in modo diretto informazioni a lungo ciclo di vita e alto valore strategico, tra cui comunicazioni diplomatiche, dati militari, proprietà intellettuale e archivi governativi.

La risposta tecnologica a questo scenario è rappresentata dalla post-quantum cryptography (PQC), ossia algoritmi crittografici progettati per resistere ad attacchi quantistici. Gli standard internazionali in fase di definizione delineano una transizione di lungo periodo, che richiederà investimenti significativi e un coordinamento sistemico tra istituzioni pubbliche, industria e comunità scientifica.

Per la Difesa, la transizione verso infrastrutture digitali quantum-safe non rappresenta soltanto un problema tecnologico, ma una priorità di pianificazione strategica e di resilienza nazionale. L'aggiornamento delle infrastrutture crittografiche coinvolgerà infatti sistemi legacy, piattaforme operative, supply chain industriali e architetture di comando e controllo, configurandosi come uno dei più ampi processi di trasformazione tecnologica nel dominio cyber e informativo.

In questo contesto, la natura dual-use delle tecnologie quantistiche impone una riflessione strutturata sulla governance dell'innovazione. L'esperienza internazionale dimostra che i Paesi tecnologicamente più avanzati sono quelli

Governance Quantistica

Modello integrato di governance per la Strategia Nazionale sulla Quantistica.

Fonte: Strategia Quantistica Italiana — Sintesi.

500.000.000 €
Investimenti attesi

3.000
Nuovi posti lavoro

10
Iniziative chiave

Comitato Politico
Responsabile per la definizione degli indirizzi strategici per l'attuazione della Strategia Nazionale.

Comitato Direzione Strategica
Rappresentanti istituzionali, accademici e industriali per garantire supervisione e coerenza.

Struttura Operativa
Gestione amministrativa dei bandi, erogazione di finanziamenti e trasferimento tecnologico.

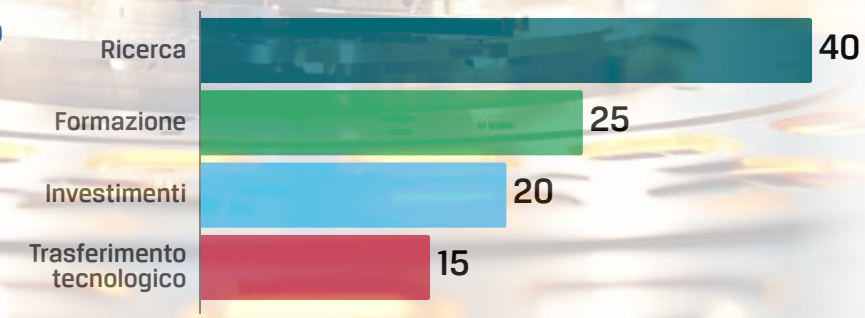
UMVS
Raccogliere dati, monitorare KPI, verificare milestone triennali e proporre aggiornamenti.

Piano Gestione Rischi
Mappatura delle dipendenze critiche, monitoraggio della mobilità dei talenti e della proprietà intellettuale, e definizione di contromisure in caso di crisi.

Fondazione
Facilitare la convergenza tra investimenti pubblici e privati per rafforzare l'ecosistema.

Conferenza Nazionale
Evento annuale per consultazione, raccolta feedback e co-progettazione con Regioni, università e imprese.

Focus Strategico
Distribuzione prevista tra ricerca, formazione, investimenti e trasferimento tecnologico.



Il **Technology Readiness Level (TRL)** è un sistema di misurazione per valutare il grado di maturità tecnologica di un sistema o di un componente. Il modello TRL è suddiviso in nove livelli, che vanno dal TRL 1, corrispondente ai primi principi scientifici osservati, fino al TRL 9, che indica una tecnologia completamente testata e validata in ambiente operativo.

capaci di orchestrare ecosistemi integrati, nei quali Difesa, università, centri di ricerca, startup e grandi industrie collaborano in modo continuativo per il conseguimento di obiettivi tecnologici condivisi. In tale quadro, la Difesa, grazie alla capacità di definire requisiti operativi e sostenere investimenti di lungo periodo, può svolgere un ruolo determinante come early adopter e catalizzatore dell'innovazione, contribuendo a ridurre il divario tra ricerca scientifica e applicazioni operative.

Per il sistema nazionale, la sfida consiste quindi nel superare la frammentazione degli investimenti e delle iniziative e nel rafforzare meccanismi di coordinamento capaci di accelerare la transizione dalla ricerca di base allo sviluppo prototipale e operativo. In questa prospettiva, la creazione di infrastrutture dedicate alla sperimentazione, integrazione e validazione tecnologica, sul modello di poli di innovazione mission-oriented, può rappresentare uno strumento efficace per valorizzare il patrimonio scientifico e industriale esistente e favorire la collaborazione tra attori pubblici e privati.

Il percorso avviato con la "Strategia italiana per le tecnologie quantistiche" rappresenta una solida base su cui costruire questa evoluzione, ma richiede un ulteriore consolidamento sul piano operativo. Come già osservato in altri ambiti ad alta intensità tecnologica, il rischio principale rimane la dispersione delle competenze e la frammentazione degli sforzi, che rallentano la trasformazione dei risultati scientifici in capacità applicative. Per evitarlo, diventa necessario dotarsi di strutture dedicate di coordinamento e sperimentazione, in grado di accompagnare le tecnologie quantistiche lungo l'intero ciclo di innovazione – dal basso Technology Readiness Level (TRL) fino al prototipo operativo – riducendo la cosiddetta valley of death dell'innovazione tecnologica.

Un riferimento concreto in questa direzione è rappresentato dal Polo Nazionale della dimensione Subacquea (PNS), che ha dimostrato come un'iniziativa interministeriale guidata dalla Difesa, ma aperta all'ecosistema civile e industriale, possa generare effetti sistemici, favorendo il rapid prototyping, l'attrazione di investimenti, l'allineamento strategico e lo sviluppo di competenze critiche. L'esperienza del PNS evidenzia come poli di innovazione mission-oriented possano fungere da acceleratori tecnologici e da strumenti di integrazione tra ricerca, industria e utilizzatori finali.

In continuità con questa esperienza e in linea con l'indirizzo politico delineato dal Ministro della Difesa durante gli Stati Generali Quantum, la creazione di un Polo Nazionale Quantistico (PNQ) consentirebbe di concentrare competenze, infrastrutture e capacità di test & validation all'interno di un framework unitario, favorendo la cooperazione pubblico-privata, la sperimentazione comparativa tra diverse soluzioni tecnologiche e il dialogo continuo tra esigenze operative e ricerca avanzata. Il PNQ dovrebbe configurarsi come una piattaforma nazionale di integrazione tecnologica, non limitata al quantum computing, ma estesa all'intero spettro delle tecnologie quantistiche e alla loro integrazione con l'intelligenza artificiale, contribuendo al tempo stesso a rafforzare la continuità tra ricerca fondamentale e sviluppo tecnologico lungo l'intera filiera dei livelli di TRL.

Un'infrastruttura di questo tipo contribuirebbe non solo a rafforzare l'autonomia tecnologica nazionale, ma anche a consolidare la credibilità internazionale del Paese nei futuri equilibri di sicurezza e nelle architetture di cooperazione tecnologica, sempre più basate sulla condivisione selettiva di capacità avanzate.

In tale quadro, le tecnologie quantistiche rappresentano un'opportunità di sviluppo capacitivo e una sfida per la sicurezza digitale e la resilienza delle infrastrutture critiche. Esse richiedono un approccio integrato che combini innovazione tecnologica, pianificazione strategica e cooperazione tra attori pubblici e privati.

La capacità di anticipare la transizione verso il paradigma quantistico costituirà uno dei fattori determinanti della sicurezza nazionale e della sovranità tecnologica dei prossimi decenni.