PRESIDENZA DEL CONSIGLIO DEI MINISTRI
SISTEMA DI INFORMAZIONE
PER LA SICUREZZA DELLA REPUBBLICA

L'AVVENTO DELLE TECNOLOGIE QUANTISTICHE

L'AVVENTO DEL QUANTUM COMPUTING

PREMESSA

Il primario settore di frontiera verso cui si sta orientando il focus della competizione globale è quello della tecnologia quantistica. In particolare, le potenzialità di tali strumenti tecnologici di rendere obsoleti gli attuali sistemi crittografici, di offrire alle comunicazioni militari o diplomatiche un cono di tutela rispetto a mirate azioni intercettive, di fornire mezzi avanzati di ricognizione/navigazione in assenza dell'ausilio satellitare, nonché di accelerare i processi di ricerca in campo scientifico, rappresentano solo alcuni esempi delle innumerevoli applicazioni pratiche delle tecnologie emergenti.

Si comprende, dunque, il motivo per cui, recentemente, la sfida posta dalle quantum technologies rappresenti uno dei principali terreni di confronto tra le grandi potenze.

LE DIRETTRICI APPLICATIVE

I cospicui investimenti e le ricerche nel settore delle tecnologie quantistiche si sono articolati lungo le tre principali direttrici applicative che lo contraddistinguono:

- quantum computing. Offre funzionalità innovative nella risoluzione di problemi complessi di ottimizzazione e simulazione non risolvibili con metodi convenzionali. Sfruttando i principi della meccanica quantistica, tale tecnologia permette di esplorare simultaneamente un numero esponenziale di soluzioni a un problema, eseguendo calcoli complessi che richiederebbero lunghi tempi di elaborazione ai computer tradizionali;
- quantum sensing. Garantisce una precisione senza precedenti nella misurazione delle proprietà fisiche, specialmente in ambienti in cui i sensori tipicamente impiegati risultano insufficienti. Si tratta di strumenti in grado di rilevare variazioni anche minime del bene analizzato e, pertanto, estremamente utili in campo medico, geologico o militare;
- quantum security and communications. Fornisce una protezione innovativa dal punto di vista crittografico, anche per quanto attiene alle comunicazioni. Dall'altro lato della medaglia, è evidente come la medesima tecnologia possa essere impiegata per decrittare conversazioni cifrate altrui.

Ne consegue, pertanto, che chiunque riesca ad acquisire la leadership su queste applicazioni otterrà inevitabilmente un vantaggio strategico. In altri termini, il Paese che svilupperà per primo un computer quantistico pienamente funzionante avrà la capacità, ad esempio, di violare gli attuali sistemi crittografici e accedere a comunicazioni riservate, nonché di ottenere la supremazia in settori di cruciale rilievo sul piano economico e sociale.

LA “CORSA QUANTISTICA”

Alla luce di tale scenario, non sorprende che, tra gli altri, Stati Uniti, Cina, Unione europea, Giappone e India stiano investendo massicciamente in programmi di ricerca quantistica. Assistiamo a una vera e propria “corsa quantistica” globale, paragonabile alla corsa agli armamenti di altre epoche, ma combattuta nei laboratori e nei centri di ricerca. Gli investimenti governativi si accompagnano a quelli dei colossi privati che, di fatto, figurano tra i principali innovatori.

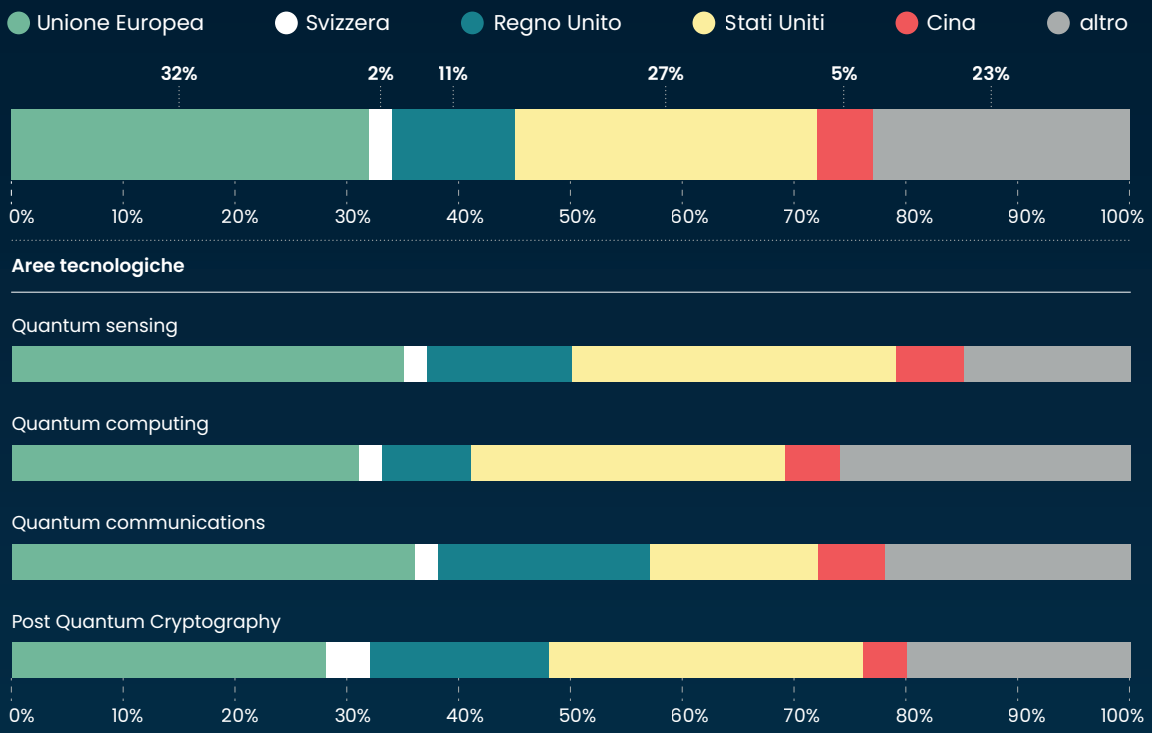
Più nel dettaglio, su 441 aziende quantistiche localizzate nel mondo, 141 (ossia il 32%) si trovano nell’Unione europea, circa un quarto negli Stati Uniti, mentre il 5% sono situate in Cina. Nonostante rappresentino una quota maggiore, le imprese europee sono più giovani e piccole rispetto a quelle presenti in altri contesti territoriali. Sul piano temporale, mentre solo il 28% delle aziende americane è stato fondato dopo il 2018, nell’UE il dato di quelle costituite nello stesso periodo si attesta intorno al 60% (in Cina la percentuale è del 50%). Quanto alle dimensioni, la quota delle grandi e medie imprese europee è pari al 13%, rispetto al 29% statunitense e all’82% sinico.

Tutto ciò si riflette, in parte, sul panorama dei brevetti ove, nell’arco temporale che va dal 2017 al 2024, sono state riscontrate circa trentamila registrazioni correlate al settore quantistico.

La Cina domina con aziende che possiedono circa il 46% dei brevetti a livello globale.

TECNOLOGIE QUANTISTICHE

SUDDIVISIONE PER LOCALIZZAZIONE GEOGRAFICA DELLE SOCIETÀ OPERANTI NEL SETTORE



Seguono gli Stati Uniti al 23%, mentre l'Unione europea e il Giappone si attestano intorno al 6%. Si segnala, tuttavia, che negli ultimi anni si è assistito a una graduale riduzione nella registrazione di brevetti da parte americana e cinese, a cui si contrappone una stabile crescita europea. Significativa anche la circostanza che i brevetti sinici tendano a essere spesso registrati soltanto nel mercato domestico, mettendo in luce un fenomeno di "home bias", che si riflette altresì nell'ambito delle proprie pubblicazioni scientifiche, in quanto citate in modo sistematico e sproporzionato negli articoli cinesi. In tale cornice, emerge inoltre la tendenza delle aziende site sul territorio dell'Unione ad aprirsi verso attività collaborative in materia di brevetti, che prevedono azioni congiunte con partner di altri Paesi (anche extraeuropei) per facilitare lo sviluppo di tecnologie quantistiche in

L'AVVENTO DEL QUANTUM COMPUTING COSTITUISCE UN PUNTO DI DISCONTINUITÀ NEL PARADIGMA DELLA SICUREZZA INFORMATICA

vista della c.d. co-brevettazione. Resta significativo il fatto che buona parte dei brevetti registrati (circa il 17%) siano posseduti da centri di ricerca e università. Il dato mette in luce come le tecnologie quantistiche siano ancora in una fase di sviluppo, evidenziando così il ruolo chiave che assumerà la ricerca (e ovviamente gli investimenti pubblici e privati in direzione della stessa) nel breve-medio periodo.

In linea di massima, quanto prospettato mette in luce un tipico fenomeno di oligopolio tecnologico, che, analogamente a quanto è avvenuto con la corsa allo spazio o la rivoluzione nucleare, favorisce l'emersione dei pochi attori che vantano sia risorse ingenti, sia una visione strategica di lungo termine.

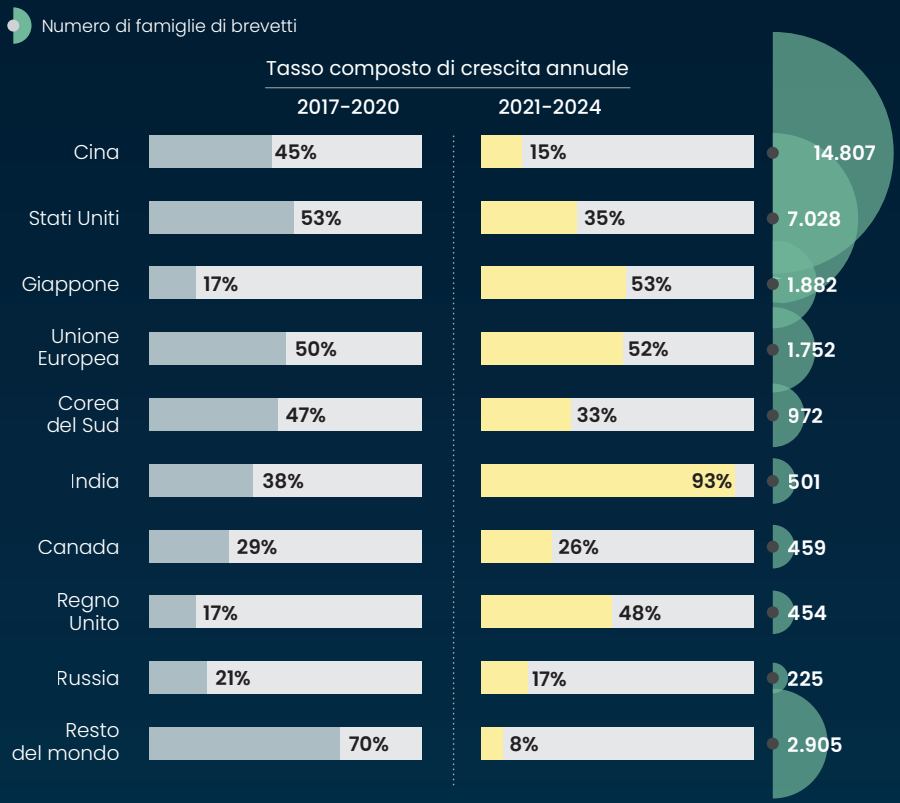
In chiave prospettica, la rapidità della rivoluzione quantistica, oltre ad aprire nuove vie di conoscenza e offrire inediti strumenti a favore del progresso dell'umanità, pone comunque delle sfide gravose la cui risoluzione richiederà necessariamente linee d'azione coerenti e coese da parte dell'accademia, dell'industria e degli Stati. A oggi, infatti, le tecnologie quantistiche non hanno raggiunto ancora quel grado di stabilità e robustezza che ci si dovrebbe attendere ai fini di una commercializzazione su vasta scala. La necessità di operare con temperature vicine allo zero assoluto e in ambienti protetti costituisce solo un esempio degli innumerevoli elementi critici che tuttora accompagnano tali tecnologie. Senza trascurare, poi, le incognite legate all'applicazione e all'impatto di questi strumenti di frontiera sui diritti fondamentali delle persone. Rileva, nel senso, la libertà e la segretezza delle comunicazioni, che, come detto, potrebbero facilmente venire carpite e portate "in chiaro" (specie ove avvengano nell'ambiente della rete internet) attraverso attività di cyber-hacking capaci di sfruttare mezzi di decrittazione quantistici.

L'ATTUALE CONVERGENZA DI MATURITÀ TECNICA, DISPONIBILITÀ DEL MERCATO E NECESSITÀ ECONOMICA STA CREANDO UN'OPPORTUNITÀ SENZA PRECEDENTI

In definitiva, l'attuale convergenza di maturità tecnica, disponibilità del mercato e necessità economica sta creando un'opportunità senza precedenti che, se adeguatamente compresa dagli attori pubblici e privati, potrà fornire un fondamentale vantaggio competitivo in materia quantistica. La traiettoria di sviluppo è stata quindi tracciata e, nei prossimi anni, accanto alle note rivalità tra superpotenze per ottenere il primato tecnologico, si assisterà verosimilmente anche all'avvio di nuovi tavoli di collaborazione

FAMIGLIE DI BREVETTI

SUDDIVISIONE PER PAESI DELLE FAMIGLIE DI BREVETTI SULLE TECNOLOGIE QUANTISTICHE NEL PERIODO 2017-2024



che, in considerazione della complessità del tema, cercheranno di definire standard comuni, condividere i risultati raggiunti sul piano scientifico, sviluppare nuove competenze, investire in modo mirato su infrastrutture e talenti, nonché implementare le catene di fornitura e le capacità produttive. Tutto ciò, per realizzare un robusto ecosistema che, anche grazie al partenariato pubblico-privato, guiderà l'innovazione, l'imprenditorialità e la crescita nel settore quantistico, con la consapevolezza che la rapidità nell'evoluzione di tali tecnologie farà da catalizzatore per una maggiore resilienza, destrezza e competitività su scala globale.

QUANTUM E CRITTOGRAFIA

All'interno di tale contesto in continua evoluzione, il quantum computing è emerso come una delle tecnologie più promettenti e, allo stesso tempo, maggiormente sfidanti del panorama tecnologico contemporaneo, a causa della sua capacità di:

- accelerare l'esecuzione di specifiche operazioni matematiche, con tempistiche impensabili per gli attuali computer;
- sfruttare le proprietà intrinseche della meccanica quantistica per affrontare classi di problemi che richiedono la valutazione di sistemi complessi, in cui l'interazione tra elementi costituisce un fattore rilevante.

Tali potenzialità, se, da un lato, aprono prospettive innovative in diversi settori scientifici e industriali, dall'altro, comportano significative implicazioni in tema di sicurezza informatica.

Al riguardo, occorre osservare che, nel corso degli ultimi decenni la sicurezza delle comunicazioni digitali è stata fortemente correlata all'impiego di algoritmi crittografici a tutela della riservatezza e dell'integrità, nonché di misure di sicurezza a tutela della

disponibilità dei dati memorizzati o trasmessi digitalmente. Pertanto, la robustezza di tali algoritmi si fonda:

- nel caso degli algoritmi crittografici simmetrici (basati sull'impiego della medesima chiave sia per la cifratura che per la decifratura dei dati, come l'algoritmo Advanced Encryption Standard - AES), sull'ipotesi per cui il tempo necessario alla conduzione di un attacco che vada a buon fine (ad esempio, attacchi di tipo brute-force) cresce esponenzialmente rispetto alla dimensione delle chiavi di cifratura impiegate, rendendo quindi impraticabili i tentativi di decifratura dei dati ove si ricorra a chiavi crittografiche di grandi dimensioni;
- nel caso degli algoritmi crittografici asimmetrici (basati sull'impiego di coppie di chiavi crittografiche matematicamente collegate: una pubblica per la cifratura e una privata per la decifratura), sulla complessità computazionale di risoluzione di specifici problemi matematici, come quello della fattorizzazione dei grandi numeri (per l'algoritmo Rivest-Shamir-Adleman - RSA), del calcolo del logaritmo discreto (per il protocollo di Diffie–Hellman) o del calcolo del logaritmo discreto su curve ellittiche (per schemi/algoritmi di Elliptic Curve Cryptography - ECC e per firme digitali su curve ellittiche, come l'Elliptic Curve Digital Signature Algorithm - ECDSA).

IL DESCRITTO SCENARIO DI RISCHIO HA DATO IMPULSO ALLA RICERCA DI NUOVI PARADIGMI DI CIFRATURA RESISTENTI AGLI ATTACCHI PERPETRATI DAI COMPUTER QUANTISTICI

L'avvento del quantum computing costituisce, tuttavia, un punto di discontinuità nel paradigma della sicurezza informatica, in quanto mette in discussione, almeno sul piano teorico, la sicurezza degli algoritmi crittografici in uso. Si pensi, nel senso:

- all'algoritmo quantistico di Shor – per la risoluzione efficace del problema della fattorizzazione dei numeri interi o del calcolo del logaritmo discreto in tempo polinomiale – che costituisce una minaccia concreta ai sistemi di crittografia asimmetrica attualmente impiegati, basati sulla risoluzione dei citati problemi matematici;
- all'algoritmo quantistico di Grover – per la risoluzione dei problemi di ricerca di un elemento all'interno di un database o di un elenco non ordinato di elementi, consentendo una velocizzazione quadratica degli attacchi di tipo brute-force – che, sebbene non riesca a violare completamente la sicurezza degli algoritmi crittografici simmetrici, rende necessario un aumento della lunghezza delle chiavi crittografiche impiegate.

Il descritto scenario di rischio ha dato impulso alla ricerca di nuovi paradigmi di cifratura resistenti agli attacchi perpetrati dai computer quantistici.

Tutto ciò ha portato allo sviluppo della c.d. post-quantum cryptography, ossia una classe di algoritmi crittografici – attualmente oggetto di ricerca – costruiti su problemi matematici ritenuti sicuri anche rispetto a potenziali attacchi perpetrati mediante l'impiego di computer quantistici.

Sebbene si tratti di ambiti in fase di consolidamento, in particolare sotto il profilo della standardizzazione e delle applicazioni crittografiche, il loro sviluppo potrebbe costituire, in prospettiva futura, una delle innovazioni più dirompenti del prossimo decennio.

QUANTUM E SICUREZZA NAZIONALE

Tanto premesso, il quantum computing deve essere considerato, nel contesto della sicurezza nazionale, come una tecnologia dual-use, il cui impatto si estende ben oltre il dominio puramente informatico, influenzando deterrenza, Intelligence, protezione delle infrastrutture critiche e competitività di carattere economico, strategico e tecnologico. Tutto ciò si concretizza nelle seguenti sfide per la sicurezza nazionale:

- minaccia alla crittografia attuale. L'avvento del quantum computing apre nuovi, inaspettati scenari di rischio alla sicurezza delle informazioni. Nel merito:
  - sebbene, come anticipato, l'algoritmo di Grover non violi completamente la sicurezza degli algoritmi crittografici simmetrici, lo stesso rende comunque necessario un aggiornamento della lunghezza delle chiavi crittografiche impiegate nell'ambito di tali sistemi;
  - l'effetto più dirompente è invece quello prodotto dall'algoritmo di Shor sui sistemi di crittografia asimmetrica. Tale algoritmo dimostra infatti – almeno sul piano teorico – che, in presenza di un computer quantistico suffi-

cientemente potente e fault-tolerant, i problemi matematici alla base dei citati algoritmi crittografici (considerati, a oggi, intrattabili per i computer tradizionali), diverrebbero risolvibili in tempi compatibili con la conduzione di attacchi informatici.

IL QUANTUM COMPUTING DEVE ESSERE CONSIDERATO, NEL CONTESTO DELLA SICUREZZA NAZIONALE, COME UNA TECNOLOGIA DUAL-USE

Sul piano securitario, ciò implicherebbe non solo il potenziale rischio di compromissione della riservatezza, dell'integrità e della disponibilità dei dati memorizzati o trasmessi digitalmente, ma anche una conseguente inaffidabilità dei meccanismi di sicurezza crittografica attualmente impiegati a tutela delle informazioni;

- rischio di attacchi retroattivi. Un ulteriore fattore di rischio è quello connesso al c.d. "harvest now, decrypt later", ossia di intercettazione e archiviazione da parte di attori ostili di grandi quantità di dati cifrati, con l'obiettivo di decifrarli in futuro, quando saranno disponibili computer quantistici dotati di sufficiente potere computazionale. Viene introdotta così una nuova dimensione temporale al concetto di minaccia, aprendo scenari che richiedono un'attenta riflessione in merito al valore strategico delle informazioni nel lungo termine ed evidenziando l'urgenza di adottare un approccio proattivo alla sicurezza crittografica;
- sovranità tecnologica e nuove asimmetrie di potere. Lo sviluppo del quantum computing richiede ingenti risorse finanziarie, infrastrutturali e competenze

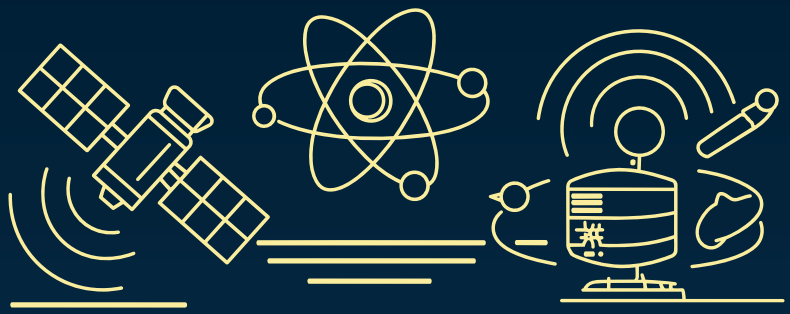
professionali altamente specializzate. In tale contesto, la diversificata possibilità di accesso a tali risorse può generare nuove forme di asimmetria strategica a livello internazionale, che potrebbero influenzare alleanze, dipendenze tecnologiche e, conseguentemente, dinamiche di potere. Il controllo della filiera di fornitura quantistica diventa quindi un elemento di rilievo in ottica di sovranità tecnologica;

- instabilità geopolitica. La percezione di un vantaggio o di uno svantaggio quantistico potrebbe incentivare comportamenti destabilizzanti in ambito geopolitico. In tale contesto, l'avvento del quantum computing rischia di alterare i rapporti di potere attualmente vigenti, con l'adozione di posture più aggressive, un incremento di attacchi informatici finalizzati all'acquisizione illecita di informazioni privilegiate e know-how specialistico, nonché la definizione di nuove alleanze strategiche.

Quanto alle opportunità per la sicurezza nazionale, rilevano:

- il supporto alle capacità analitiche intelligence. La capacità teorica dei sistemi quantistici di elaborare enormi moli di informazioni eterogenee e provenienti da fonti diversificate costituisce un fattore abilitante a sostegno delle capacità analitiche e previsionali nazionali. Tale fattore si traduce in un conseguente vantaggio strategico e tecnologico, frutto di una rinnovata capacità di valutazione strategica e di trasformazione dei dati in conoscenza utile al potere decisionale;

- l'efficientamento dei sistemi di difesa informatica. La capacità dei sistemi quantistici di elaborazione di grandi volumi di informazioni può contribuire al complessivo efficientamento dei sistemi di difesa a tutela delle infrastrutture critiche nazionali. Nello specifico, algoritmi quantistici quali quello di Grover forniscono un vantaggio rilevante nelle operazioni di ricerca su set di dati non strutturati, con applicazione dirette nella scansione di grandi database, nell'individuazione di pattern comportamentali noti e nella rilevazione di anomalie. Tale vantaggio risulta rilevante in contesti in cui la velocità di analisi e correlazione delle informazioni rappresenta un fattore critico, come nei sistemi di monitoraggio in tempo reale, nell'analisi dei log e nei sistemi di rilevamento e risposte alle intrusioni informatiche;



- lo sviluppo di sistemi di comunicazione sicura. Il quantum computing ha un impatto duplice sulla sicurezza informatica: se, da un lato, algoritmi come quello di Shor e di Grover mettono a repentaglio la sicurezza degli attuali protocolli crittografici, dall'altro, tali tecnologie abilitano nuovi strumenti di difesa. In particolare, i sistemi quantistici possono essere sfruttati per la generazione di numeri casuali ad alta entropia (impiegati, a titolo esemplificativo, per la generazione di chiavi crittografiche e parametri di autenticazione sicuri), per la distribuzione sicura delle chiavi crittografiche (Quantum Key Distribution), consentendo di ri-

levare eventuali tentativi di intercettazione durante lo scambio delle chiavi o per il rafforzamento dei meccanismi di autenticazione e di verifica dell'integrità dei dati trasmessi digitalmente;

- l'OSINT e la disinformazione. Lo sviluppo di sistemi quantistici può inoltre costituire un valido supporto al settore OSINT, con particolare riferimento all'efficientamento della raccolta, dell'analisi e della valorizzazione informativa dei dati raccolti in fonti aperti. In tale contesto, l'applicazione di algoritmi quantistici potrebbe accelerare il processo di correlazione delle informazioni e di individuazione di trend emergenti.

In definitiva, il quantum computing introduce un cambiamento strutturale nel paradigma della sicurezza informatica, la cui influenza sulla sicurezza nazionale dipenderà in larga parte dalla capacità di anticiparne gli effetti.

Il quantum computing ha altresì una forte dimensione geopolitica: le decisioni in questo ambito richiedono una cooperazione a livello internazionale per la definizione di standard comuni finalizzati alla protezione delle catene di approvvigionamento tecnologico (supply chain) e alla gestione di potenziali rischi sistemici su scala globale.

"Per una tecnologia di successo,
l'onestà deve avere la precedenza sulle pubbliche relazioni,
perchè la natura non può essere ingannata"

(Richard Feynman, Premio Nobel per la fisica nel 1965
per gli studi sulla Quantistica)

La Relazione al Parlamento in versione digitale

È possibile visualizzare e scaricare la Relazione accedendo al sito web istituzionale:

https://www.sicurezzanazionale.gov.it

oppure utilizzando il QR Code di seguito.

Dato alle stampe nel febbraio 2026

www.sicurezzanazionale.gov.it

#sicurezzanazionale