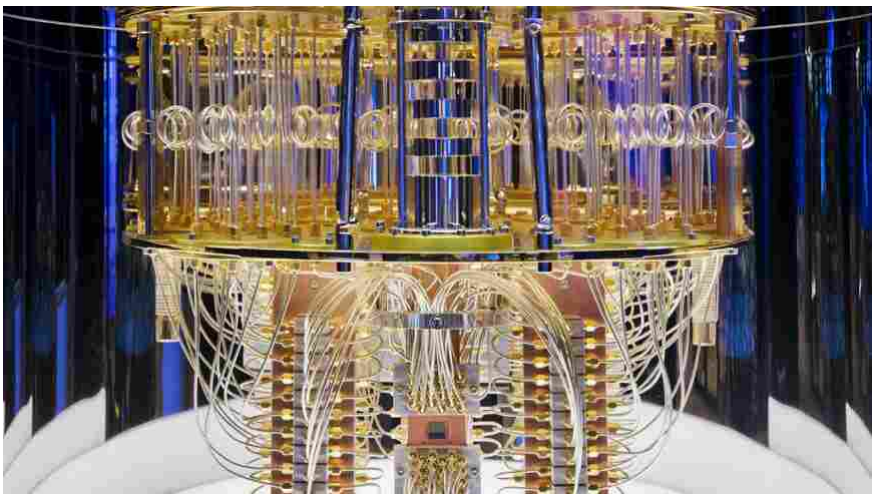
START MAGAZINE

INNOVAZIONE

La superpotenza del futuro dovrà dominare la quantistica. Ecco perché

4 Giugno 2023 07:47



di Paolo Savona e Fabio Vanorio

LOADING...

"Lo Stato che per primo raggiungerà la supremazia quantistica sarà in grado di proteggere i propri segreti con un livello di sicurezza superiore a quello degli altri e avrà un accesso illimitato agli Stati che lo hanno perso". Pubblichiamo un estratto del libro "Geopolitica dell'infosfera" (Rubbettino) di Paolo Savona e Fabio Vanorio

La ricerca e lo sviluppo del calcolo quantistico stanno accelerando. Nel 2022, IBM prevede di rendere pubblico Osprey, processore a 433 qubit. Entro il 2023, l'azienda prevede di rilasciare Condor, processore da 1.121 qubit, in corrispondenza del quale IBM ritiene di poter raggiungere la supremazia quantistica.

Nel 2022, Microsoft prevede di fornire con Azure Quantum, un accesso quantistico al cloud mediante una piattaforma che fornisca alle aziende risorse quantistiche senza la necessità di infrastrutture e spese elevate. Ricerca e innovazione nella scienza e nella tecnologia quantistica sono in continuo aumento, con investimenti attuali a livello mondiale che sfiorano i 30 miliardi di dollari.

Nel complesso, entro il 2027, il mercato globale della tecnologia quantistica raggiungerà i 42,4 miliardi di dollari entro il 2027, l'informatica quantistica guiderà il mercato con 16,1 miliardi di dollari a un tasso di crescita annuale composto del 39,4% (Vance 2022). Il Nord America sarà il più grande mercato regionale per le tecnologie quantistiche in generale. La Cina guiderà il mercato delle tecnologie quantistiche nell'area

Asia-Pacifico con 5,41 miliardi di dollari entro il 2027 e un tasso di crescita annuale composto del 38,5%. La Germania guiderà il mercato europeo delle tecnologie quantistiche con 3,6 miliardi di dollari entro il 2027, con un tasso di crescita annuale composto del 33,1%.

Nel 2020, la Casa Bianca ha dichiarato di voler raddoppiare i finanziamenti per la quantistica non legata alla difesa, portandoli a 1,2 miliardi di dollari entro il 2022. Parallelamente agli investimenti, anche il panorama delle minacce è destinato ad accelerare. Lo Stato che per primo raggiungerà la supremazia quantistica sarà in grado di proteggere i propri segreti con un livello di sicurezza superiore a quello degli altri e avrà un accesso illimitato agli Stati che lo hanno perso (Majot and Yampolskiy 2015). La capacità di mitigare le minacce quantistiche significa, dunque, un'estensione cronologica del potere dello Stato e un vantaggio di influenza globale per i primi che la raggiungeranno (Tibbetts 2019). Dato il potenziale di impatto del calcolo quantistico, gli Stati Uniti, l'Unione Europea, la Cina, il Giappone e altri stanno facendo significativi investimenti nel Quantum Computing, così come nei campi correlati della comunicazione e del rilevamento quantistico.

Notevoli progressi sono stati compiuti nell'hardware, nel software e negli algoritmi alla base dei computer quantistici, così come nei campi in cui la Quantum Computing potrebbe essere applicata. Il Quantum Computing accelererà la capacità di decifrare le informazioni protette dalle attuali tecniche di crittografia a chiave pubblica. Mentre le diverse applicazioni del calcolo quantistico saranno senza dubbio fondamentali per la crescita economica e la competitività globale a lungo termine, in termini di cybersicurezza la capacità dirompente di una rottura dell'attuale crittografia a chiave pubblica sarebbe una delle più impegnative sfide da affrontare. L'attuale crittografia a chiave pubblica si basa sul fatto che un computer classico può facilmente moltiplicare grandi numeri primi, ma non è in grado di invertire un tale calcolo senza migliaia di anni di elaborazione.

Nel 1994, Peter Shor teorizzò che un grande computer quantistico con tolleranza ai rumori (quindi senza decoerenza) potrebbe trovare i fattori primi dei numeri interi in una frazione del tempo necessario a un computer convenzionale. Questo renderebbe istantaneamente obsoleti molti dei comuni standard di crittografia in circolazione. Questa capacità è, per ora, fuori portata. Si stima che lo sviluppo di un computer quantistico che possa compromettere sistemi tipo RSA 2048 sono ancora lontani più di un decennio (National Academies of Sciences, Engineering, and Medicine 2019). Le implicazioni di un simile evento, anche se futuro, per la sicurezza nazionale, le comunicazioni civili e i dati memorizzati restano, comunque, significative. Molti sistemi e processi, come le firme digitali, le comunicazioni il commercio elettronico e l'identità digitale, si basano su meccanismi che diventerebbero vulnerabili qualora la crittografia asimmetrica diventasse violabile. Ogni industria e settore sarebbero colpite, ponendo enormi problemi per i governi che proteggono i segreti di Stato così come per le aziende responsabili della protezione dei dati dei clienti e degli utenti. Ci vogliono decenni per sviluppare una crittografia resistente ai quanti e per passare a un nuovo protocollo di sicurezza. Poiché i tempi sia per lo sviluppo dei computer quantistici che per la mitigazione delle minacce quantistiche sono ugualmente lunghi e incerti, è fondamentale attribuire priorità allo sviluppo, alla standardizzazione e alla diffusione di una crittografia resistente ai quanti in modo da essere preparati per il momento in cui il potenziale teorico dei computer quantistici diventerà una realtà. Il Quantum Computing non pone solo minacce ai sistemi crittografici a chiave pubblica, ma offre anche opportunità che possono aiutare a ridurre le minacce alla cybersicurezza. Ad esempio, i progressi nel Machine Learning possono ridurre drasticamente il profilo della minaccia e migliorare la latenza nella riduzione della vulnerabilità. Inoltre, i miglioramenti negli algoritmi legati alla ricerca operativa possono portare a metodi più veloci di aggiornamento, riparazione e verifica che a loro volta possono ridurre le finestre di attacco.

La corsa ai quanti è pericolosa, poiché non tutti i casi d'uso contribuiranno positivamente alla soluzione dei grandi problemi. Come per tutte le tecnologie emergenti (Baccarella et al. 2020), anche l'informatica quantistica ha il suo lato oscuro. Nelle mani sbagliate, la pura potenza dei quanti può causare problemi altrettanto grandi quanto ne può risolvere. Le innovazioni attuali e le raccomandazioni implicite per garantire la sicurezza dello Stato nazionale possono essere così riassunte.

• Anti-malware quantistico Ricercatori hanno sviluppato soluzioni utilizzando il framework open source Qiskit (https://qiskit.org/) come base per lo sviluppo di programmi per computer quantistici che possono essere estesi con funzioni antivirus e di pattern matching (Deshpande et al. 2022), oltre a implementare protocolli che si avvicinano ai classici utilizzati nei sistemi militari. Reti di comunicazione quantistica saranno soggette ad attacchi di hacker, produttori di virus e altri malintenzionati. Gli attacchi prenderanno di mira porte logiche quantistiche, stati quantistici e algoritmi quantistici. Rispetto all'elaborazione dell'informazione classica, esistono più modi per attaccare l'elaborazione dell'informazione quantistica,

ed ICINN

perché a causa della sovrapposizione, gli stati quantistici contengono più condizioni concomitanti (più gradi di libertà) rispetto alle loro controparti classiche. Si presume che la correzione degli errori quantistici non sia sufficiente a rilevare il malware quantistico, poiché è stata progettata per gestire piccoli errori. Facchi et al. (Facchi et al. 2018) hanno introdotto il concetto di malware quantistico. Questo si può presentare sotto forma di porta logica quantistica o come un intero algoritmo quantistico progettato e controllato dagli aggressori. La caratteristica fondamentale del malware quantistico è di essere composto da un linguaggio macchina quantistico che codifica le porte logiche e le misure quantistiche. Un importante vettore di attacco per il malware quantistico è quello di sfruttare il protocollo probabilistico per l'autenticazione dei messaggi quantistici, la rete virtuale privata quantistica sicura, che presuppone che il mittente e il destinatario non siano soggetti ad attacchi da parte di terzi almeno durante l'invio e la misurazione degli stati quantistici. L'aspetto quantistico di questo protocollo preserva l'entanglement attraverso la rete. Una soluzione per migliorare la robustezza delle informazioni quantistiche memorizzate è la codifica di ogni qubit di dati in un codice quantistico di rilevamento degli errori. Ciò consente l'applicazione della tolleranza ai guasti quantistici e permette ai difensori di verificare se i dati sono stati modificati, attraverso l'uso del rilevamento degli errori quantistici.

• Rilevamento quantistico delle botnet Scienziati del Ministero federale tedesco per gli Affari economici e l'energia hanno finanziato il lavoro di un modello ibrido di deep learning quantistico classico per il rilevamento di botnet (Herr et al. 2021). L'intelligenza artificiale quantistica e l'apprendimento automatico quantistico sono componenti fondamentali dell'apprendimento profondo quantistico ibrido per fornire sicurezza informatica per il rilevamento delle botnet. I risultati della ricerca hanno rivelato che il modello di deep learning quantistico ha ottenuto risultati più rapidi rispetto al modello classico: l'accuratezza ha raggiunto il 94,7% (n=100) e il 93,9% (n=1.000). L'obiettivo dell'utilizzo di un computer quantistico nel generatore è che si propone di campionare i computer quantistici in modo più efficiente dalle distribuzioni classiche, caricando ed elaborando grandi quantità di dati ad alta dimensionalità.

• Scambi di chiavi quantistiche Attualmente, il protocollo quantistico più robusto e diffuso è il Quantum Key Distribution (QKD), che utilizza i concetti del principio di indeterminazione di Heisenberg e del teorema di non-clonazione per consentire a due parti di comunicare in modo sicuro su un canale non sicuro. Le chiavi quantistiche vengono codificate bit per bit su singoli fotoni e trasmesse come flusso di fotoni attraverso un canale quantistico, come la fibra ottica o lo spazio libero. Un hacker che cerchi di intercettare il flusso di fotoni nel collegamento quantistico non avrà successo in quanto qualsiasi interruzione o modifica dei fotoni altera lo stato codificato del fotone, causando un errore rilevabile. Utilizzando l'entanglement e la sovrapposizione quantistica, il mittente e il destinatario possono creare un sistema per rilevare le intercettazioni sul canale quantistico. In base al livello di errore causato dall'intercettazione, le due parti possono determinare se la chiave è stata compromessa. In tal caso, il mittente e il destinatario possono interrompere la comunicazione. L'unico ostacolo principale della QKD è che la trasmissione di fotoni è limitata a circa 60 miglia, per cui è necessario creare una rete di nodi fidati per consentire la condivisione delle chiavi su lunghe distanze e con più utenti. La più grande rete QKD è attualmente distribuita in Cina, con un'estensione di 4600 km e un collegamento tra le città di Shanghai, Hefei, Jinan e Pechino e un collegamento satellitare di 2600 km tra due osservatori spaziali (Vance 2022).

• Firewall quantistici È stato sviluppato un firewall virtuale basato sui quanti, utilizzando i componenti quViCE (Quantum Virtual Computing Environment) e quC (Quantum Converter) per fornire risorse quantistiche per architettare un firewall software e per convertire i bit in quBit e i quBit in bit (Vance 2022). Il problema principale che un Firewall quantistico cerca di risolvere riguarda il traffico di rete virtuale (Amellal et al. 2015). In molte reti virtuali, quando molte macchine virtuali sono collegate, a causa di congestioni nel traffico di rete si creano ritardi consistenti nello svolgimento di operazioni. Il firewall virtuale quantistico consente 223 di gestire la sicurezza della rete dell'infrastruttura virtuale in base alle macchine virtuali, definendo le regole del traffico di rete e rafforzando la sicurezza dell'ambiente di calcolo virtuale quantistico. Il firewall utilizza una tecnica a regole ad albero, che filtra i pacchetti in modo simile a un albero in base ai loro attributi, come l'indirizzo IP e i protocolli. Il vantaggio proposto dal firewall virtuale quantistico è che consente di controllare l'utilizzo della larghezza di banda di ciascuna macchina virtuale nell'infrastruttura, evitando un utilizzo eccessivo e la negazione del servizio alle applicazioni critiche a causa dell'incoerenza quantistica o del problema del rumore quantistico. La soluzione introduce la pseudo-telepatia quantistica come proprietà di alcuni giochi che consente strategie vincenti solo ai giocatori in grado di utilizzare informazioni quantistiche (Brassard et al. 2015).

Le tecnologie emergenti sviluppate per uso commerciale vengono sempre più spesso proposte per la difesa creando ulteriori sfide normative. La protezione degli interessi degli Stati nazionali dipende da un'adeguata governance dello sviluppo per evitare che vengano sfruttate vulnerabilità non intenzionali.

Nonostante le recenti raccomandazioni di esperti di difesa e ricercatori, gli Stati nazionali devono affrontare la prospettiva di armare l'informatica quantistica e limitare l'esportazione di aspetti chiave della tecnologia. La ricerca per proporre nuove regole normative può aiutare a meglio governare le sfide inerenti alle applicazioni del calcolo quantistico, e a controllare efficacemente le potenziali minacce delle nuove tecnologie purché da ciò non ne risulti un soffocamento dell'innovazione e degli investimenti per la ricerca.

computer quantistici | quantistico

Articoli correlati

L'Europa non potrà fare la transizione verde senza la Cina. Parola di Olanda

By Redazione Start Magazine

Hinton (ex-Google) ha ragione sul pericolo dell'intelligenza artificiale?

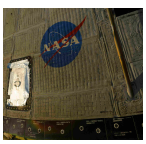
By Luca Sambucci

Il boom dell'Ia generativa sta facendo la fortuna di Nvidia, Broadcom e non solo

By Marco Orioles

Ci saranno davvero regole comuni fra Ue e gli Usa sull'intelligenza artificiale?

By Carlo Terzano



Ecco che cosa ha rivelato la Nasa sugli Ufo

By Chiara Rossi

Le peripezie della Corea del Nord sui satelliti spia

By Chiara Rossi

Il debutto di ChatGpt in Parlamento (in veste di senatore)

By Giulia Alfieri

Ita Airways e Inps. Ecco dove l'innovazione digitale deve ancora decollare

By Claudio Trezzano

Chip, perché Tsmc e Asml non invidiano Nvidia

By Marco Dell'Aguzzo

La disinformazione non è più affare di Twitter (in Europa, per ora)

By Giulia Alfieri

Share This

Tweet | Share | Share | Email

GENERAL DATA PROTECTION REGULATION UE 2016/679 INFORMATIVA SUL TRATTAMENTO DATI PERSONALI (articolo 13)