L'HUFFINGTON POST

Trump accelera sul supercomputer quantistico: un nuovo fronte aperto con la Cina

LINK: https://www.huffingtonpost.it/economia/2026/06/23/news/trump_ordini_esecutivi_quantum-22196476/

Trump accelera sul supercomputer quantistico: un nuovo fronte aperto con la Cina La firma su due ordini esecutivi del presidente per indicarlo come priorità di sicurezza nazionale e fissare due scadenze al 2028 e al 2031. Sullo sfondo la corsa contro Pechino e una minaccia che gli esperti ipotizzano da trent'anni: il Q-Day, ovvero il giorno della vulnerabilità totale. L'analisi di Simone Montangero (Università di Padova) di Adele Sarno 2026-06-23T16:06 La firma su due ordini esecutivi del presidente per indicarlo come priorità di sicurezza nazionale e fissare due scadenze al 2028 e al 2031. Sullo sfondo la corsa contro Pechino e una minaccia che gli esperti ipotizzano da trent'anni: il Q-Day, ovvero il giorno della vulnerabilità totale. L'analisi di Simone Montangero (Università di Padova) Mentre Donald Trump firmava due nuovi ordini esecutivi sul quantum computing nello Studio Ovale, accanto a lui sedevano i vertici di Ibm e Google. Una scena che racconta più delle firme. Per anni il computer quantistico, ossia quello che sfrutta le leggi della fisica quantistica per fare calcoli impossibili alle macchine tradizionali, è rimasto confinato nei laboratori universitari e nei centri di ricerca. Oggi entra ufficialmente nella strategia industriale e geopolitica degli Stati Uniti. Dopo semiconduttori, intelligenza artificiale e spazio, Washington apre un nuovo fronte tecnologico e, come già accaduto con l'intelligenza artificiale, lo trasforma in una priorità di sicurezza nazionale. Sullo sfondo c'è sempre la sfida con la Cina di Xi Jinping. Il timore non è soltanto restare indietro, ma lasciare a Pechino il vantaggio in una tecnologia destinata ad avere ricadute sulla ricerca scientifica, sulla difesa, sulla cybersicurezza. Nessuno sa quando arriverà il primo computer quantistico davvero rivoluzionario. Ma negli Stati Uniti nessuno vuole che sia la Cina ad arrivarci per prima. Gli ordini esecutivi di Trump puntano a sviluppare entro il 2028 un computer quantistico capace di affrontare problemi che oggi richiederebbero anni anche ai supercomputer più avanzati. Per farlo, secondo il Wall Street Journal, la Casa Bianca vuole coinvolgere agenzie federali, università e aziende private per trasformare il quantum da promessa scientifica a strumento con applicazioni concrete, dalla scoperta di nuovi farmaci alla simulazione di fenomeni fisici complessi. Una parte importante del piano riguarda però la difesa. Trump ha incaricato i dipartimenti del Commercio e della Difesa di sviluppare entro cinque anni sensori quantistici che possano affiancare o sostituire il Gps, una capacità decisiva

nei conflitti in cui il segnale satellitare viene disturbato o bloccato. C'è poi un secondo obiettivo. Gli stessi computer quantistici potrebbero un giorno mettere in crisi i sistemi di crittografia che proteggono reti governative, infrastrutture critiche e comunicazioni riservate. Per questo il secondo ordine esecutivo accelera il passaggio a nuovi standard di sicurezza informatica progettati per resistere agli attacchi quantistici entro il 2031. A prima vista potrebbe sembrare una questione per fisici e laboratori universitari. In realtà riguarda medicina, energia, difesa, cybersicurezza e intelligence. Ed è proprio per questo che gli Stati Uniti considerano il quantum una tecnologia strategica al pari dell'intelligenza artificiale e dei semiconduttori. "Il quantum sta uscendo dalla ricerca universitaria e sta entrando nella geopolitica", spiega Simone Montangero, professore di Fisica teorica all'Università di Padova e autore, insieme a Giuliano Benenti e Giulio Casati, di Il computer impossibile (Raffaello Cortina) . Il motivo è che governi e specialisti conoscono da decenni un potenziale rischio: un computer quantistico sufficientemente potente potrebbe aggirare molti dei sistemi che oggi proteggono dati e comunicazioni. "Sappiamo da trent'anni che se avessimo avuto i computer quantistici avremmo potuto rompere la crittografia che tiene in piedi il nostro mondo", osserva Montangero. Tradotto: conti correnti, comunicazioni diplomatiche, segreti militari, reti energetiche e altre infrastrutture strategiche potrebbero diventare vulnerabili. Quando paghiamo con una carta di credito, consultiamo il conto online, inviamo un'email o inseriamo una password, diamo per scontato che nessun altro possa leggere quei dati. Questa sicurezza si basa sulla crittografia, cioè su sistemi matematici che rendono le informazioni incomprensibili a chi non possiede la chiave giusta. Gli esperti di sicurezza hanno persino un nome per il momento in cui questo equilibrio potrebbe saltare: Q-Day, il giorno in cui un computer quantistico riuscirà a spezzare gli attuali sistemi crittografici. Nessuno sa quando arriverà. Ma è proprio questa incertezza che sta spingendo governi e aziende a prepararsi con anni di anticipo. Per capire il problema bisogna entrare, almeno per un momento, nel cuore della crittografia moderna. E Montangero ci aiuta a farlo: "L'algoritmo RSA si basa sulla fattorizzazione di due numeri. Prendo due numeri primi di duemila cifre e ne faccio il prodotto. Trovare i due numeri originari, partendo solo dal prodotto, col miglior supercalcolatore che c'è al mondo richiederebbe 20.000 anni". Per capire meglio: l'idea è simile a quella delle tabelline. Sapere che 3 per 7 fa 21 è immediato. Fare il percorso inverso è difficile: partendo da 21 bisogna capire quali numeri lo hanno generato. "Con numeri piccoli è facile. Con numeri lunghi migliaia di cifre diventa un problema praticamente impossibile da risolvere. È proprio su questa difficoltà che si basa la sicurezza digitale moderna. Quando usiamo una carta di credito, inseriamo una password o inviamo una comunicazione riservata, stiamo sfruttando un sistema che funziona perché i computer tradizionali impiegherebbero tempi enormi per trovare quella chiave". Finché questi problemi matematici restano troppo complessi da risolvere, la sicurezza regge. Ma un computer quantistico sufficientemente potente cambierebbe le regole del gioco: "Il primo che ha un computer quantistico abbastanza potente prende e legge

tutto quello che c'è. A quel punto non ci possiamo più fidare del sistema bancario, di internet, delle comunicazioni protette. Per ora una macchina del genere non esiste. Ma non è più considerata fantascienza. Per questo governi, banche e aziende stanno già iniziando a sostituire gli attuali sistemi di sicurezza con nuove forme di crittografia progettate per resistere anche all'era quantistica. Magari succederà fra dieci anni, magari fra trenta", conclude Montangero. Non è un caso che Trump abbia dichiarato: "Investiremo nella leadership americana nel quantum come mai prima d'ora" È anche per questo che la data del 2028 scelta da Trump non sembra casuale. Poche settimane prima della firma degli ordini esecutivi, QuEra Computing, spin off dei laboratori di Harvard e MIT, ha annunciato Libra, un computer quantistico con correzione degli errori che, secondo la roadmap presentata insieme ad Amazon Web Services, dovrebbe essere disponibile via cloud entro il 2028. Se le promesse verranno mantenute, aziende, università e governi potranno accedere da remoto a una macchina progettata per affrontare calcoli oggi ai limiti dei supercomputer tradizionali. Anche l'altra data fissata dalla Casa Bianca, il 2031, guarda allo stesso problema da una prospettiva opposta. Nessuno sa quando arriverà il cosiddetto Q-Day, il momento in cui un computer quantistico riuscirà davvero a spezzare la crittografia attuale. Ma sostituire i sistemi di sicurezza di banche, ospedali, ministeri, reti energetiche e infrastrutture critiche richiede anni di lavoro. E Trump non vuole farsi trovare impreparato perché sullo sfondo c'è la Cina. Nessuno sa con precisione quanto siano avanti i laboratori di Pechino, ma secondo Montangero sarebbe un errore sottovalutarli. "Non possiamo escludere che domani ci mostrino risultati al livello dei migliori risultati occidentali". Il timore americano è semplice: se il primo grande salto nel quantum dovesse arrivare dalla Cina, Pechino potrebbe ottenere un vantaggio nella ricerca scientifica, nella cybersicurezza e nelle applicazioni militari. C'è poi una minaccia che i servizi di intelligence considerano già concreta. Si chiama harvest now, decrypt later: intercettare oggi comunicazioni cifrate che non possono ancora essere lette, conservarle e decifrarle in futuro quando i computer quantistici saranno abbastanza potenti. "Pensiamo alle comunicazioni delle ambasciate", spiega Montangero. "Magari oggi non riesco a leggerle, ma posso archiviarle e riprovarci fra cinque o dieci anni". È anche per questo che la scadenza del 2031 non appare lontana come potrebbe sembrare. Quando il Q-Day arriverà, potrebbe essere troppo tardi per iniziare a prepararsi. Qualche parlamentare protesta, ma gli Stati membri (Germania in primis) vogliono aumentare i rimpatri della comunità afghana e hanno dato mandato alla Commissione di negoziare. Salvo poi escludere che si tratti di un riconoscimento del regime di Kabul. Un portavoce talebano dice che si è parlato anche di riavvio dei servizi consolari e di ripristino della fiducia reciproca