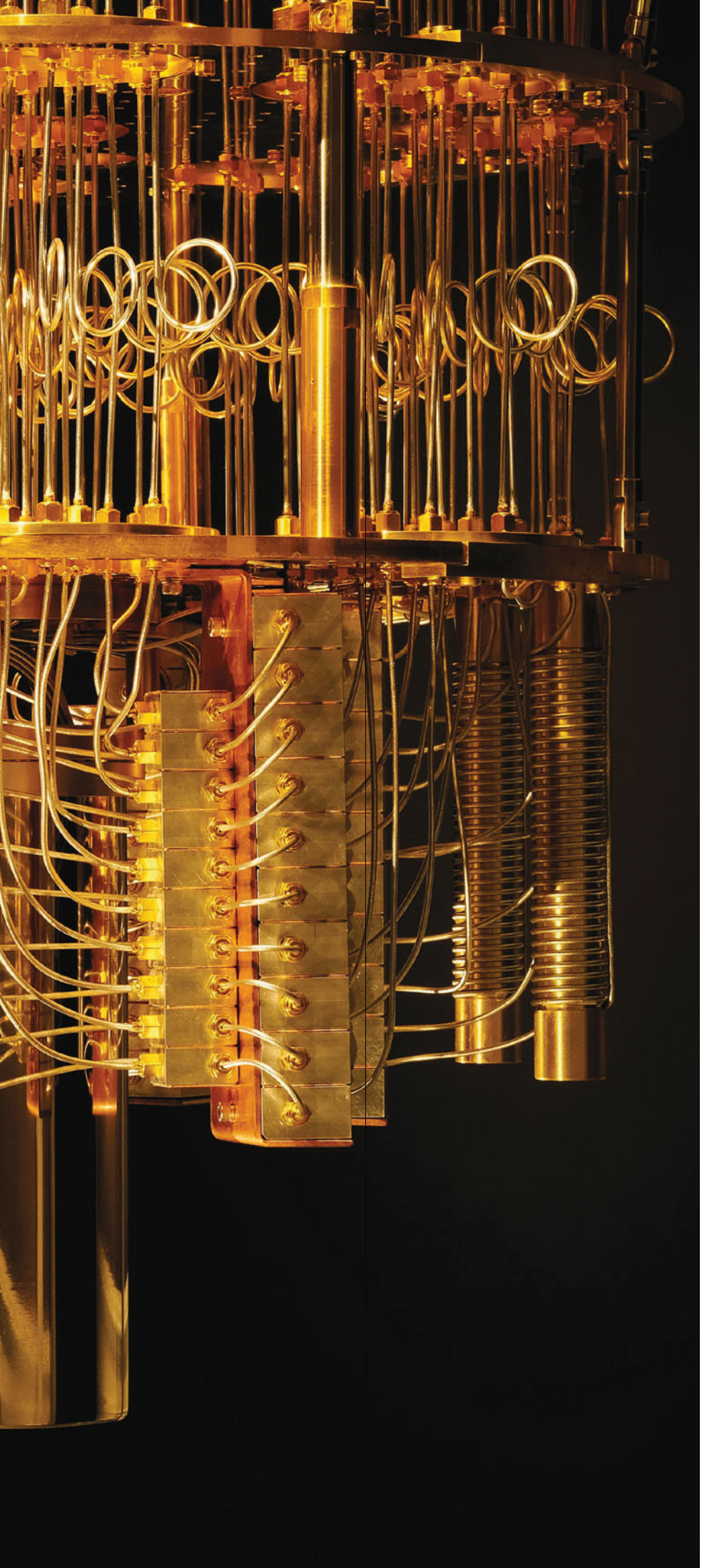
TIME

O SALTO QUÂNTICO

Como a computação quântica – "a nova fronteira da Humanidade" – irá transformar o mundo e criar uma "corrida espacial" no século XXI

— **POR CHARLIE CAMPBELL,** YORKTOWN HEIGHTS, NOVA IORQUE



GRAHAM CARLOW

U

Um dos segredos para se construir o computador mais potente do mundo está provavelmente em cima do lavatório da sua casa de banho. No Watson Research Center da IBM, no condado de Westchester, estado de Nova Iorque, os cientistas têm sempre à mão uma caixa de fio dental – Reach é a sua marca preferida –, caso precisem de utilizar os computadores quânticos, do tamanho de um bidão de óleo, o mais recente dos quais é milhões de vezes mais rápido a concluir certas tarefas do que um portátil.

No interior do contentor, metálico e brilhante, do System One da IBM, resguardado pelo mesmo tipo de vidro que protege a *Mona Lisa* [no Museu do Louvre], há três cilindros de circunferência decrescente, semelhantes a um conjunto de matrioscas. Todos juntos encerram um candelabro de fios de prata que descem, em cascata, através de grossas placas de ouro e chegam a um *chip* quântico na base.

Para funcionar corretamente, este *chip* exige um superarrefecimento de 0,015 kelvins – um pouquinho acima do zero absoluto e ainda mais frio do que o Espaço sideral. A maioria dos materiais tem tendência a contrair ou a quebrar quando sujeito ao frio intenso, mas é extraordinário como o fio dental mantém a sua integridade quando é necessário prender os fios mais rebeldes. "Só funcionam, porém, os fios sem cera e sem sabor; caso contrário, os vapores que libertam estragam tudo", esclarece Jay Gambetta, vice-presidente do departamento quântico da IBM. É curioso que um objeto caseiro seja usado numa tecnologia definida para transformar praticamente tudo.

A capacidade única de a Mecânica Quântica [a parte da Física que estuda

as partículas atómicas e subatómicas] processar pilhas de dados já está a otimizar rotas de milhares de camiões-cisterna que atravessam o mundo, bem como a ajudar a decidir que pacientes nas unidades de cuidados intensivos requerem uma assistência mais urgente e a imitar processos químicos de nível atómico para projetar melhor novos materiais.

Também promete reforçar o poder da Inteligência Artificial para aperfeiçoar os algoritmos capazes de, finalmente, tornar em realidade veículos sem condutor e drones que podem ser usados como táxis. As simulações de Inteligência Artificial quântica exibem "um grau de aptidão e de eficácia que é inimaginável", diz à *Time* Chris Inglis, diretor do Departamento de Cibersegurança Nacional [responsável por aconselhar o Presidente dos EUA sobre matérias de cibersegurança].

Os primeiros utilizadores da Mecânica Quântica são empresas que gerem ativos – para as quais a incorporação de cálculos quânticos envolve poucos custos indiretos –, mas outras companhias com fins comerciais também não se ficam atrás. A espanhola Multiverse Computing executou com sucesso projetos-piloto para clientes multinacionais, como a BASF e a Bosch, demonstrando como os seus algoritmos quânticos podem duplicar os lucros nas trocas comerciais em moeda estrangeira e detetar quase quatro vezes mais defeitos na linha de produção.

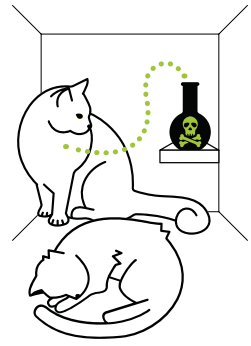
"Os algoritmos quânticos da Aprendizagem Profunda [que usa redes neurais artificiais para permitir que computadores respondam, por exemplo, a texto, voz e imagem mais depressa e com mais precisão do que os humanos] são completamente diferentes dos algoritmos clássicos", indica Enrique Lizaso Olmos, CEO da Multiverse. "É possível torná-los mais rápidos e capazes de tentar novas estratégias; são também muito melhores no que toca a obter a correlação realmente importante em muitos dados."

Colossos como a Google, a Amazon ou o Alibaba – sem mencionar Estados que disputam a supremacia tecnológica – estão numa corrida para dominarem este espaço. Prevê-se que a indústria global de computação quântica deverá crescer dos $413 milhões [cerca de €388 milhões] em 2020 para $8,6 mil milhões [pouco mais de €8 mil milhões] em 2027, segundo a International Data Corporation.

Enquanto os computadores tradicionais dependem de bits binários – dígitos que ligam ou desligam, conhecidos como "0" (zeros) e "1" (uns) – para processar informações, os qubits, que sustentam a computação quântica, são partículas subatómicas minúsculas que conseguem alcançar uma combinação simultânea dos dois estados, como uma moeda girando no ar.

A TEORIA

O austríaco Erwin Schrödinger (1887-1961), Prémio Nobel da Física, foi o criador do "Paradoxo do Gato": a famosa experiência mental que ilustra o princípio da incerteza no mundo quântico.



> Fecha-se um gato numa caixa com um frasco de veneno, uma fonte emissora de partículas radioativas alfa e um dispositivo composto por um detetor de radiações e um martelo. Se o detetor registar a presença de uma partícula, o martelo é acionado e quebra o frasco. As probabilidades são de 50/50.

> Segundo a mecânica quântica, o gato está vivo e morto – em ambos os estados – até ser observado. Só teremos a certeza de que ele está vivo ou morto se abrirmos a caixa, ou seja se interferirmos no resultado.

Os futuros computadores quânticos terão capacidade de abrir fronteiras até à data insondáveis para a Matemática e a Ciência

À BEIRA DE UMA REVOLUÇÃO

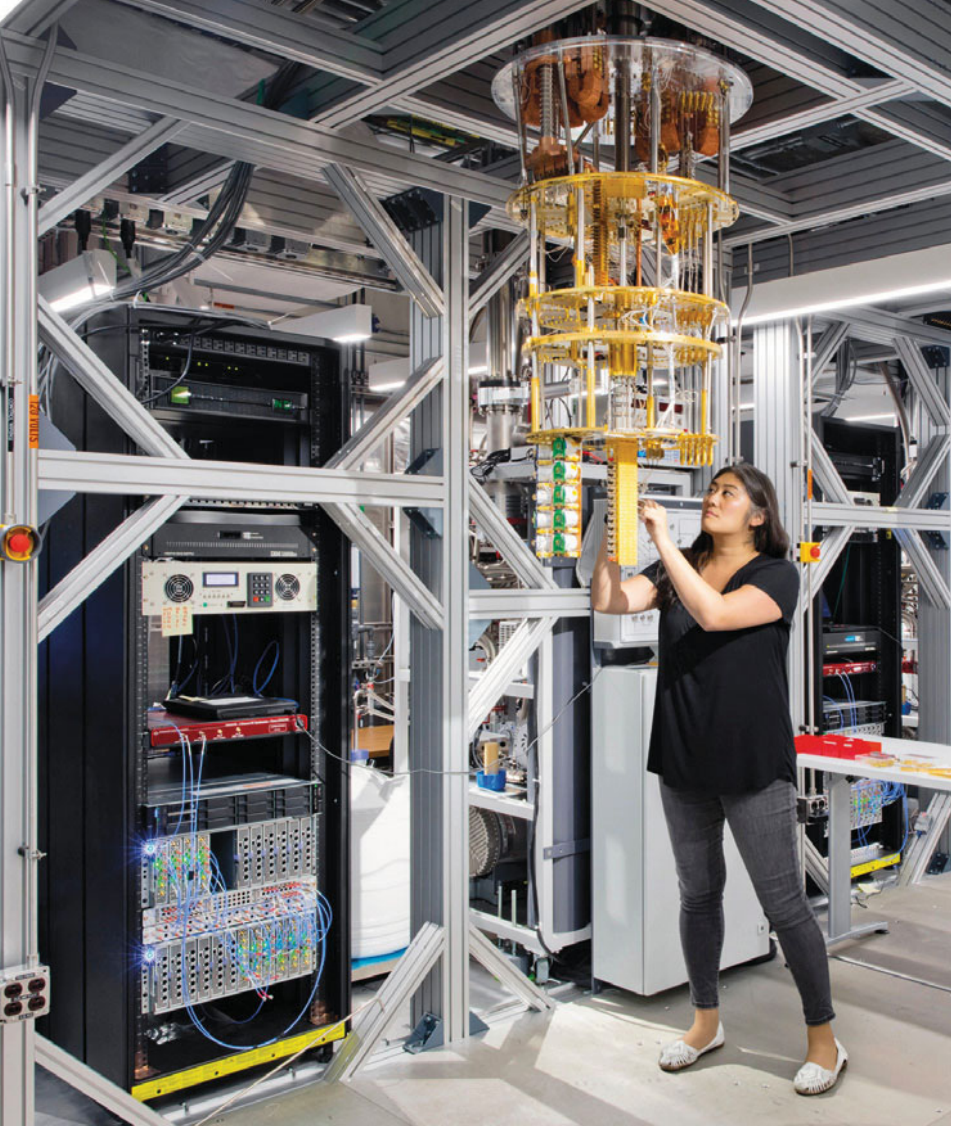
Este salto de um processamento dual para outro multivariado aumenta exponencialmente o poder da computação. Problemas complicados, que atualmente demoram vários anos a entender, poderão ser solucionados em apenas alguns segundos por um supercomputador mais robusto. Os futuros computadores quânticos terão capacidade de abrir fronteiras até à data insondáveis para a Matemática e a Ciência, ajudando a resolver desafios existenciais, como as alterações climáticas e a segurança alimentar.

Uma abundância de descobertas recentes e de investimentos estatais significa que estamos, atualmente, à beira de uma revolução quântica. "Acredito que, nos próximos cinco anos e em termos de inovação quântica, iremos mais longe do que fizemos nos últimos 30", salienta Jay Gambetta, da IBM.

No entanto, qualquer disruptor vem com risco, e os computadores quânticos são uma grande dor de cabeça para a segurança nacional. A sua capacidade de resolução de problemas irá em breve tornar obsoleta toda a criptografia existente, comprometendo as comunicações, as transações financeiras e até mesmo as defesas militares. "As pessoas descrevem a computação quântica como uma nova corrida espacial", observa Dan O'Shea, diretor de operações da *Inside Quantum Technology*, uma publicação exclusivamente dedicada a este setor.

Em outubro, o Presidente dos EUA, Joe Biden, visitou o centro de dados quânticos da IBM, em Poughkeepsie, Nova Iorque, considerando que a computação quântica é "vital para a [nossa] economia e igualmente importante para a [nossa] segurança nacional". Numa nova era de competição pelo poder, os EUA e a China estão particularmente empenhados em conquistar esta tecnologia e, assim, não perderem terreno vital.

"É a tecnologia da próxima revolução industrial", assegura Tony Uttley, presidente e diretor de operações da Quantinuum, empresa com sede no



CONNIE ZHOU

EUA à frente A liderança na computação quântica pertence à IBM, que possui mais de 60 computadores em funcionamento

Colorado, que oferece aplicações quânticas comerciais. "É como o advento da internet ou o início da computação clássica."

Na realidade, é surpreendente como a computação tradicional nos levou tão longe. Desde o inovador *Apple II*, do final dos anos 1970, até aos *smartphones* e supercomputadores de hoje, todos os processadores dividiam as tarefas num sistema binário. Mas a vida é muito complexa, e transmitir informações de maneira tão rudimentar é como dar um concerto de Rachmaninoff em código Morse.

A computação quântica também está mais em sintonia com a Natureza. Moléculas – os blocos de construção do universo – são conjuntos de átomos unidos entre si por eletrões, que, por seu turno, giram em redor do núcleo. A maneira como estes eletrões ocupam essencialmente dois estados ao mesmo tempo é o que as partículas quânticas replicam, apresentando aplicações para as ciências naturais e materiais, ao preverem, por exemplo, como medicamentos interagem com o corpo humano ou como se comportam determinadas substâncias sujeitas a corrosão. O fabrico tradicional progride com base em suposições, cálculos de tentativa e erro. Ao espelhar o mundo natural, a computação quântica permite que os avanços sejam propositadamente planeados.

As maiores empresas do mundo, e também centenas de *startups*, querem aproveitar a computação quântica, mas a liderança pertence à IBM – International Business Machines. A companhia possui mais de 60 computadores quânticos em funcionamento – mais do que o resto do mundo – e tem uma lista de parceiros, que inclui gigantes em praticamente todos os setores, da ExxonMobil à Sony.

É um regresso bem-vindo ao apogeu da tecnologia para uma empresa célebre, fundada, há mais de um século, para produzir cartões perfurados [mas também relógios, balanças e até máquinas de cortar queijo, antes de contribuir para a invenção da internet]. Nos últimos anos, a IBM havia ficado atrás de rivais como a Apple e a Microsoft, por ter falhado em relação à computação em nuvem e à Inteligência Artificial. Até certo ponto, a computação quântica representa uma redenção. "É ótimo estar de volta ao topo", rejubila um executivo. "Não é segredo que deixámos as coisas escaparem, quando não saltámos para a nuvem."

À PROCURA DA PERFEIÇÃO

Em novembro de 2022, a IBM revelou o seu novo *chip*, Osprey, de 433 qubits – o processador quântico mais potente do mundo, cuja velocidade, se representada em bits tradicionais, excederia em muito o número de átomos do universo conhecido. A IBM tem mais de 20 computadores quânticos disponíveis no seu Qiskit, um *kit* de ferramentas quânticas de código aberto, até ao momento com mais de 450 mil downloads. Para construir uma indústria de base quântica, algumas máquinas são de acesso gratuito, mas os clientes que pagam, como startups ou académicos, têm à sua disposição, por via remota e em regime de aluguer, outras mais possantes.

A IBM tem um projeto ousado para lançar um processador de 1 121 qubits, neste ano, e, até 2025, ultrapassar os 4 mil qubits, criando circuitos quânticos modelares que ligam vários *chips* de processadores num mesmo computador. "A modularidade é um grande ponto de inflexão", refere Dario Gil, vice-presidente e diretor de investigação da IBM. "Agora, já temos maneira de projetar máquinas que terão dezenas de milhares de qubits." É, pois, ilimitado o uso industrial da computação quântica.

Na sede da BMW, em Munique, há uma parede que dá noites sem dormir aos engenheiros que projetam estes automóveis. Criar do zero um novo modelo demora pelo menos quatro anos. Primeiro, os técnicos usam uma ferramenta de computador para esboçarem um exterior que combine beleza e viabilidade. Em seguida, é esculpido em argila um modelo à escala real e colocado num túnel de vento, para se avaliar a aerodinâmica. Após inúmeras decisões sobre o interior, segue-se o desempenho do motor, e assim por diante, até se chegar ao teste final: um protótipo que é conduzido a cerca de 60 km/hora e que embaterá naquela parede que tira o sono aos engenheiros – tudo para se testar a reação do carro num acidente Se este não satisfizer vários critérios de segurança, volta à prancha do designer.

É aqui que a computação quântica pode ajudar, prevendo com precisão o desempenho sob stresse de materiais

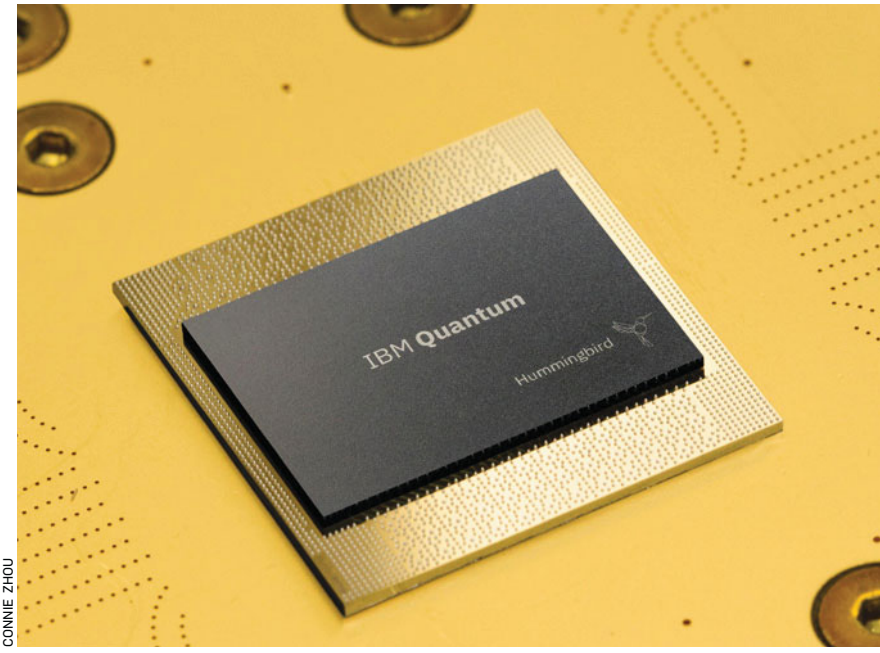
complexos com diferentes formas. "Se os testes que simulam a colisão forem mais consistentes, pode-se economizar até seis meses em todo o processo", anota Carsten Sapia, vice-presidente para a estratégia, direção e segurança de investigação e tecnologia do grupo BMW, associado da empresa quântica francesa Pasqal. "A computação quântica também nos ajudará a encontrar o modelo perfeito, no que respeita ao *design*, ao máximo espaço interior e a uma melhor aerodinâmica."

Isto é só o início. Os negócios modernos estão cheios de problemas de otimização, ideais para os algoritmos quânticos, capazes de economizar tempo, energia e recursos. "Não estamos apenas a construir tecnologia, temos também de permitir que a força de trabalho a use", explica Katie Pizzolato, diretora de estratégia quântica e investigação de aplicações na IBM.

Carsten Sapia, da BMW, está convencido de que é fácil dar vários usos à tecnologia quântica: o desafio está em garantir que todas as divisões do grupo serão capazes de a utilizar. O construtor alemão enfrenta dificuldades em comunicar com a China, a partir da Europa, para garantir a manutenção e a monitorização do software de direção das suas viaturas, devido às restrições cada vez mais apertadas na transferência de dados entre fronteiras. "No futuro, contaremos com a tecnologia quântica em todos os lugares do mundo para administrar os nossos negócios", confia Sapia. "Mas como podemos configurá-la para que, aconteça o que acontecer a uma escala geopolítica, ainda tenhamos acesso a essa tecnologia?"

EUA VS. CHINA

Nos últimos anos, a computação quântica deixou de ser uma nota de rodapé e conquistou o lugar cimeiro da agenda da segurança global. Por enquanto, há 17 países já com estratégias quânticas nacionais e outros quatro em fase de desenvolvimento. A China investiu cerca de $25 mil milhões [€23,5 mil milhões] em investigação quântica, desde os anos 1980, segundo o *Quantum Computing Report*. O principal cientista chinês nesta área, Pan Jianwei, liderou o lançamento do primeiro satélite quântico do mundo, em 2016. Em 2021, o seu computador quântico de 56 qubits quebrou um recorde. O 14º Plano Quinquenal da China, publicado em março de 2021, estabelece o domínio da computação quântica como prioridade política. "A linha ténue entre indústria e segurança nacional na China dá-lhe uma vantagem", reconhece David Spirk, antigo diretor de dados do Departamento de Defesa dos EUA.



CONNIE ZHOU

Competição com a China Em novembro de 2022, a IBM revelou o seu novo *chip*, Osprey, de 433 qubits – o processador quântico mais potente do mundo

A resposta da Casa Branca chegou em maio de 2021, com um Memorando de Segurança Nacional, ordenando a todas as agências federais norte-americanas que se procedesse à transição para a segurança pós-quântica, devido aos "riscos significativos para a segurança económica e nacional".

Dado que a atualização das infraestruturas críticas pode demorar décadas e que, literalmente, tudo o que se encontra ligado à internet está em risco, é urgente agir agora. "Sabemos que, embora a computação quântica seja maravilhosa para a Humanidade, a primeira coisa que as pessoas farão é militarizá-la", realça Skip Sanzeri, fundador e diretor de operações da QuSecure, uma empresa de cibersegurança pós-quântica, contratada pelas Forças Armadas e governos federais dos EUA para empreender o que, diz ele, poderá a ser uma modernização dos sistemas atuais no valor de um bilião de dólares [€94 mil milhões].

Os mecanismos modernos da guerra assentam na velocidade. O computador mais rápido será uma arma decisiva

Ainda assim, temendo que os EUA corram o risco de ficar para trás, David Spirk pede uma aposta na computação quântica semelhante ao Projeto Manhattan [que permitiu o fabrico das primeiras bombas nucleares, entre 1942 e 1947]. Segundo o Fórum Económico Mundial, dos mais de $30 mil milhões [€28 mil milhões] gastos globalmente no ano passado, o investimento da China representou cerca de metade e o da União Europeia quase um quarto. A U.S. National Quantum Initiative só desembolsou $1 200 milhões [menos de €1 130 milhões] – um montante que Spirk descreve como "trivial" quando comparado com a despesa total dos EUA na Defesa: um bilião de dólares. "Não estamos à espera de uma vaga – ela já está aqui", alerta.

As apostas não podiam ser mais elevadas. Hoje, praticamente toda a cibersegurança – quer se trate de mensagens no WhatsApp, quer de transferências bancárias quer de "apertos de mão digitais" [a autenticação da comunicação entre dois dispositivos através de assinaturas digitais] – tem como base o RSA, um algoritmo de criptografia assimétrica, de chave pública e não secreta, usado para a transmissão segura de dados. Se um computador

CONNIE ZHOU

normal precisa de milhares de milhões de anos para decifrar o RSA, um computador quântico faz isso em apenas algumas horas. Num artigo publicado em dezembro último (cujas conclusões geraram um aceso debate), uma equipa de cientistas da China afirma que um algoritmo quântico é capaz de descodificar o RSA com um computador de 372 qubits.

Nos EUA, a corrida agora passa por se criar segurança pós-quântica – uma tarefa que cabe ao U.S. National Institute of Standards and Technology (NIST). Em 2016, este instituto anunciou um concurso para programadores de novos algoritmos de criptografia pós-quântica. Os resultados foram mistos: um dos finalistas anunciados, em 5 de julho de 2022, apresentou uma cifra considerada muito segura, mas, em pouco mais de uma hora, alguém tentou quebrá-la com um computador normal.

Até certa medida, já é tarde demais. Embora computadores quânticos suficientemente potentes para decifrar o RSA possam estar abertamente disponíveis dentro de poucos anos, piratas informáticos já estão a apoderar-se de dados confidenciais e a armazená-los, sabendo que, muito em breve, a eles poderão ter acesso através de computadores quânticos. "Não haverá plano de recuperação se deixarmos passar os dias sem conseguirmos um protocolo de segurança quântica", avisa Dario Gil, vice-presidente da IBM.

GRANDE DOSE DE FÉ

A guerra na Ucrânia também serviu de alerta. Foi o primeiro grande conflito da História que começou com ataques cibernéticos, quando redes de comunicações e de infraestruturas vitais se tornaram alvos da Rússia, determinada a estabelecer bases militares da invasão. Serviços públicos, redes de energia, *media*, bancos, empresas e organizações sem fins lucrativos foram submetidos a um *cyber blitzkrieg*, com impacto na distribuição de medicamentos, alimentos e outros bens de emergência.

Os mecanismos modernos da guerra e da segurança nacional assentam na velocidade e na precisão na tomada de decisões. "Se o nosso computador for mais rápido do que o deles, ganhamos nós – é muito simples", comenta David Spirk, do Departamento de Defesa norte-americano. "A computação quântica é o próximo salto."

Intenções malignas não são o único perigo. Com os EUA envolvidos numa nova "guerra fria", também não se sabe se a China e a Rússia estariam dispostas a adotar os novos protocolos do NIST, sobretudo porque, no passado, a criptografia RSA terá sido violada pela Agência de Segurança Nacional dos Estados Unidos da América (NSA).

Em setembro de 2022, Jack Sullivan, o conselheiro de Segurança Nacional da administração Biden, admitiu que a computação quântica terá "uma importância descomunal na próxima década", acrescentando que o controlo das exportações pode ser usado para manter a vantagem dos EUA.

Sistemas de segurança pós-quânticos concorrentes nas esferas de influência de Washington e de Pequim têm o potencial de dividir o mundo em blocos divergentes, com graves consequências para o comércio global. "A balcanização do que conhecemos hoje como uma internet livre e aberta é claramente possível", admitiu Chris Inglis, diretor de Cibersegurança Nacional que aconselha o Presidente dos EUA.

A preocupação em relação à computação quântica não resulta apenas dos riscos para a segurança. Confiamos nos computadores clássicos, em parte porque podemos verificar os seus cálculos com papel e uma caneta. Porém, os computadores quânticos envolvem uma física tão misteriosa e lidam com problemas tão complexos que é extremamente difícil fazer-se uma verificação convencional.

Por enquanto, é possível simular muitos cálculos quânticos num supercomputador tradicional e apurar o resultado. Só que chegará um momento em que confiar num computador quântico exigirá uma grande dose de fé. "Consolidarmos a confiança em todo o ecossistema é muito importante", destaca Tony Uttley, o presidente da Quantinuum.

A Boeing, por exemplo, está a colaborar com a equipa quântica da IBM, desde 2020, no projeto de novos materiais para a próxima geração de aeronaves. Todavia, tendo em conta grandes riscos para a sua reputação, a empresa não tem pressa. "As ferramentas de modelagem que usamos para desenhar os nossos aviões são controladas bem de perto", informa Jay Lowell, engenheiro-chefe de tecnologia disruptiva na Boeing. "Transformar a computação quântica num código operacional é um enorme, enorme obstáculo."

E é um obstáculo que a IBM conhece muito bem. No entanto, com os seus computadores quânticos de código aberto, oferecendo acesso a académicos e a empresários, a empresa espera mitigar a hesitação – ou, como diz o vice-presidente, Dario Gil: "Esta é uma nova fronteira da Humanidade."

— Com Leslie Dickstein

TIME
© 2023, TIME Inc. Todos os direitos reservados.
Traduzido da TIME Magazine
e publicado com autorização da TIME Inc.