

EMILY EDWARDS, JOHN QUANTUM INSTITUTE (JQI)

Forscher reihen Atomrümpfe aneinander wie auf einer Kette und steuern sie mit Strahlungspulsen. Die Quantenobjekte werden so zu Informationsträgern. In Quantencomputern ermöglichen es die Eigenschaften dieser »Qubits«, manche Rechnungen in Rekordzeit auszuführen.

PHYSIK

QUANTENTECHNOLOGIEN

VOR DEM GROSSEN SPRUNG

Weltweit investieren Staaten und Unternehmen in die Entwicklung futuristischer Technologien auf Basis der Quantenphysik. Nun startet auch in Europa ein groß angelegtes Forschungsprogramm, das die letzten Hürden beseitigen soll.



Tommaso Calarco (links) ist Professor am Institut für Komplexe Quantensysteme der Universität Ulm, wo er Kontrolltechniken für Vielteilchen-Quantensysteme entwickelt, um Quantentechnologien effizienter zu machen. Er ist seit über einer Dekade maßgeblich an der Koordinierung der Europäischen Quantentechnologie-Gemeinschaft beteiligt und gilt als einer der gedanklichen Väter des Quanten-Flaggschiffs der EU. **Max Riedel** ist promovierter Quantenphysiker und Senior Consultant für Universitätsbeziehungen bei der Siemens AG. Seit Januar 2017 ist er an die Universität Ulm als Projektmanager für Europäische Aktivitäten delegiert und unterstützt dort Tommaso Calarco bei der Vorbereitung des Quanten-Flaggschiffs.

» spektrum.de/artikel/1561160

► An einem warmen Sommerabend des Jahres 1998 hielt eine schwere, schwarze Limousine vor den Pforten des Instituts für Experimentalphysik der Universität Innsbruck. Und obwohl das Institut zu den führenden der Welt auf seinem Gebiet zählt und prominenten Besuch durchaus gewöhnt ist, war dieser Gast ein ganz besonderer: Der 14. Dalai Lama wollte mit eigenen Augen einen der Grundbausteine des Universums sehen. Wie die meisten von uns hatte er in der Schule gelernt, dass Physiker seit Anfang des 20. Jahrhunderts Atome und Lichtquanten (so genannte Photonen) mit Hilfe der Quantentheorie beschreiben. Allerdings hatten es die Gründerväter der modernen Physik für unmöglich gehalten, einzelne Atome zu fangen, direkt sichtbar zu machen oder gar gezielt zu verändern.

Doch genau dies war den Innsbrucker Experimentalphysikern um Rainer Blatt gelungen. In ihrem Labor hielten sie mitten in einer Ultrahochvakuumkammer und mit Hilfe elektrischer Felder ein einzelnes Barium-Ion in der Schwebe. Die Innsbrucker Forscher beschossen diesen Atomrumpf mit grünem Laserlicht, welches das Ion ständig in alle Richtungen streute, ähnlich einem Staubkorn im Sonnenschein. Beobachtern zeigte sich der schwebende Materiebaustein also als winziger grüner Punkt.

Und mehr noch: die Experimentatoren brachten das Ion wiederholt in eine Überlagerung – auch Superposition genannt (siehe »Superposition und Verschränkung«, S. 15) – aus zwei quantenmechanischen Zuständen: einem, in dem das Ion das Laserlicht des Abbildungsstrahls streut und

damit sichtbar ist, und einem, in dem es das Abbildungslicht nicht streut und damit unsichtbar bleibt. Das Besondere an einer solchen Superposition ist, dass das Ion bis zum Zeitpunkt der Messung, wenn also der Abbildungs-laser angeschaltet wird, quasi in beiden Zuständen »gleichzeitig« verharrt. Erst bei dem Kontakt mit den Photonen des Lasers entscheidet es sich, welchen der beiden es einnimmt – viele Leser kennen wahrscheinlich Schrödin-

AUF EINEN BLICK DIE ZWEITE QUANTENREVOLUTION

- 1** Physiker können Quantenobjekte mittlerweile gezielt steuern. Damit rücken neuartige Sensoren, Netzwerke und Computer in Reichweite.
- 2** Weltweit fließen seit einigen Jahren große Beträge in diese Quantentechnologien. Nun hat auch die Europäische Union ein ambitioniertes Forschungsprogramm gestartet, das »Quanten-Flaggschiff«.
- 3** Noch müssen Forscher viele wissenschaftliche und technologische Probleme lösen. Gelingt dies, könnte die Quantenphysik in den nächsten Jahrzehnten zahlreiche Branchen revolutionieren.

gers Katze als Analogon zum beschriebenen Phänomen. Anhand des zufällig blinkenden Ions konnte der Dalai Lama hier also Zeuge einer der wichtigsten, aber unintuitivsten Eigenschaften der Quantenwelt werden.

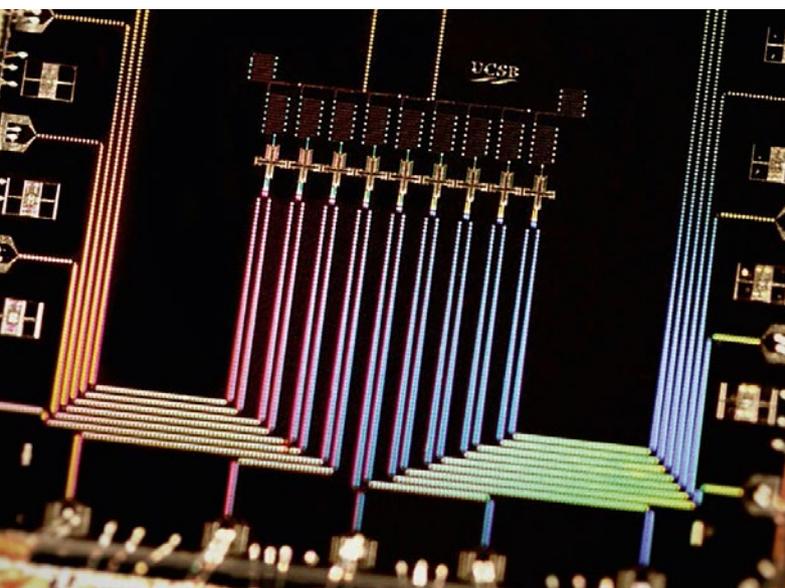
Was der berühmte Geistliche für eine philosophische Laborspielerei gehalten haben mag, ist 20 Jahre später Grundlage eines ambitionierten Großforschungsprojekts der Europäischen Union: Von 2018 an fördert sie die Quantenforschung mit 500 Millionen Euro; noch einmal der gleiche Betrag soll während der zehnjährigen Laufzeit des Programms aus den Fördertöpfen der EU-Mitgliedsstaaten kommen. Wir waren maßgeblich daran beteiligt, dieses Projekt Wirklichkeit werden zu lassen und wollen hier die Vision hinter dem Projekt beschreiben.

Langfristig sollen durch das »Quanten-Flaggschiff«, an dem sich hunderte Forschungsgruppen aus ganz Europa beteiligen werden, Technologien entstehen, die auf der Superposition und anderen quantenphysikalischen Phänomenen des Mikrokosmos basieren. Unserer Einschätzung nach haben diese das Zeug dazu, unser Kommunikationswesen und andere Bereiche zu revolutionieren. Und jetzt ist aus unserer Sicht der Zeitpunkt gekommen, ihre Entwicklung im großen Stil zu fördern.

Natürlich gibt es bereits seit Jahrzehnten Technologien, die auf den Gesetzen der Quantenphysik basieren, beispielsweise Laser, Transistoren oder Atomuhren. Sie fußen jedoch darauf, dass wir große Gruppen von Lichtteilchen, Elektronen oder Atomen steuern. Mittlerweile aber können Wissenschaftler die Quanteneffekte einzelner Quantenobjekte kontrollieren – aus Sicht vieler Experten gleicht dies einer »zweiten Quantenrevolution«.

Wer gezielt einzelne Atome und Lichtquanten verändert, kann über völlig neue Anwendungen nachdenken, beispielsweise ultraempfindliche Quantensensoren für

Der Kalifornier John Martinis platzierte 2015 neun supraleitende Qubits auf einem Mikrochip und bereitete damit die Entwicklung größerer Quantencomputer vor.



Magnetfelder und andere Messgrößen. Auch könnten abhörsichere Netzwerke auf Basis einzelner Photonen zum neuen Standard digitaler Kommunikation werden. Und Quantencomputer sowie Quantensimulatoren eröffnen in vielen Bereichen neue Perspektiven, von der Materialforschung über die Verkehrsflusssteuerung bis hin zur künstlichen Intelligenz (siehe **Spektrum** November 2015, S. 78).

Neben der bereits erwähnten Superposition nutzen Quantenwissenschaftler vor allem das Phänomen der Verschränkung aus. Bei ihr korrelieren die Zustände zweier Teilchen miteinander, auch wenn diese weit voneinander entfernt sind. Die vielleicht spektakulärste Anwendung der Verschränkung ist die so genannte Quantenteleportation, die im Jahr 1997 der Innsbrucker Arbeitsgruppe um Anton Zeilinger erstmals gelang. Anders als in der Fernsehserie »Star Trek« wird hierbei nicht Materie übertragen, sondern ein quantenphysikalischer Zustand. Eine Datenübertragung mit Überlichtgeschwindigkeit durch Quantenteleportation ist ausgeschlossen, auch wenn man dies immer wieder liest. Nichtsdestotrotz hat sie enormes Anwendungspotenzial in der Kommunikationstechnik – mehr dazu später.

Alte Technologien weiterentwickeln, neue erfinden

Superposition und Verschränkung widersprechen mit ihrer starken Zufallskomponente dem gesunden Menschenverstand so sehr, dass Albert Einstein sie anzweifelte und den berühmten Ausspruch »Gott würfeln nicht!« prägte. Er glaubte, dass wir die Gesetze, denen die Welt im kleinsten folgt, einfach noch nicht genau kennen und es »verborgene Variable« geben müsse, mit deren Hilfe man den scheinbaren Zufall doch berechnen könnte. Niels Bohr hielt dagegen und soll geantwortet haben, dass wir Gott nicht vorschreiben könnten, wie er die Welt zu lenken hat. Es sollte viele Jahre dauern, bis der Disput (zumindest nach der Überzeugung der allermeisten Physiker) gelöst war. 2015 – mehr als 80 Jahre nach Einsteins und Bohrs Streit – zeigten drei Experimente, so genannte »schlupflochfreie« Bell-Tests, in Delft, Wien und Boulder unabhängig voneinander, dass es keine verborgene Variablen geben kann. Damit bewiesen sie endgültig die Vollständigkeit der Quantentheorie: Gott würfeln doch!

Wie diese Beispiele zeigen, haben wir heute eine unglaublich gute Kontrolle über einzelne Quanten. Im Rahmen der zweiten Quantenrevolution wollen wir diese Kontrolle nun außerhalb des Labors nutzbar machen. Daneben wollen wir aber auch bestehende Quantentechnologien weiterentwickeln. Ein Beispiel hierfür sind die hochgenauen Atomuhren, die bereits an Bord von Navigationssatelliten im Einsatz sind. Mit ihrer Hilfe bestimmt man die Position des Empfängers durch den Vergleich der Laufzeit von Signalen von mindestens vier verschiedenen Satelliten. Dazu ist es nötig, dass die Uhren in allen Satelliten die exakt gleiche Zeit (bis auf wenige milliardstel Sekunden) zeigen.

Atomuhren nutzen aus, dass alle Atome einer Sorte (auf GPS-Satelliten verwendet man unter anderem Zäsium und Rubidium) die exakt gleiche Elektronenkonfiguration haben. Eines der Elektronen wird von seinem natürlichen

Grundzustand in einen energetisch höheren Zustand angeregt, indem es ein Photon einer ganz bestimmten Energie und damit einer ganz bestimmten Frequenz absorbiert. In einer Atomuhr misst man diese Frequenz extrem genau und nutzt so die Atome gewissermaßen als Uhrenpendel. Die besten heutigen Atomuhren sind so präzise, dass sie weniger als eine Sekunde falsch gehen würden, wenn man sie zur Geburt des Universums vor 13,8 Milliarden Jahren angeschaltet hätte. Damit ist die Zeit die mit Abstand am genauesten bestimmbare Messgröße.

Streng genommen ist die Energiedifferenz zwischen Grundzustand und angeregtem Zustand nur für einzelne, vollkommen isolierte Atome konstant. Äußere Einflüsse, wie etwa elektromagnetische Felder, können die Energieniveaus der Zustände und damit auch die Übergangsfrequenz beeinflussen. Atomuhren werden daher aufwändig abgeschirmt, und es werden spezielle Paare von Elektronenkonfigurationen gewählt, die möglichst unempfindlich gegen Störungen sind.

Für Quantensensoren dreht man den Spieß um: Man wählt Zustandspaare, deren Energieniveaus stark von äußeren Einflüssen wie beispielsweise Magnetfeldern abhängen. Eine Änderung des Felds wird dadurch in eine Änderung der Uhrenfrequenz konvertiert, die Forscher wiederum hochpräzise messen können. Für Quantensensoren kommen neben Atomen eine Vielzahl anderer Quantensysteme zum Einsatz, zum Beispiel so genannte NV-Zentren in Diamant (bei denen im Diamantgitter ein Kohlenstoffatom durch ein Stickstoffatom und eine Fehlstelle ersetzt ist), supraleitende Schaltkreise oder sogar mechanische Nanostrukturen.

Die Anwendungsgebiete für diese Technologie sind vielfältig. Quanten-Magnetfeldsensoren ermöglichen schon heute die so genannte Magnetoenzephalografie, mit der sich die Gehirnaktivität messen lässt. Die Sensoren verwenden so genannte SQUIDs (Superconducting Quantum Interference Devices), die jedoch aufwändig mit flüssigem Helium auf wenige Kelvin über dem absoluten Nullpunkt gekühlt werden müssen. Künftige Exemplare sollen auch bei Raumtemperatur funktionieren und damit weitaus kompakter, energieeffizienter und kostengünstiger sein. Möglicherweise wird man sie sogar als Mensch-Maschine-Schnittstelle einsetzen können: Eine Reihe kompakter Sensoren, eingearbeitet in einer Haube, würde dann bestimmte zuvor eintrainierte Gehirnstrommuster erkennen und diese Signale über Funk an technische Geräte (von der Spielekonsole bis zum Rollstuhl) weitergeben.

So genannte Quanten-Inertialsensoren könnten hingegen zur satellitenunabhängigen Navigation eingesetzt werden, die wichtig für die Sicherheit von Schiff- und Luftfahrt ist. Diese Variante der Technologie beruht auf dem Prinzip des Welle-Teilchen-Dualismus und kehrt die Rolle von Licht und Materie im Vergleich zu einem normalen Interferometer um: Eine fallende Atomwolke wird mit Hilfe eines Laserstrahls in Superposition aus Grund- und angeregtem Zustand gebracht. Letzterer erhält durch die Absorption des Lasers einen kleinen Stoß senkrecht zur Fallrichtung, so dass die beiden Zustände unterschiedliche Wege im Raum zurücklegen.

Superposition und Verschränkung

Quantenobjekte befinden sich oft in einer Überlagerung mehrerer Zustände, Physiker sprechen von Superposition. Bei einem Photon überlagern sich beispielsweise die Polarisierungsrichtungen des Lichtfelds, nennen wir sie hier H und V (für horizontal und vertikal). Das Besondere einer Superposition dieser beiden Zustände ist, dass sich die Natur erst bei einer Messung für einen der beiden Zustände entscheidet, und zwar völlig zufällig. Bis dahin existieren sie gewissermaßen gleichzeitig. Das Konzept der Superposition kann man auch auf mehrere Teilchen ausweiten und spricht dann von Verschränkung – die beiden Begriffe führen häufig zu Verwirrung, beschreiben sie im Kern doch dasselbe Phänomen. Verschränkt man beispielsweise zwei Photonen 1 und 2 miteinander in einer Superposition $H_1H_2 + V_1V_2$, so wird man bei einer Messung entweder beide horizontal polarisiert (H_1H_2) oder vertikal polarisiert (V_1V_2) finden, niemals jedoch in zwei unterschiedlichen Zuständen (alternativ könnte man natürlich auch eine antikorrelierte Verschränkung $H_1V_2 + V_1H_2$ präparieren und würde dann die beiden Lichtteilchen immer in unterschiedlichen Zuständen finden). Dem Experimentator ist es unmöglich vorauszusagen, welches der beiden Messergebnisse eintritt. Sogar wenn man die Messungen exakt gleichzeitig an weit entfernten Orten durchführt und damit ausschließt, dass eine Messung die andere beeinflusst haben kann (da dies eine Wechselwirkung mit Überlichtgeschwindigkeit benötigen würde, was laut Relativitätstheorie nicht möglich ist), hat dieses Ergebnis Bestand.

Ein weiterer Strahl sorgt dafür, dass sich die Atomwolken wieder aufeinander zubewegen, und ein dritter bringt die beiden Zustände schließlich zur Interferenz. Letztlich misst man die Population der beiden Zustände in der Atomwolke und kann aus dem Verhältnis zum Beispiel bestimmen, inwieweit sich das Gesamtsystem während des Versuchs gedreht hat. Eine dritte Variante, so genannte Quanten-Gravitationssensoren, messen direkt die Beschleunigung der jeweiligen Zustände. So können sie sehr präzise die Masseverteilungen unter der Erdoberfläche abbilden, was für Firmen interessant ist, die Bauvorhaben planen oder nach Rohstoffen suchen.

Die nächste Generation von Quantensensoren könnte übrigens nicht nur das Prinzip der Superposition, sondern auch das der Verschränkung ausnutzen. Was damit möglich ist, zeigt der Physiknobelpreis 2017, der für die Entdeckung von Gravitationswellen an drei Physiker des LIGO-Observatoriums vergeben wurde: Gravitationswellendetektoren wie LIGO können ihre enorme Sensitivität weiter



PICTURE ALLIANCE / PHOTOSHOT

Mit Hilfe des chinesischen Quantensatelliten »Micius« (oben) übertrugen Forscher um Jian-Wei Pan 2017 einen Verschlüsselungskode nach Österreich, um ein quantengesichertes Telefonat mit Anton Zeilinger (rechts) zu führen.

steigern, wenn sie verschränkte Photonen verwenden (»gequetschtes Licht«). Bei den Geräten handelt es sich um riesige optische Interferometer, die winzige Längenänderungen eines ihrer Arme messen. Werden die Detektoren mit »klassischem« Licht betrieben, so ist die Auslesegenauigkeit durch das so genannte Schrotrauschen beschränkt. Es geht darauf zurück, dass die Photonen unabhängig voneinander das Interferometer durchlaufen und es zu statistisch bedingten Schwankungen an den Lichtdetektoren kommt – die Anzahl der Photonen zu einem bestimmten Zeitpunkt streut gewissermaßen wie das Geschoss einer Schrotflinte. Aus diesem Grund wird LIGO mit extrem starken Lasern betrieben, die das Verhältnis von Signal zu Rauschen maximieren. In der Praxis ist die maximale Lichtleistung aber zum Beispiel durch die Erwärmung der Spiegel begrenzt. Der deutsche Detektor GEO600, an dem seit Jahrzehnten Technologie für LIGO entwickelt wird, verwendet daher bereits nicht-klassisches Licht, bei dem die Photonen paarweise miteinander verschränkt sind, wodurch die Lichtstärke weniger stark streut. Denn die Photonen sind nicht mehr völlig unabhängig unterwegs, sondern sie wissen gewissermaßen über den Weg eines Nachbarn Bescheid, was das Rauschen mit heutiger Technik um mehr als das Zehnfache reduzieren kann.

Das Quanten-Flaggschiff soll auch Fortschritte in einem anderen Bereich der Quantentechnologien bringen. Wie das zufällig morsende Dalai-Lama-Ion zeigt, messen wir ein Teilchen, das sich in Superposition zweier Zustände befindet, immer nur in genau einem der beiden Zustände – wir können jedoch nicht voraussagen, in welchem. Nach der Messung befindet sich das Teilchen in einem eindeutig definierten Zustand, die Superposition wird durch die Messung aufgehoben. Man kann einen Superpositionszustand also nie kopieren, ohne das Original zu zerstören. Dieses No-Cloning-Prinzip macht sich die Quantenkommunikation, genauer die Verteilung von Quantenschlüsseln (englisch: Quantum Key Distribution, QKD) zu Nutze. Sie stellt einen abhörsicheren Austausch von Nachrichten und Daten in Aussicht (siehe **Spektrum** August 2016, S. 64).



ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN (ÖAWI)

Um das zu verstehen, stellen wir uns zunächst vor, dass Anna mit ihrer Freundin Barbara chatten will. Möchte Anna eine geheime, quantenkodierte Botschaft an Barbara senden, schickt sie ihr zunächst über einen Quantenkanal einen zufälligen digitalen Schlüssel, kodiert in der Polarisation (der Schwingungsrichtung) einzelner Photonen, die etwa durch ein Glasfaserkabel zu ihr gelangen. Der Trick ist, dass Anna zufällig die Photonen entweder horizontal/vertikal oder diagonal links/diagonal rechts polarisiert und sie dies Barbara zunächst nicht mitteilt – sie benötigt also zwei Zufallsgeneratoren, einen für die Bitfolge des Schlüssels (0 oder 1) und einen für die Wahl der Polarisationsbasis. Schaltet sich nun Barbaras eifersüchtiger Exfreund Ernst dazwischen, um die Schlüsselübertragung aus Nullen und Einsen abzuhören, muss er die Polarisationsbasis erraten und wird wegen des No-Cloning-Prinzips die Zeichenkette verändern, denn der Abhörvorgang stellt ja eine Messung dar.

Anna und Barbara können den Lauschangriff erkennen, indem sie nach der Schlüsselübertragung eine gewöhnliche, also abhörbare Leitung verwenden: Zunächst teilt Anna Barbara die Wahl der Polarisationsbasis mit, und

beide verwenden nur die Schlüsselbits, bei denen beide zufällig die gleiche Basis gewählt haben. Dann vergleichen sie einige Bits des von Barbara empfangenen mit dem von Anna gesendeten Schlüssel: Wenn sie Unterschiede feststellen, wissen sie, dass jemand mitgehört hat. Wenn die Stichproben gleich sind, können sie (mit einer gewissen Wahrscheinlichkeit) davon ausgehen, dass niemand gelauscht hat und den Schlüssel dazu verwenden, ihre Daten zu verschlüsseln und über eine klassische Leitung zu übertragen.

Was nach Sciencefiction klingt, kann man bereits seit rund zehn Jahren kaufen. Der Weltmarktführer ist ein Schweizer Unternehmen, das 2001 von vier Wissenschaftlern der Universität Genf gegründet wurde. Mittlerweile gibt es unseres Wissens weltweit eine Hand voll Firmen, die entsprechende Systeme anbieten. Inzwischen sind sogar Systeme erhältlich, die sich nahtlos in bestehende Kommunikationsnetzwerke integrieren lassen. Diese werden schon heute für sichere Kommunikation zwischen Datenzentren oder Finanzinstituten verwendet. Doch noch sind einige Hürden zu überwinden, die den breiten Einsatz dieser Technologie für alle Internetnutzer verhindern.

Insbesondere begrenzen Übertragungsverluste in den Glasfaserleitungen die Reichweite in der Praxis auf ein paar hundert Kilometer. Bei klassischer Telekommunikation werden Verluste durch optische Verstärker aus einer Photodiode und einem Laser ausgeglichen. Sie müssen dafür jedoch das Signal messen, so dass die sichere Quantenverschlüsselung bei jeder Verstärkerstation unterbrochen wird. In Quantentechnologie-Laboren wird daher intensiv an »Quanten-Repeater« geforscht, mit denen sich die Reichweite der Verschränkung erweitern lässt, ohne den Superpositionszustand zu zerstören.

Hierzu ist zunächst die Übertragung der im Photon gespeicherten Quanteninformation in ein anderes System nötig, das letztlich ein neues Photon mit der gleichen Information aussendet. In den vergangenen Jahren wurden auf diesem Gebiet große Fortschritte erzielt. So hat etwa eine Forschergruppe um Hugues de Riedmatten vom Barcelona Institute of Science and Technology im Jahr 2017 den Quantenzustand einer ultrakalten Gaswolke mittels eines Photons in ein Festkörpersystem übertragen. Und Kollegen aus Delft haben im selben Jahr eine besonders robuste Form der Verschränkung zwischen zwei Stickstofffehlstellen in Diamanten hergestellt.

Große Erfolge hat auch die Volksrepublik China vorzuweisen. Sie hat Quantentechnologien zu einem strategischen Forschungsbereich in ihrem 13. Fünfjahresplan ernannt und zeigt, dass Quantenkommunikation im großen Maßstab heute schon machbar ist: Im September 2017 haben Regierungsvertreter und Wissenschaftler einen 2000 Kilometer langen faserbasierten QKD-Link zwischen Peking und Schanghai eingeweiht, der aus Teilstücken zwischen 32 vom Staat kontrollierten Knotenpunkten besteht.

Bereits im August 2016 hatte China den wissenschaftlichen Satelliten Micius in die Erdumlaufbahn geschossen, mit dem ein Team um Jian-Wei Pan Experimente zum Schlüsselaustausch im Weltall durchgeführt hat. Daneben

sind den Physikern damit Experimente zur Quantenteleportation über eine Entfernung von mehr als 1200 Kilometern geglückt, was einem neuen Weltrekord entspricht (siehe **Spektrum** August 2017, S. 8). Langfristiges Ziel ist es, ein Quantensatellitennetzwerk aufzubauen, das globale quantenverschlüsselte Kommunikation mit Hilfe von einzelnen verschränkten Photonen ermöglicht.

Allerdings: Aus Sicht vieler Cybersicherheitsexperten können die aktuellen Verschlüsselungsverfahren zwar eventuell gebrochen werden, stellen derzeit jedoch nicht das schwächste Glied in der Kette der sicheren Datenübertragung dar. Computerviren und Informationsweitergabe durch Personen sind weitaus größere Probleme. Zudem wird an alternativen mathematischen Algorithmen zur Verschlüsselung geforscht, die nur ein Software-Update der bestehenden Kommunikationsinfrastruktur, jedoch keine neue Hardware benötigen. Somit würden sie auch für die Verschlüsselung in Funknetzen funktionieren. Allerdings gibt es bei diesen Lösungen, »Post-Quantum Kryptographie« genannt, keine Garantie dafür, dass nicht doch einmal ein findiger Mathematiker eine Entschlüsselungsmethode entwickelt. Die QKD hingegen bietet Sicherheit, die auf fundamentalen Naturgesetzen basiert.

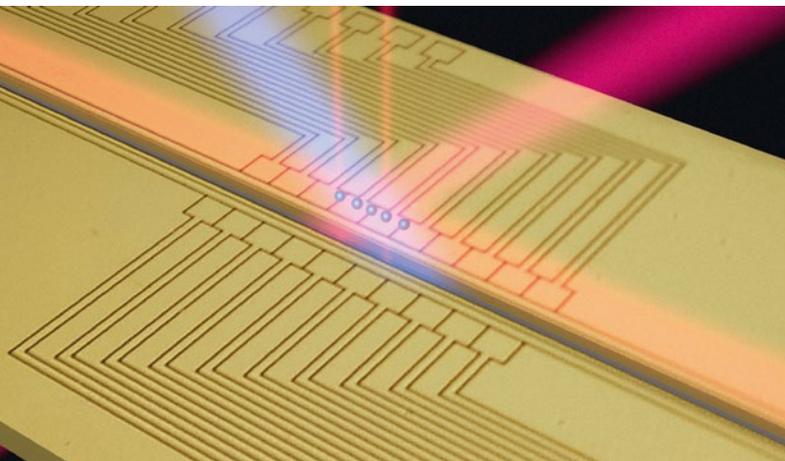
Die »Mondmission« des Projekts ist die Entwicklung eines vollwertigen Quantencomputers

Die bisher genannten Anwendungen werden sicher großen Einfluss auf die jeweiligen Anwendungsgebiete und Industriezweige haben. Die »Mondmission« der Quantentechnologien ist allerdings die Entwicklung von Quantencomputern. Sie versprechen bisher unvorstellbare Rechenleistung zum Lösen bestimmter Problemtypen und haben damit das Potenzial, viele verschiedene Bereiche unserer digitalisierten Gesellschaft zu transformieren.

Quantencomputer kodieren die Informationen nicht in klassischen Bits, die die Werte 0 oder 1 annehmen können, sondern in Qubits, die eine beliebige Superposition aus 0 und 1 annehmen können. Quantenalgorithmen verwenden neben klassischen Rechenoperationen wie Addition und logischen Verknüpfungen auch die Verschränkung zwischen verschiedenen Qubits. Daraus ergibt sich bei bestimmten Rechenaufgaben ein erheblicher Geschwindigkeitsvorteil.

1994 entwickelte der amerikanische Informatiker Peter Shor einen Quantencomputer-Algorithmus, der große Zahlen in ihre Primfaktoren zerlegen kann – und dies sehr viel schneller als alle bekannten klassischen Algorithmen. Die gängigen Verfahren, mit denen wir beispielsweise unsere E-Mails oder sichere Seiten im Netz verschlüsseln, beruhen darauf, dass es zwar leicht ist, zwei große Zahlen miteinander zu multiplizieren, aber sehr schwer, eine große Zahl in ihre Primfaktoren zu zerlegen. Mit heutigen Supercomputern betrüge die benötigte Rechenzeit zum Knacken der gängigen RSA-2048-Verschlüsselung daher mehrere Millionen Jahre. Ein ausreichend großer Quantencomputer, auf dem der Shor-Algorithmus läuft, könnte das Problem hingegen in wenigen Tagen lösen.

Dies erklärt, warum sich viele Regierungen für Quantencomputer interessieren. Allerdings sind inzwischen



RAINER BLATT, UDORN-INSBRUCK

Forscher um Rainer Blatt von der Universität Innsbruck nutzen Mikrochips, um aufgereichte Ionen gefangen zu halten und mit Laserlicht zu manipulieren.

weitere wichtige Anwendungsgebiete für Quantencomputer entstanden, die teilweise eine ähnliche Beschleunigung von Rechenoperationen in Aussicht stellen. Die Liste reicht vom Finden von Daten in unstrukturierten Listen, über die Optimierung von komplexen Systemen mit vielen Freiheitsgraden (etwa in der Lagerlogistik oder der Analyse von Verkehrsströmen), über die Berechnung von chemischen Systemen für die Chemie, Pharma- oder Materialforschung bis hin zu Anwendungen im maschinellen Lernen. Kein Wunder also, dass große IT-Firmen wie Google, IBM, Intel, Microsoft und Alibaba inzwischen viele Ressourcen in die Entwicklung eigener Quantencomputer und die entsprechende Softwareinfrastruktur stecken.

Dies wiederum weckt die Aufmerksamkeit von Risikokapitalgebern und vieler Firmen anderer Branchen, die Anwendungsfälle für ihr Unternehmen identifizieren wollen. Zudem verstärkt es das Engagement von Regierungen, die entsprechende Innovationsökosysteme in ihren Ländern schaffen wollen. Man kann dem Thema Quantencomputing somit eine gewisse Eigendynamik nicht absprechen. Manche sprechen sogar von einem Hype, bei dem sich zeigen muss, ob das große Interesse langfristig gerechtfertigt ist.

Andererseits lässt sich nicht von der Hand weisen, dass es in den vergangenen Jahren immense Fortschritte in der Entwicklung von Quantencomputern gegeben hat. Schaut man sich etwa die Entwicklung der Qubit-Anzahl von supraleitenden, auf Schaltkreisen basierenden Quantencomputern an, ist diese von 2 im Jahr 2009 über 5 im Jahr 2015 und 17 im Jahr 2017 auf mittlerweile 72 gestiegen. Allerdings gilt nach wie vor, dass noch immer viele Herausforderungen zu meistern sind, bis solche Geräte den Status von Prototypen hinter sich lassen können (siehe Artikel S. 22). Zum einen gibt es unterschiedliche physikalische Systeme, die für Quantencomputer in Frage kommen, mit unterschiedlichen Vor- und Nachteilen. Die momentan vielversprechendsten sind ultrakalte Ionen, bei denen die Qubits in atomaren Zuständen (ähnlich wie bei

atomaren Uhren) kodiert werden, und besagte supraleitende Schaltkreise, bei denen der Wert der Qubits der Flussrichtung eines Stroms entspricht.

Auf Letztere setzen die meisten zuvor genannten Firmen, und bei allen gibt es noch erheblichen Ingenieursaufwand, um die Systeme zu miniaturisieren, automatisieren, robuster zu machen und kostengünstiger zu fertigen. Die derzeit größten funktionierenden Quantencomputer bestehen aus rund 20 Ionen oder mehreren Dutzend supraleitenden Schaltkreisen. Diese Größenordnung galt lange als magische Schwelle, denn ab rund 50 Qubits sollten Quantencomputer mit heutigen klassischen Supercomputern nicht mehr ohne Weiteres simulierbar sein (siehe **Spektrum** Februar 2018, S. 62).

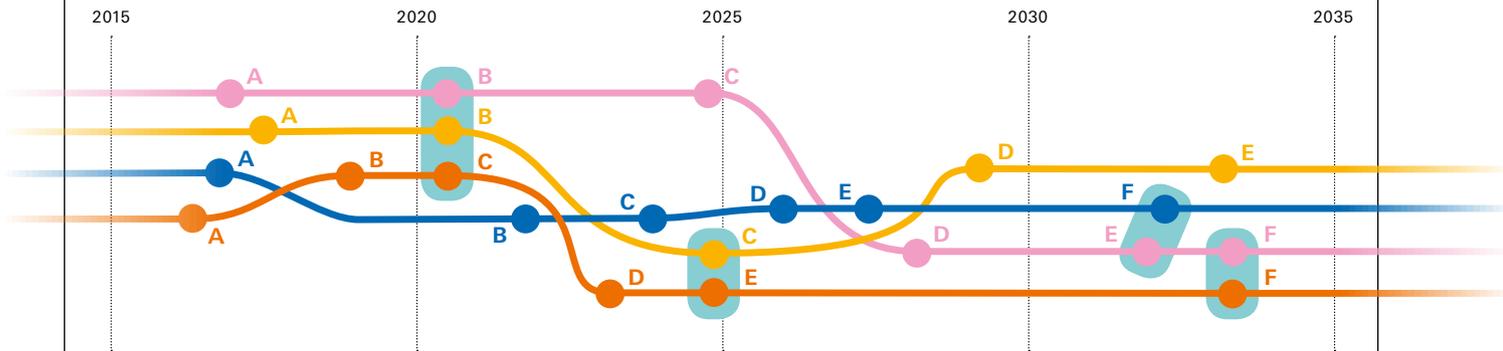
Zum anderen kämpfen Quantencomputer mit dem gleichen Problem wie Atomuhren: Überlagerungen und verschränkte Zustände reagieren extrem empfindlich auf äußere Einflüsse. Je mehr mikroskopische Bauteile man verschränkt, desto stärker schlägt dieser Dekohärenzeffekt zu Buche. Quantencomputer – basierend auf heutiger Technologie – sind daher in der Länge des zuverlässig abgearbeiteten Programms und der Anzahl der maximal koppelbaren Qubits Grenzen gesetzt. Zwar gibt es Quantenfehlerkorrekturverfahren, sie sind jedoch noch recht ineffizient. Theoretisch werden, je nach Hardwarefehler rate und Algorithmenlänge, Millionen bis Milliarden von physikalischen Qubits benötigt, um ein paar tausend fehlerkorrigierte logische Qubits zu erzeugen. Praktisch ist dies eine enorme Herausforderung. Es muss also noch weitere Durchbrüche in Forschung und Quanteningenieurwesen geben, bevor unsere derzeitige E-Mail-Verschlüsselung in Gefahr gerät. Es gibt allerdings bereits viel versprechende Ansätze, bestimmte Probleme auch mit kleineren, nicht fehlerkorrigierten Quantencomputern zu lösen, zum Teil in Kombination mit klassischen Supercomputern. Dies ist ein sehr aktives Forschungsgebiet mit viel Industriebeteiligung.

Quantensimulatoren für spezielle Aufgaben

Besonders interessant sind hier so genannte Quantensimulatoren. Vom physikalischen Aufbau her ähneln sie Quantencomputern, führen aber keine Algorithmen aus, die aus einer Aneinanderreihung logischer Verknüpfung von Qubits bestehen. Vielmehr wird die Wechselwirkung zwischen den Bausteinen so eingestellt, dass das Verhalten des Quantensimulators äquivalent zu dem eines viel komplexeren, nicht kontrollierbaren Quantensystems ist. Dies ist einem Windkanal ganz ähnlich, wo Parameter wie Luftdruck, Strömungsgeschwindigkeit und Modellgröße aufeinander abgestimmt werden, um etwa den Wiedereintritt eines Spaceshuttles in die Atmosphäre zu simulieren.

Will man Quantensysteme mit klassischen Computern nachstellen, wird oft der Speicherplatz zum Nadelöhr: Jeder zusätzliche Quantenspin, der simuliert werden soll, verdoppelt den benötigten klassischen Speicherplatz, und dieses exponentielle Wachstum übertrifft recht schnell selbst die Kapazität der größten Supercomputer (50 Spins benötigen etwa eine Million Gigabyte an Speicher). Quantensimulatoren haben dieses Problem nicht.

Meilensteine der Quantentechnologien – ein Zeitplan



1. Kommunikation

- A** Basistechnologie der Quanten-Repeater
- B** Sichere Datenübertragung zwischen zwei Quantenlinks
- C** Quantennetzwerke zwischen weit entfernten Städten
- D** Kreditkarten mit Quantenverschlüsselung
- E** Quanten-Repeater übertragen quantenverschlüsselte Informationen und geben Alarm bei Lausangriff.
- F** Europaweites Internet, das Quantentechnologie und klassische Kommunikationstechnik verwendet

2. Simulatoren

- A** Bewegung von Elektronen in Materialien können simuliert werden.
- B** Neue Algorithmen für Quantensimulatoren und Netzwerke
- C** Entwicklung neuartiger Materialien
- D** Anspruchsvolle Simulationen von magnetischen und elektrischen Quanteneffekten
- E** Simulation der Quantendynamik chemischer Reaktionen, Unterstützung des Designs neuer Arzneimittel

3. Sensoren

- A** Quantensensoren für Nischenanwendungen (z. B. Magnetfeldmessungen)
- B** Genauere Atomuhren zur Netzwerksynchronisation
- C** Quantensensoren in der Fertigungsindustrie
- D** Tragbare Quanten-Navigationsgeräte
- E** Quantensensoren erlauben die räumliche Abbildung des lokalen Gravitationsfelds
- F** Quantensensoren in der Unterhaltungselektronik und in Smartphones

4. Computer

- A** Einsatz eines logischen Qubits mit einfacher Fehlerkorrektur
- B** Entwicklung neuer Quantencomputer-Algorithmen
- C** Kleine Quantenprozessoren, die anwendungsrelevante Algorithmen ausführen
- D** Spezialisierte Quantencomputer mit mehr als 100 physischen Qubits, die Probleme aus Materialwissenschaft und Chemie lösen
- E** Verbindung von Quantenschaltkreisen mit klassischer Hardware bei niedrigen Temperaturen
- F** Allzweck-Quantencomputer, die klassische Computer bei manchen Anwendungen übertreffen

SPEKTRUM DER WISSENSCHAFT, NACH: QUANTUM MANIFESTO S. 8

In den vergangenen Jahren haben Wissenschaftler diese immer besser gemacht: So fangen sie heute routinemäßig mehrere hundert neutrale Atome in einem Gitter aus Licht ein und untersuchen damit Phasenübergänge oder topologische Effekte in Vielkörper-Quantensystemen. Auch der in den Medien viel zitierte »Quantencomputer« der kanadischen Firma D-Wave ist eine besondere Art von Quantensimulator, ein so genannter Quanten-Annealer. Langfristig versprechen sich Forscher von Quantensimulatoren eine Reihe von Durchbrüchen, unter anderem im Optimieren des energieintensiven Haber-Bosch-Verfahrens zur Düngerherstellung, das ein bis zwei Prozent des Weltenergiebedarfs benötigt, oder im Verständnis der Hochtemperatur-Supraleitung in komplexen Materialien.

Die Quantentechnologien bewegen sich momentan also rasant voran, und in den USA und China werden große Summen investiert. Aber was ist mit Europa? Tatsächlich sind hier im weltweiten Vergleich die meisten Quantenwissenschaftler tätig. Das ergibt zumindest eine Analyse der Fachveröffentlichungen zwischen 2013 und 2015. Ihr zufolge stammten 2455 Autoren aus der EU, aus China 1913 und aus Nordamerika 1564. Auch die Europäische Kommission investiert in den Bereich und hat die Quantenwissenschaft in den vergangenen 20 Jahren mit insgesamt 550 Millionen Euro gefördert.

Allerdings wird Grundlagenforschung in Europa seltener unter dem Blickwinkel einer möglichen Anwendbarkeit und späteren Kommerzialisierung betrachtet als etwa in

den Vereinigten Staaten. Im Bereich der Digitalisierung hat es Europa beispielsweise wiederholt versäumt, von selbst entwickelten technologischen Trends zu profitieren. Diesen Fehler sollten wir bei den Quantenwissenschaften nicht wiederholen.

So laufen bereits seit Jahren die Vorbereitungen für ein fokussiertes Forschungsprogramm, das auch als Starthilfe für die europäische Industrie in Sachen Quantentechnologien dienen soll. Dabei hat die Europäische Kommission immer wieder nicht nur Forschungsvorhaben, sondern auch so genannte Koordinierungs- und Unterstützungsprojekte gefördert. Dadurch hat sie die Zusammenarbeit innerhalb der interdisziplinären Forschergemeinschaft – neben Festkörper- und Atomphysikern arbeiten auch Chemiker, Informatiker, Ingenieure und Elektrotechniker an Quantentechnologien – unterstützt und eine gemeinsame Forschungsagenda gefördert.

Vorläufiger Höhepunkt dieser gemeinsamen Anstrengungen war die Veröffentlichung des »Quantum Manifesto«, das 2015/16 auf den Weg gebracht und letztlich von mehr als 3500 Mitgliedern der Quantenforscher-Gemeinschaft unterschrieben wurde. Darin haben wir den aktuellen Stand sowie die Chancen von Quantentechnologien auf allgemein verständliche Weise erklärt und die Europäische Kommission aufgefordert, ein strategisches Förderprogramm für Quantentechnologien zu initiieren.

Zudem verfassten Quantenforscher eine Reihe von Positionspapieren, unter anderem zur Perspektive der europäischen Industrie, die aus Sicht des für Technologie-Entwicklung zuständigen Generaldirektorats DG Connect eine wichtige Voraussetzung für die Förderung war. Gleichzeitig rührten gut vernetzte Kollegen, insbesondere aus den EU-13-Staaten, in ihren Heimatländern die Werbetrommel für Quantentechnologien. Und auch die Europäische Kommission fertigte unabhängige Berichte an.

Eine wichtige Rolle bei der Entstehung des Quanten-Flaggschiffs spielte sicherlich auch das Bewusstsein von großen Investitionen in anderen Ländern, neben den USA und China sind hier vor allem Kanada, Australien und Japan zu nennen. Die Überzeugungsarbeit trug Früchte: Im Rahmen einer großen Konferenz unter der niederländischen EU-Präsidentschaft im Mai 2016 kündigte die Kommission offiziell an, dass sie das Flaggschiff starten würde.

Sein Ziel ist, Europas Position an der Spitze der Forschung zu festigen und gleichzeitig als Region für Innovationen und Investitionen in die Quantentechnologien zu etablieren. Viele Ausgründungen aus europäischen Laboren sind bereits weltweit erfolgreiche Zulieferer, etwa für Lasersysteme, Elektronik oder Vakuum- und Kühlsysteme. Diese Position wollen wir weiter stärken und auch die Gründung von neuen Start-ups fördern. Darüber hinaus sollen Firmen aus anderen Industriezweigen befähigt und ermutigt werden, Quantentechnologien in Anwendungen zu überführen und auf den Markt zu bringen.

Ganz wesentlich hierfür sind aus unserer Sicht die Ausbildung und Förderung junger Wissenschaftler und Experten sowie die Weiterbildung von Berufstätigen. Gleichzeitig dient das Flaggschiff als Zugpferd, um ergänzende Förderprogramme sowie private Investitionen anzustoßen.

Einen solchen Effekt sehen wir bereits jetzt, zwei Jahre nach der offiziellen Verkündung des Projekts. Viele Mitgliedsstaaten der EU haben Quantentechnologie-Programme gestartet oder wollen dies in den kommenden Monaten tun. Auch außerhalb Europas wird das Flaggschiff als wichtiges Signal für den Fortschritt des Felds angesehen. Eine Rolle spielt dabei sicherlich, dass es nicht nur durch das Europäische »Forschungsministerium« DG Research getragen wird, sondern insbesondere auch durch DG Connect, das Europäische »Ministerium« für Digitalisierung und Kommunikation.

Bei der Umsetzung des Quanten-Flaggschiffs haben wir auch auf die Erfahrungen der beiden bereits vorher gestarteten Flaggschiff-Initiativen (Graphen-Flaggschiff und Human Brain Project) zurückgegriffen. So hat sich gezeigt, dass der Alleingang eines einzelnen Konsortiums zwar zielgerichtet sein kann, jedoch zu Uneinigkeit innerhalb der Community über die richtigen Ziele und – wie im Fall des Human Brain Projects – gar zu öffentlichem Protest führen kann (siehe **Spektrum** Februar 2016, S. 58). Kernprinzipien des Quanten-Flaggschiffs sind daher transparente Entscheidungen und das Einbeziehen aller Beteiligten. Wir sehen die Initiative also nicht als einzelnes Großprojekt, sondern als Förderprogramm mit übergreifender Forschungsagenda.

Insgesamt wird es aus vier Anwendungsbereichen bestehen: Quantensensorik und Metrologie, Quantenkommunikation, Quantencomputing und Quantensimulation (siehe »Meilensteine der Quantentechnologie – ein Zeitplan«, S. 19). Für jeden dieser Bereiche sind Ziele für drei, sechs und zehn Jahre definiert, wobei wir diese immer wieder dem wissenschaftlichen und technischen Fortschritt anpassen wollen. Zudem planen wir eine eigene Förderung für Projekte aus der Grundlagenforschung, die nicht unmittelbar auf Anwendungen abzielt. Wir versprechen uns auch viel davon, die Kooperation zwischen Forschungsinstituten, Technologiezentren, Industrie und Quantentechnologie-Start-ups zu fördern. So kann man am ehesten Anwendungspotenzial von Forschungsarbeiten erkennen.

Die ersten Wissenschaftsprojekte sollen noch dieses Jahr starten

Unser Konzept wurde von der Europäischen Kommission gut aufgenommen: Im Februar dieses Jahres hat sie die erste, mit 130 Millionen Euro dotierte Ausschreibung für Forschungsanträge abgeschlossen – die ersten Wissenschaftsprojekte des Quanten-Flaggschiffs werden damit noch Ende 2018 starten.

Wir werden immer wieder gefragt, was die Erfolgsaussichten unseres Projekts sind – und mit Bedenken zum Timing und zum Umfang des Flaggschiffs konfrontiert. Andere Regierungen, darunter die der Volksrepublik China, nehmen viel größere Fördersummen in die Hand und konzentrieren diese auf wenige Projekte. Dies führt zu beeindruckenden Ergebnissen wie dem bereits erwähnten Quantenkommunikationssatelliten Micius und der Peking-Schanghai-Verbindung. Manche Skeptiker behaupten sogar, Europa habe das Rennen im Bereich der Quanten-



Auf dem Weg zum Quantenflaggschiff mussten die Physiker auch Günther Oettinger vom Nutzen der Quantenphysik überzeugen (hier an der Universität Ulm). Der damalige Digital-Kommissar der EU soll gefordert haben, dass die Forscher das Interesse der europäischen Industrie an Quantentechnologien dokumentieren und dass nicht nur die größten Mitgliedstaaten von dem Projekt profitieren.

computer bereits verloren, da fast alle Nachrichten dazu aus den USA zu kommen scheinen.

Die Zweifel sind auf den ersten Blick berechtigt, aber unserer Meinung nach in zwei Aspekten nicht weit genug gedacht. Erstens hat das Rennen erst begonnen. Gerade in den vielversprechendsten Bereichen der Quantentechnologien gibt es noch grundsätzliche Herausforderungen zu lösen, unter anderem bei den Quanten-Repeater und der Fehlerkorrektur für Quantencomputer. Es ist bezeichnend, dass bis auf wenige Ausnahmen industrielle Großunternehmen, die potenzielle Nutzer von Quantentechnologien sind, zwar verstärkt Interesse zeigen, aber große Investitionen jenseits von ein paar Millionen Euro bisher noch ausgeblieben sind. Sie sehen, wie viele andere auch, die Gefahr überzogener Erwartungen.

Europa sollte hier aus unserer Sicht seine Ausdauer unter Beweis stellen. Nur eine Kombination aus breiter Förderung vieler verschiedener Stoßrichtungen einerseits und gezielter Förderung von ambitionierten Forschungs- und Innovationsvorhaben mit klaren Projektzielen und Zeitplänen andererseits (wie zum Beispiel dem Bau eines europäischen Quantenverschlüsselungsnetzwerks oder europäischer Quantencomputerzentren) wird letztendlich zum Erfolg führen.

In der jetzigen Phase des Quanten-Flaggschiffs ist die Förderung noch vergleichsweise breit angelegt, um sich nicht zu früh auf die vermeintlich gewinnenden Technologien festzulegen. Eine Besonderheit der europäischen Herangehensweise ist sicherlich die starke Einbindung der gesamten Wissenschaftlergemeinschaft bei der Erarbeitung der Forschungsagenda, um eine Benachteiligung bestimmter Fachbereiche zu verhindern.

Zweitens ist die Metapher des Wettrennens womöglich die falsche. Gerade im Bereich der Quantentechnologien ist eine globale Zusammenarbeit seit Jahrzehnten gang und gäbe. So kooperiert beispielsweise das Quantentechnologie-Institut der Technischen Universität Delft in den Niederlanden sehr eng mit dem amerikanischen Unternehmen Intel bei der Entwicklung supraleitender Quantencomputer-Chips. Und die Gruppe von Anton Zeilinger arbeitet mit dem chinesischen Programm unter Jian-Wei Pan – der bei Zeilinger einst seine Doktorarbeit geschrieben hat – zusammen.

Die Staaten Europas werden Quantentechnologien nicht nur in Konkurrenz zu anderen Regionen vorantreiben, sondern auch gemeinsam mit ihnen. Bill Phillips, amerikanischer Nobelpreisträger und Quantentechnologiepionier, brachte es Ende Januar dieses Jahres in einer Anhörung im Europäischen Parlament auf den Punkt: »Wird es Wettbewerb oder Kooperation zwischen den USA und Europa geben? Lassen Sie es mich quantenphysikalisch ausdrücken: beides!« Daher ist auch der Zeitpunkt für das Europäische Quanten-Flaggschiff genau richtig. Europa kann auf führende Forschung bauen und hat eine starke Industrie, insbesondere im Fertigungssektor, im Gesundheits- und Pharmabereich sowie in der Chemieindustrie. Hier ergeben sich viele Anwendungen für Quantentechnologien, von Produktions- und Logistikprozessen über verbesserte Bildgebung bis zur Optimierung von chemischen Prozessen. Die technische Entwicklung hat sich gerade in den vergangenen zwei bis drei Jahren massiv beschleunigt; dennoch bleiben grundsätzliche Hürden.

Sobald diese genommen sind, könnten Quantentechnologien in Zukunft fast alle Bereiche der Gesellschaft beeinflussen. Dann wird sich zeigen, ob Europa in die richtigen Technologien genug investiert hat. Sowohl die Kommission als auch das Europäische Parlament stehen jedenfalls geschlossen hinter Quantentechnologien als strategisch wichtigem Feld für Europas Zukunft. Sie sind gewillt, gegebenenfalls benötigte Anpassungen vorzunehmen – das wurde bei öffentlichen Sitzungen wie auch in Gesprächen im Hintergrund immer wieder klar. Es gibt noch viele Ungewissheiten: Quantentechnologien sind ein typisches »high risk, high gain«-Projekt. Doch wer nicht wagt, der nicht gewinnt! ◀

QUELLEN

Acín, A. et al.: The European Quantum Technologies Roadmap, 2018, [arXiv.org/abs/1712.03773](https://arxiv.org/abs/1712.03773) (eingereicht bei New Journal of Physics)

De Touzalin, A. et al.: Quantum Manifesto, Mai 2016, <http://quope.eu/manifesto>

Mlynek, J. et al. (High-Level Steering Committee): Quantum Technologies Flagship Final Report, Juni 2017, <http://tinyurl.com/qt-hlsc-report>