

Ein Quantum Risiko

Schneller, effizienter, vernetzter, disruptiver: Wie Quantentechnologien sich auf die globale Sicherheit auswirken werden – und was das für Deutschland und Europa bedeutet.

Von Valentin Weber

Über Jahrhunderte haben Technologien Innovationsführern einen entscheidenden Vorteil gegenüber anderen Staaten verschafft. Das heutige Internet, das unter der damaligen US-Agentur Advanced Research Projects Agency entwickelt wurde, brachte den USA beträchtlichen Reichtum. Sieben der zehn größten Unternehmen weltweit haben derzeit ihren Standort in den USA und sind im Hardware- und Software-Bereich für internetbezogene Geräte tätig. Durch den frühen Ausbau der Internetinfrastruktur in den USA wurden außerdem viele globale Daten durch die USA geleitet, was den USA wiederum die Überwachung globaler Datenströme erleichterte.

Nun verspricht die Quantentechnologie solche Durchbrüche in der Wirtschaft, birgt aber auch massive Gefahren für die nationale Sicherheit. In ihrem 2023 veröffentlichten „Handlungskonzept Quantentechnologien“ billigt die Bundesregierung der Quantentechnologie disruptives Potenzial zu. China und Russland haben vor Kurzem ein „absolut abhörsicheres“ Quantensatelliten-Kommunikationssys-

tem getestet, das Zvenigorod, eine Stadt nahe Moskau, und Ürümqi, eine Stadt im Westen Chinas, verbindet.

Diese Kooperation zwischen Moskau und Peking zeigt, dass ein neuer Wettlauf um die Überlegenheit in Quantentechnologien entstanden ist. Der chinesische Staat hat im internationalen Vergleich die meisten Fördermittel ausgegeben, gefolgt von der EU, den Vereinigten Staaten und Japan. Bei den USA muss man hier besonders den Privatsektor erwähnen, der mehr als in anderen Staaten zur Entwicklung dieser Technologien beisteuert – man denke hier etwa an Google und IBM. Vor allem in China, wo fast alle staatlichen Bestrebungen in einem einzigen Forschungsinstitut in Hefei konzentriert sind, scheint das private Investment in Quantentechnologien zögernd zu verlaufen.

Wie Quantum die Welt verändern wird

Quantentechnologien werden in drei Bereiche gegliedert: Quantencomputing, Quantenkommunikation und Quantensensorik. Quantencomputer können im Vergleich zu klassischen Computern eine Vielzahl an



Dr. Valentin Weber ist Senior Research Fellow am Zentrum für Geopolitik, Geoökonomie und Technologie der Deutschen Gesellschaft für Auswärtige Politik (DGAP).

Rechenproblemen gleichzeitig lösen. Die Effizienzsteigerung geht ins Millionenfache. Mit dieser Rechenleistung können zum Beispiel neue Medikamente und neue Materialien für Solarzellen gefunden werden.

Durch ihre immense Rechenleistung werden Quantencomputer einen Großteil der heutigen verschlüsselten Nachrichten und Datenbanken von Staaten wie Banken brechen können. Verschlüsselung stellt, einfach gesagt, schwierige mathematische Probleme dar. Unter Quantentechnologien haben Computer das disruptivste Potenzial, sie sind aber wegen technologischer Hürden am weitesten von potenziellen kommerziellen und militärischen Anwendungen entfernt. Staaten fangen bereits heute verschlüsselte Daten von anderen Staaten ab, speichern sie und warten auf einen zukünftigen Zeitraum, wo Quantencomputer diese entschlüsseln können. Kompromittierende Informationen zu Spionen oder geheimen Projekten könnten auch noch in zehn oder 20 Jahren von Wert sein. Diese Praxis des Speicherns ist als „store now decrypt later“ bekannt.

Quantentechnologie steigert die Rechenleistung im Vergleich zu anderen Rechnern millionenfach

Quantenkommunikation wird schon früher verfügbar sein. Im Jahr 2017 gelang es österreichischen und chinesischen Wissenschaftlern, einen Quantenkommunikationslink zwischen Peking und Wien durch den Satelliten Mozi zu erstellen. Wie oben erwähnt, wurde der gleiche Satellit 2023 benutzt, um eine Verbindung zwischen den autoritären Verbündeten China und Russland zu erstellen. Die Technolo-

gie, die verwendet wurde, der sogenannte Quantenschlüsselaustausch, ist einer der Hauptanwendungsbereiche der Quantenkommunikation.

Die quantenverschlüsselte Verbindung gilt als abhörsicher, da jeder Versuch, die Verbindung zu belauschen, den Informationsfluss beeinträchtigen und sofort bemerkt werden würde. Da es jedoch einige Schwachstellen gibt, wie den Satelliten selbst, rät die US National Security Agency davon ab, Quantenschlüsselaustausch für die Sicherung von nationalen Sicherheitssystemen zu verwenden. Europa und China sind hier anderer Ansicht. Die EU plant mit ihrer European Quantum Communication Infrastructure ein sicheres Kommunikationsnetzwerk für die EU-27 und Überseeterritorien durch Glasfasernetze und Satelliten. In China wurde so ein Netzwerk schon zwischen Städten wie Peking und Schanghai realisiert und umspannt derzeit über 4000 Kilometer.

Präzision der Quantensensorik

Kommerziell am vitalsten sind derzeit nicht Quantencomputer oder gar Quantenkommunikation, sondern die Quantensensorik. Hier geht es darum, dass Quantentechnologien genauere Messungen vollbringen können als traditionelle Messgeräte. Diese Technik wird schon in einer ersten Testphase vom Militär des Vereinigten Königreichs angewandt, um unabhängiger von Satellitennavigationssystemen wie GPS oder Galileo zu werden. Quantensensoren schaffen es hierbei, Schiffe durch das Messen des Erdmagnetfelds präzise zu positionieren. Im Gegensatz zur Satellitennavigation sind Quantensensoren sehr schwer zu stören. Die Gefahr der Störung von Satellitennavigation wird derzeit in Russlands Krieg gegen die Ukraine sichtbar, wo deswegen täglich Dutzende Drohnen abstürzen.

Im Bewusstsein der großen Auswirkungen auf die internationale Sicherheit haben Staaten bereits begonnen, Kooperationen zur Förderung dieser neuen Technologie aufzubauen. Derzeit entstehen sowohl regionale als auch überregionale Projekte. Das Testen eines Quantenkommunikationslinks zwischen China und Russland war auch als Proof of Concept für ein BRICS-weites Quantenkommunikationsnetzwerk gedacht. In der AUKUS-Quantenvereinbarung verlautbaren die strategischen Partner Australien, das Vereinigte Königreich und die USA, dass sie gemeinsames Investment in Quantentechnologien für Positionierung, Navigation und Timing fördern werden. Der sicherheitspolitische Zusammenschluss „Quad“ (USA, Australien, Indien und Japan) umfasst auch gemeinsame Forschungsvorhaben für Quantentechnologien.

Es gibt einen merklichen Unterschied zwischen Allianzen, in denen die USA vertreten sind, und regionalen und überregionalen Einheiten, in welchen sie kein Teil sind. US-Allianzen fokussieren sich sehr stark auf Quantentechnologien, die bei der Navigation helfen können, oder auf andere Schwerpunkte wie Post-Quanten-Kryptografie. In der NATO-Quantenstrategie sowie in den Quad- und AUKUS-Vereinbarungen liegt der Fokus weniger auf der Teildisziplin der Quantenkommunikation. Andere Bündnisse – hierzu zählen die EU und die BRICS-Staaten – arbeiten aber aktiv am Ausbau von Quantenkommunikationsnetzwerken.

Diese Abwendung der USA von Quantenkommunikation und dem sogenannten QKD-Verfahren (Quantenschlüsselaustausch) lässt sich darauf zurückführen, dass die NSA und das National Institute of Standards von Quantenkommunikationstechnologien abraten, um sich vor Quantencomputern zu schützen. Begrün-

Ein Quanten-Internet würde das hergebrachte World Wide Web eines Tages ergänzen, aber nicht vollständig ersetzen

dung: Quantenkommunikationstechnologien führten neue Komplexitäten ein und brächten viele Schwachstellen mit sich. Um sich vor leistungsstarken Quantencomputern zu schützen, rät die NSA zur Post-Quanten-Kryptografie. Diese Form der Kryptografie ist mathematisch so komplex, dass selbst Quantencomputer Schwierigkeiten haben, sie zu lösen. Amazon verwendet schon seit 2019 Post-Quanten-Kryptografie, um seine Internetverbindungen zusätzlich zu schützen.

Die bestmögliche Sicherheit vor Quantencomputern liegt nicht allein in Quantenkommunikationsnetzwerken oder der Kryptografie, sondern in ihrer Kombination. Falls die eine Sicherheitsvariante kompromittiert wird, bleibt noch die zweite. Somit haben die EU und China hier wohl einen Vorsprung gegenüber den USA, die in Quantenkommunikationstechnologien keine kurzfristigen Vorteile sehen.

Der Weg zu einem Quanten-Internet

Eines Tages könnten eben diese Quantenkommunikationsnetzwerke, die in Europa und China gebaut werden, zu einem sogenannten Quanten-Internet führen. Ähnlich wie bei dem traditionellen Internet entsteht nach einem Zusammenschluss von genügend Geräten in einem Quantenkommunikationsnetzwerk ein Quanten-Internet. Das Quanten-Internet würde nicht das klassische Internet ersetzen, sondern ergänzen. Es würde zum Beispiel für kritische Infrastrukturen mehr Sicher-

heit bringen, wirtschaftliche Effizienz zwischen Unternehmen fördern und auch die Privatsphäre erhöhen – außerdem wäre es die Infrastruktur, in der Quantencomputer miteinander kommunizieren würden.

Mit der Quantum Internet Alliance (QIA), einem Zusammenschluss zahlreicher europäischer Forschungsinstitute und Unternehmen, ist Europa international gut aufgestellt. Ziel der QIA ist, einen Prototyp eines Quanten-Internets in Europa zu bauen.

Innerhalb der EU war bis vor Kurzem Deutschland Zugpferd in der Ausgabe öffentlicher Gelder für Quantentechnologien (46 Prozent), gefolgt von Frankreich (26,3 Prozent). Das finanzielle Investment Deutschlands hat sich gelohnt: Bei der Anzahl an Universitäten, die Masterstudiengänge in Quantentechnologien anbieten, liegt Deutschland unter 50 Staaten an zweiter Stelle, und auch bei Start-ups in diesem Bereich liegt es im europäischen und weltweiten Spitzenfeld.

Kommerziell kann Deutschland bei Quantensensorik und Lasern für Quantentechnologien punkten. So konnte etwa Bosch Airbus als Pilotkunden gewinnen, um Quanten-Magnetsensoren markttüchtig zu machen. Die Kooperation der zwei europäischen Unternehmen macht die Positionierung von Airbus-Flugzeugen störungsresistenter. Andere Quantensensoren von Bosch könnten es ermöglichen, die aktuelle Ladekapazität von E-Batterien in Autos genauer zu messen und damit Autofahrern die Sorge zu nehmen, dass die angezeigte Reichweite vielleicht nicht erreicht wird. Trumpf wiederum arbeitet an der genaueren Steuerung von Armprothesen durch Quantensensoren und somit an deren leichterem Handhabung.

Bei der Herstellung von hochqualitativen Lasern für Quantentechnologien zählen das Münchner Unternehmen Toptica Photonics und ihr Tochterunternehmen Toptica Eagleyard zu den Vorreitern. Selbst die USA sind stark von diesem

Quantencomputer können im Vergleich zu herkömmlichen Rechnern eine Vielzahl von Rechenoperationen gleichzeitig lösen. Das Bild zeigt einen Prototypen in der Physikalisch-Technischen Bundesanstalt BTB.

Bild nur in
Printausgabe verfügbar

Unternehmen und seinen Technologien abhängig. Ebenso bedeutend ist Osram Opto Semiconductors aus Regensburg, ein Unternehmen, das durch den Ankauf des US-Unternehmens und Laser-Herstellers Vixar noch attraktiver geworden ist.

So stark Deutschland und Europa in der Förderung der Quantenkommunikation und Quantensensorik sind, so weit hinten sind sie in der Entwicklung führender Quantencomputer. Dies wäre nicht weiter schlimm, da weder die USA noch China in allen Quantenteildisziplinen führend sind. Am disruptivsten – wirtschaftlich wie militärisch – werden jedoch groß angelegte Quantencomputer sein. Und hier sind die USA und China federführend.

Die leistungsfähigsten Quantencomputer befinden sich derzeit alle in Nordamerika und China so wie auch die am weitesten fortgeschrittenen Firmen wie Google Quantum AI, IBM und Amazon. In Europa finden sich ebenfalls Quantencomputer. Diese sind allerdings stark abhängig von ausländischen Technologien, so etwa der Supercomputer des kanadischen Herstellers D-Wave am Jülich Supercomputing Centre in Nordrhein-Westfalen. Die Bundesregierung hat bereits drei Milliarden Euro bis 2026 veranschlagt, um einen wettbewerbsfähigen Quantencomputer in Deutschland zu situieren.

Deutschland mag wohl bei kommerzialisierten Computern hinterherhinken; bei Publikationen im Forschungsgebiet Quantentechnologie liegt Deutschland knapp hinter den USA, China und Großbritannien.

Prioritäten, um die Spitze zu halten

Deutschland und Europa sind recht gut aufgestellt in der Entwicklung von Quantentechnologien. Wie kann diese Vorreiterrolle gehalten oder gestärkt werden? Eine Priorität muss sein, die neu entstandenen

Quantenlieferketten weitgehend unabhängig von China zu halten. Derzeit kommen kritische Komponenten vor allem aus Europa, den USA, Japan und anderen asiatischen Staaten. Aus China kommen vor allem seriengefertigte Produkte etwa der Optik oder Elektronik. Dies ist verkraftbar, da diese Technologien billiger sind, aber, falls nötig, auch anderswo produziert werden könnten. Die Bundesregierung muss hier ansetzen und kontinuierlich beobachten, dass sich Deutschlands Lieferkettenabhängigkeiten, wenn sie denn schon bestehen, auf Nichtsystemrivalen beziehen. Dies wäre vor allem aus einer Perspektive strategischer Autonomie wünschenswert.

Europa muss seine gute Position dringend verteidigen, indem es Personal hält, Wissensabfluss verhindert und Unternehmen die Technologie zur Verfügung stellt

Derzeit gibt es seitens der USA für Quantentechnologien noch keine Exportbeschränkungen, da noch nicht genau absehbar ist, welche Technologie militärischen Nutzen haben könnte. Sobald sich das jedoch herauskristallisiert, könnte es Handelsbeschränkungen gegen China geben. Diese könnten auch deutsche Unternehmen betreffen. Deutschland sollte daher im Auge behalten, welche Quantentechnologien am ehesten militärisch anwendbar sein könnten.

Im Januar 2024 veröffentlichte die NATO die Zusammenfassung ihrer ersten Quantenstrategie mit dem Ziel, die

Allianz quantenbereit zu machen. Sie benennt einige Anwendungsbereiche, etwa Quantencomputing zum Brechen von Verschlüsselungen. Unter anderem könnten Quantenradare die Radarreichweite um über 40 Prozent erhöhen und somit vor allem für die Erkennung von Tarnkappenflugzeugen und U-Booten genutzt werden. Diese Anwendungen sind zwar noch Zukunftsmusik. Die experimentelle Forschung in diesen sensiblen Bereichen sollte dennoch besondere Aufmerksamkeit erhalten, um Technologieabfluss frühzeitig zu verhindern. So sollten insbesondere Forschungsk Kooperationen mit chinesischen Instituten, die mit dem Militär zusammenhängen, so weit wie möglich unterbunden werden.

Auch Kooperationen, die nicht direkt dem chinesischen Militär zugutekommen, können problematisch sein. Hier ist die österreichisch-chinesische Zusammenarbeit im Bereich der Quantenkommunikation zu erwähnen. Unter der Schirmherrschaft von Anton Zeilinger (Nobelpreisträger für Physik 2022) und seinem ehemaligen Doktoratsstudenten an der Universität Wien, Jian Wei Pan, wurde 2017, wie oben erwähnt, eine quantenverschlüsselte Videokonferenz zwischen China und Österreich etabliert – die erste überhaupt in der Geschichte. Wie schon erwähnt, führte dies 2023 zu einer ähnlichen Etablierung eines Kommunikationskanals zwischen Russland und China. Das heißt: Eine anfangs in europäischer Kooperation entstandene Leistung wurde von europäischen Systemrivalen für ihre Zwecke benutzt, um künftige Absprachen zwischen China und Russland geheim zu halten.

Um das zu verhindern, sollten Forschungsinstitute Schulungen erhalten. Diese sollten insbesondere informieren, welche Kooperationen mit Blick auf die nationale Sicherheit problematisch sein

könnten. Gleichzeitig muss mehr getan werden, um talentiertes Personal mittel- und langfristig in Europa zu halten. Jian Wei Pan zog nach seiner Zeit als Postdoktorand an der Universität Heidelberg zurück nach China: Dort leitet er das bereits genannte milliarden schwere Forschungsinstitut in Hefei. Viele Erfolge Chinas in der Quantenkommunikationsforschung gehen direkt auf Pan zurück.

Ganz wichtig für die Wettbewerbsfähigkeit ist auch, Unternehmen so schnell wie möglich Quantentechnologien zur Verfügung zu stellen, um deren Produktivität zu steigern und so rascher einen internationalen Vorteil zu erlangen. Deutschland hat hier schon einen wichtigen Schritt getan, indem es eine Cloud finanziert, mit der Firmen Zugang zu Quantenanwendungen erhalten. Die Cloud wird im ersten Schritt durch ein vom Bundeswirtschaftsministerium beauftragtes Unternehmenskonsortium aufgebaut.

Wie im klassischen Cloud Business lassen auch im Quanten-Cloudbereich US-Unternehmen nicht auf sich warten und wollen mit souveränen Quanten-Cloudpunkten, nur eben mit amerikanischer Soft- und Hardware. In diesem Sinne plant IBM eine souveräne Quanten-Cloud-Region im deutschen Ehningen, die europäischen Forschungsinstituten Zugang zu Quanten-Cloud-Technologien verschaffen soll. Natürlich ist es zu begrüßen, dass mehr Kapazitäten in Europa aufgebaut werden; es sollte jedoch ein genaues Augenmerk darauf liegen, dass europäische Initiativen nicht aus dem Markt gedrängt werden. Deswegen sollte Deutschland die Kapazitäten der vom Bundeswirtschaftsministerium ins Leben gerufenen Quanten-Cloud erhöhen und sie auch anderen europäischen Forschungsinstituten zur Verfügung stellen. **IP**