Metis

# Studie

## Quantentechnologie: Implikationen für Sicherheit und Verteidigung

Nr. 25 | Mai 2021



Institut für
Strategie & Vorausschau

# Zusammenfassung

**Der Fortschritt bei der Manipulation quantenmechanischer Prozesse erlaubt es, deren besondere – aus alltäglicher Sicht bizarr anmutenden, aber in der Quantenphysik seit über hundert Jahren bekannten – Eigenschaften zunehmend für technische Anwendungen nutzbar zu machen. Die damit verbundenen Hoffnungen sind groß, die Erfolgsaussichten jedoch noch ungewiss. Die vorliegende Studie stellt den Stand der Forschung in vier quantentechnologischen Bereichen vor, bewertet vorausschauend sicherheitspolitische und militärische Implikationen und leitet Handlungsempfehlungen ab.**

## Alles Quanten oder was?

Bringen schon bald mit Quantensensoren bestückte Waffensysteme, die quantenverschlüsselt über ein Quanteninternet mit Quantencomputern kommunizieren den militärischen Quanten(vor)sprung? Spätestens mit Googles Ankündigung im Oktober 2019, erfolgreich »Quantenüberlegenheit« (siehe unten) gegenüber klassischen Supercomputern demonstriert zu haben, erhielt die bereits zuvor schwelende sicherheitspolitische Diskussion um das disruptive Potenzial militärisch genutzter Quantentechnologie erneuten Auftrieb. Seither machen zahlreiche neue Wortkompositionen mit dem »Quanten«-Präfix die Runde.

Richtig ist zunächst, dass im Zeitraum bis 2030 eine sicherheitspolitische Revolution durch Quantentechnologie eher unwahrscheinlich sein dürfte. Dies legen zumindest Expert*innenbefragungen aus dem Jahr 2020 nahe, nach denen zahlreiche andere, weiter gereifte „emerging and disruptive technologies" der Quantentechnologie mit Blick auf ihre militärstrategische Bedeutung noch klar den Rang ablaufen (Abb. 1).[1]

Richtig ist aber auch, dass Durchbrüche bei quantenbasierten Rechnern, Sensoren und Verschlüsselungsverfahren in der Tat einen erheblichen Fähigkeitsgewinn mit weitreichenden sicherheitspolitischen Implikationen nach sich ziehen *könnten* und Gegenmaßnahmen teilweise erst theoretisch erörtert werden.

In Summe erscheint es daher geboten, das Feld der Quantentechnologie aus einem sicherheitspolitischen Blickwinkel heraus nicht nur vorausschauend und unaufgeregt zu beobachten, sondern für einzelne Felder bereits jetzt Aktivmaßnahmen ins Auge zu fassen.[2]

## Warum Quantencomputer?

Der Siegeszug des klassischen Computers beruht auf Verkleinerung. Produktionskosten wurden gesenkt, die Leistungsfähigkeit zeitgleich erhöht. Doch inzwischen kommt eine physikalische Barriere in Sicht.

Gegenwärtiger Industriestandard sind Prozessoren, deren kleinste Komponenten Kantenlängen von um die 7 Nanometern (nm) – also 7 Milliardstel Meter – aufweisen. Das ist etwa zwölf Mal kleiner als ein einzelnes Coronavirus, 1 200 Mal kleiner als ein rotes Blutkörperchen und 12 000 Mal kleiner als ein menschliches Haar. Für kommende Chipgenerationen sind Komponenten mit Strukturbreiten von 2nm geplant.

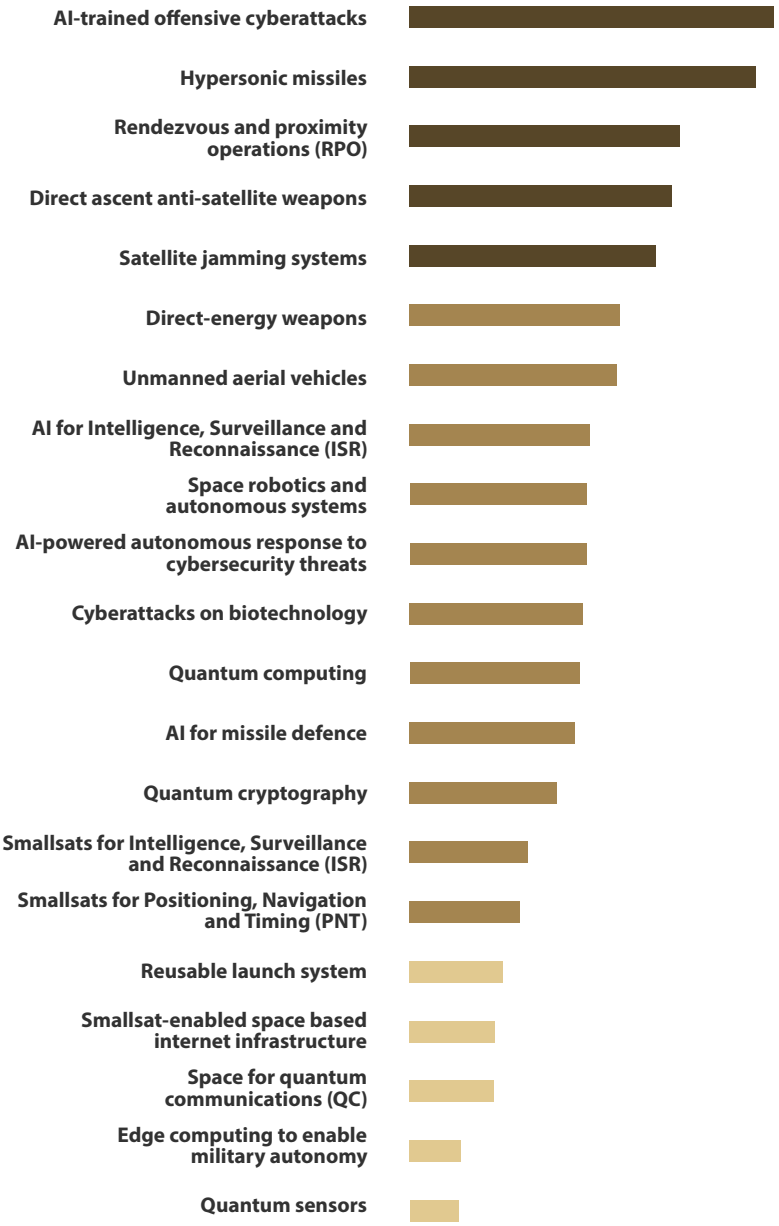
1 Die für diese Expert*innenbefragungen von Marina Favaro genutzte, von der RAND Corporation entwickelte *Systematic Technology Reconnaissance, Evaluation, and Adoption Methodology* (STREAM) dient dazu, aktuelle und zukünftige Technologien anhand einer Reihe von Auswirkungen und Umsetzungskriterien zu systematisieren, zu priorisieren und zu bewerten.

2 Siehe „Großmächte und Digitalisierung – welche Folgen für unsere Weltordnung?", Metis Studie Nr. 8 (Oktober 2018).

Die bislang äußerst erfolgreich angewandte Strategie der Verkleinerung bei klassischen Computern lässt sich allerdings theoretisch nur so lange fortsetzen, bis die kleinsten Funktionskomponenten auf einem Chip schlussendlich aus nur noch einem einzelnen Atom bestehen. Danach dürfte ihr Design – zumindest nach heutigem Kenntnisstand – an eine harte Grenze stoßen. Denn im subatomaren Bereich stehen quantenmechanische Effekte den auf klassischer Physik beruhenden Funktionsprinzipien bisheriger Computer entgegen.

Nicht zuletzt vor diesem Hintergrund wächst seit den 1990er Jahren das Interesse an Quantencomputern. Inzwischen sind sie aus der theoretischen Forschung über die experimentelle Praxis bis in die Rechenzentren und die Cloud für begrenzte, kommerziell verfügbare Probeanwendungen vorgedrungen.

***Abb. 1 Neue Technologien, per STREAM geordnet nach ihrem Potenzial, die globale strategische Stabilität zu beeinträchtigen.*** | Quelle: Marina Favaro, in: The 2020 UK PONI Papers, Royal United Services Institute.




Zwar waren quantenmechanische Erkenntnisse bereits grundlegend für die Entwicklung moderner Technologien des 20. Jahrhunderts, wie etwa Mikroelektronik oder Laser. Diese nutzten aber – wie im Falle der Computerchips gesehen – makrophysikalische Phänomene. Demgegenüber setzt Quantentechnologie gezielt auf die physikalischen Effekte im Größenbereich von einzelnen Atomen und darunter. Quantencomputer führen also das Prinzip der Verkleinerung auf der nächst-niedrigeren Stufe fort, indem sie die dort geltenden, fundamental anderen physikalischen Gesetzmäßigkeiten für Rechenoperationen nutzbar machen.

Superposition ist das erste dafür verwendete Phänomen (Abb. 4): Es beschreibt eine Überlagerung von Zuständen. Konkret nutzen Quantencomputer Superposition in Quantenbits (Qubits), die, anders als klassische Bits mit ihren nur zwei diskreten Zuständen (1 oder 0), alle zwischen 1 und 0 liegenden Zustände zeitgleich annehmen können. Quantencomputer bieten also eine im Vergleich zu klassischen Computern gigantische Parallel-Rechenleistung. Sie skalieren auch besser – zumindest in der Theorie. Denn idealiter verdoppelt jedes zusätzliche Qubit die Rechenleistung. Ihre Leistungsfähigkeit wächst also exponentiell. Bei Rechenaufgaben mit exponentiell zunehmender Komplexität erschließen Quantencomputer dort *schnell* (in Sekunden oder Minuten) Lösungen, wo selbst die größten klassischen Supercomputer zu lang (zehntausende Jahre) benötigen würden. Das ist es, was Google 2019 anhand eines rein akademischen, speziell auf die Stärken von Quantencomputern zugeschnittenen Rechenproblems mit seinem 53 Qubit-Quantenprozessor *Sycamore* nach eigenen Angaben demonstrieren konnte – und was gemeinhin unter dem Begriff der »Quantenüberlegenheit« verstanden wird.

Verschränkung ist das zweite genutzte Phänomen (Abb. 5). Es besagt, dass zwei oder mehrere Teilchen miteinander verknüpft sein, also – auch über große Distanzen hinweg – den gleichen Zustand annehmen können. Die zahlreichen Möglichkeiten zur flexiblen Manipulation solcher miteinander verschränkten Qubits trägt zur Geschwindigkeit bei, mit der Quantencomputer die besagten komplexen Rechenprobleme zu bewältigen imstande sind.

Allerdings produzieren Quantencomputer große Datenmengen mit hohen Fehlerraten – letzteres auch deswegen, weil zum Beispiel bereits kleinste Temperaturschwankungen die Qubits in ihren delikaten quantenmechanischen Zuständen stören. Die Herausforderung liegt somit darin, Anzahl und Langlebigkeit der Qubits zu erhöhen sowie zeitgleich effektivere Fehlerkorrekturmechanismen zu implementieren, um das gewünschte Rechenergebnis zu extrahieren, also das richtige Signal aus dem lauten »Datenrauschen« des Quantencomputers »herauszuhören«. Die *Noisy Intermediate-Scale Quantum* (NISQ)-Technologie für Quantencomputer mit 50 bis 100 Qubits gilt aktuell als Übergangslösung auf dem Weg hin zur Entwicklung weniger verrauschter Rechner mit mehr Qubits, die dem Quantenrechnen endlich breitere, wirklich praxisrelevante Anwendungsgebiete erschließen sollen. Aus aktueller Sicht scheinen dafür wohl bis zu 1 Millionen Qubits nötig. IBM peilt aktuell bis 2023 das Überschreiten der 1 000 Qubit-Marke an. Der Weg ist also noch sehr lang.

Erschwerend kommt hinzu, dass die beiden aktuell dominierenden Designs – Schaltkreise aus supraleitenden Metallen (genutzt u. a. von Google, IBM und Rigetti Computing) sowie Ionenfallen (genutzt u. a. von Honeywell und IONQ) – in der Praxis schlecht skalieren. Grund sind die Kontrollsysteme für die fragilen, streng abgeschirmten Qubits. Das auf Supraleitung beruhende Design (Abb. 2) nutzt Mikrowellen zur Programmierung, muss all seine Qubits aber mit großem Aufwand bis nahe an den absoluten Nullpunkt von minus 273 Grad Celsius heruntergekühlt halten. Systeme mit Qubits aus im Vakuum von Magnetfeldern in der Schwebe gehaltenen, geladenen Atomen funktionieren demgegenüber zwar bei Raumtemperatur, benötigen aber nicht beliebig zu verkleinernde Lasersysteme zur Programmierung.

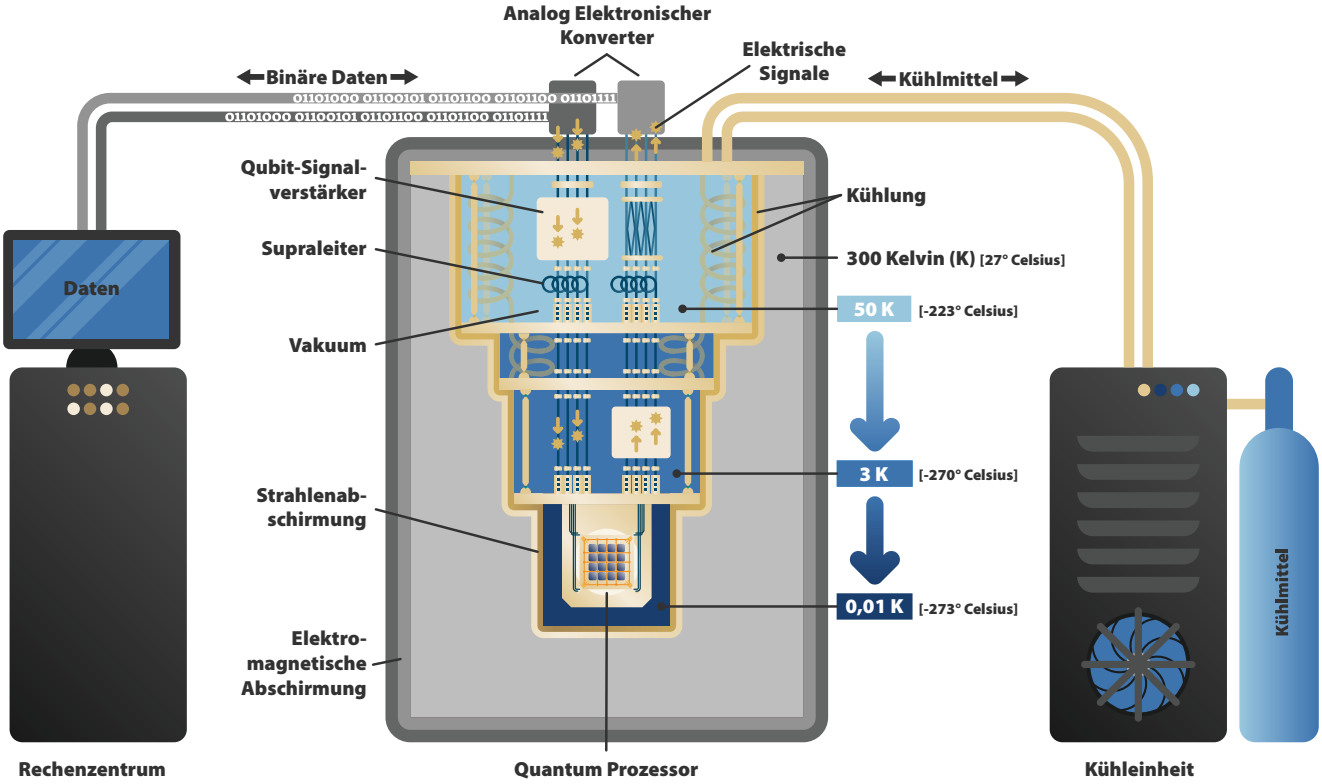



***Abb. 2** Schematische Darstellung eines auf Supraleitung basierenden Quantencomputers.* | Quelle der Vorlage: VectorMine auf shutterstock.com

***Abb. 3*** ***Wissenschaftlerin in IBM Quantum Labor.*** | Quelle: flickr.com/photos/ibm_research_zurich/; Credit: Connie Zhou für IBM

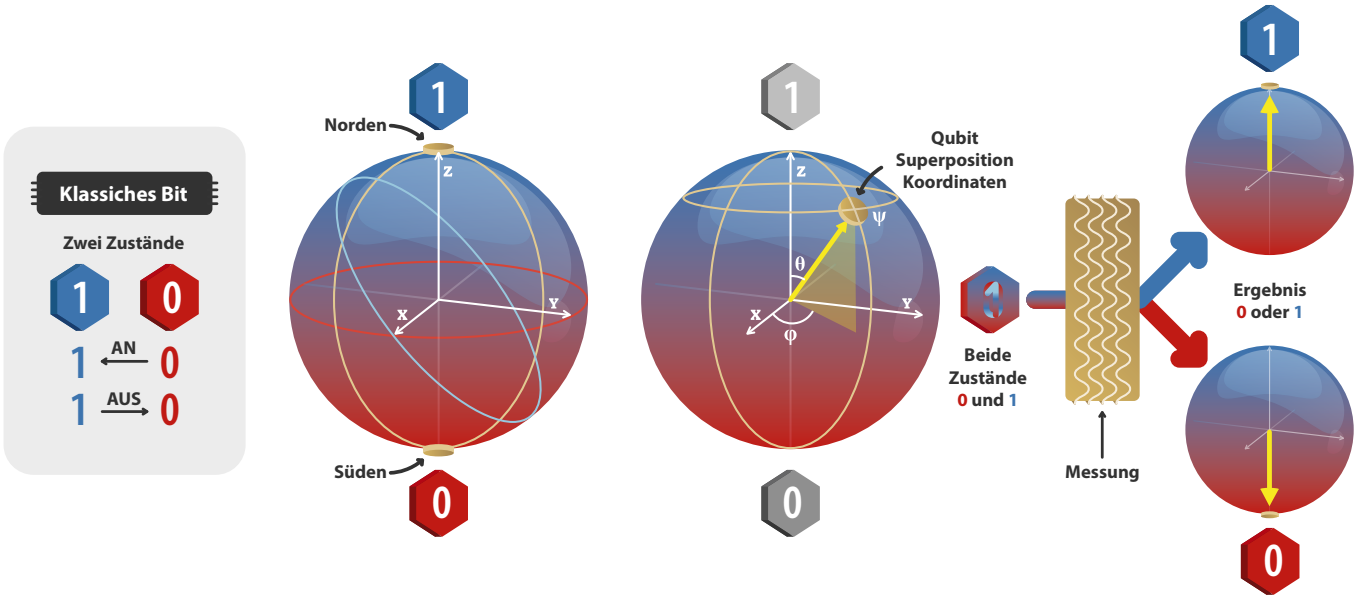



***Abb. 4** Schematische Darstellung vom Rechnen mit Qubits.* | Quelle der Vorlage: VectorMine auf shutterstock.com

Zusammenfassend lässt sich festhalten, dass der bereits jetzt anlaufende Parallelbetrieb von klassischen Computern und auf hochspezielle Probeanwendungen begrenzten Quantencomputern auf absehbare Zeit erhalten bleiben wird, weil bis zur breiten Nutzbarmachung letzterer (durch Verkleinerung massenproduktionsfähiger Architekturen) noch zahlreiche hohe Hürden zu nehmen sind. Es ist gut möglich, dass dabei keines der beiden oben skizzierten Designs das Rennen macht und sich stattdessen eine der zahlreichen in der Entwicklung befindlichen Alternativen als Hardwareplattform für Quantencomputer durchsetzt. Skeptiker*innen merken an, dass Quantencomputern auch das gleiche Schicksal wie der Kernfusion drohen könnte: Jahrzehnt für Jahrzehnt wird der Technologie der Durchbruch vorhergesagt. Aber er scheint sich nie zu realisieren.

## Sicherheitspolitische Implikationen

Die Triebfedern hinter der Entwicklung von Quantentechnologie sind wissenschaftliche und kommerzielle. Aber Durchbrüche im Feld könnten zukünftig auch weitreichende sicherheits- und verteidigungspolitische Implikationen entfalten – nicht in Form eines singulären Ereignisses wie im Falle der Entwicklung der Atombombe, sondern durch ihre Breitenwirkung. Die Rolle von Quantentechnologie wäre – so sich ihre Versprechen denn tatsächlich realisieren – die eines massiven Trendverstärkers mit Blick auf das Streben nach Informationsüberlegenheit. Das gesamte Spektrum von Führung, Information, Kommunikation, Computersystemen, Nachrichtenwesen, Überwachung und Aufklärung könnte berührt werden. Konkret im Raum stehen Aussichten auf gesteigerte Präzision, Effizienz, und Automatisierung.

### Kryptokommunikation

Das quantenphysikalische Phänomen der Verschränkung kann zum Verschlüsseln von Kommunikation genutzt werden. Häufig ist hierbei davon die Rede, dass quantenverschränkte Verbindungen unmöglich ohne eine sofort erkennbare Störung abzuhören seien, wodurch ein *unbemerktes* Mitlauschen naturgesetzlich ausgeschlossen sei. Das klingt gut und ist in der Theorie nicht falsch.

Doch die Umsetzung ist knifflig und die Technik noch nicht in der Breite einsatzreif. Bisherige Demonstrationsprojekte funktionieren entweder nur über kurze Glasfaserleitungen oder benötigen eine große Zahl an Repeatern (wofür in der Forschung Satellitenkonstellationen als effizienteste Lösung diskutiert werden). Darüber hinaus erweist sich auch quantenverschlüsselte Kommunikation anfällig für „side-channel attacks", bei denen nicht das kryptographische Verfahren selbst, sondern seine praktische Implementierung in einer Anwendungsumgebung angegriffen wird – um die Information eben doch unbemerkt über Seitenkanäle abzuzapfen.

Selbst wenn zeitnah, also gen Ende dieses Jahrzehnts, ein Durchbruch in der Breitenanwendung quantenverschlüsselter Verbindungen gelänge, so wären – zumindest aus einer sicherheitspolitisch eng verstandenen, also militärischen Sicht – die Implikationen überschaubar.

**Sensorik**

Sensorik ist das quantentechnologische Feld mit den meisten konkreten, bereits nutzbaren Anwendungen. Anders als Quantencomputer benötigen Quantensensoren keine großen Zahlen miteinander verschränkter Teilchenpaare; auch das für genaue Messungen natürlich hinderliche »Rauschen« hat die Forschung in den letzten zwei Jahrzehnten durch erhebliche Fortschritte beim Herstellen und Manipulieren der Quantenzustände von Teilchen besser im Griff. Ähnlich wie im Feld der Computer wird außerdem auch hier die Nutzung verschiedener physikalischer Prinzipien und Designs gleichzeitig vorangetrieben.

Messungen von Masse, Zeit, Ort, Geschwindigkeit, Beschleunigung oder elektromagnetischer Feldstärken können mit Quantensensoren um Größenordnungen präziser stattfinden als mit klassischen Sensoren. Räumliche Auflösungen im Nanometerbereich sind möglich. Quantenuhren ermöglichen präzise Synchronisation von Abläufen. Quantengyroskope für Trägheitsnavigationssysteme oder Quantensensoren für Erdmagnetfeldmessungen können autonome Fortbewegung unabhängig von GPS oder anderen Satellitennavigationssystemen ermöglichen. Kompakte und bei Raumtemperatur funktionierende Quantenmagnetometer sind in der Entwicklung. Ihr möglicher Anwendungsbereich erstreckt sich von der U-Boot-Ortung bis hin zu Gehirn-Computer-Schnittstellen.[3]

Spekulationen zu einem leistungsfähigen chinesischen Quantenradar, das, so fürchteten vor einigen Jahren sicherheitspolitische Kreise in Washington, schon bald die Stealth-Technologie obsolet machen könnte, lassen sich (zumindest auf Basis offen zugänglicher Quellen) nicht erhärten. Das unterstrich jüngst erneut das Defense Science Board des Pentagon.

Das breite Feld der Quantensensorik nähert sich einer militärischen Nutzung am schnellsten an. Aber es ist nicht seriös vorhersagbar, welche Sensortechnologie wann Serienreife erreichen und ihren Weg ins Feld der Sicherheit und Verteidigung finden wird. Da Sensorik zudem etliche Anwendungsbereiche tangieren könnte, ist die Vielzahl möglicher Implikationen im Rahmen dieser Studie nicht abschätzbar.

**Kryptoanalyse**

Etablierte kryptographische Verfahren machen sich den Umstand zunutze, dass bestimmte mathematische Probleme durch klassische Computer nicht in einem überschaubaren Zeitrahmen berechnet werden können. Quantencomputer haben, wie oben gesehen, das Potenzial, hier einen Paradigmenwechsel einzuleiten, also nach bisherigen Standards sicher verschlüsselte Datenbestände in kürzester Zeit zu entschlüsseln. Auch eingelagerte, bis dato nicht zu entschlüsselnde Datenbestände könnten jäh offengelegt werden.

Noch ist dies ein theoretisches Szenario. Trotzdem hat das Nachdenken über quantencomputerresistente Verschlüsselungsverfahren für die Welt der klassischen Computer und des Internets längst begonnen. Das National Institute for Standards and Technology (NIST) in den USA hat beispielsweise bereits 2016 einen Prozess ins Leben gerufen, um solche Verfahren zu entwickeln, zu standardisieren und zur Verfügung zu stellen. Erste Ergebnisse für solche gegenüber Quantencomputern sichere Verschlüsselungen werden 2022 / 2023 erwartet.

3 Siehe „Konventionelle Rüstungskontrolle und neue Technologien", Metis Studie Nr. 20 (September 2020).

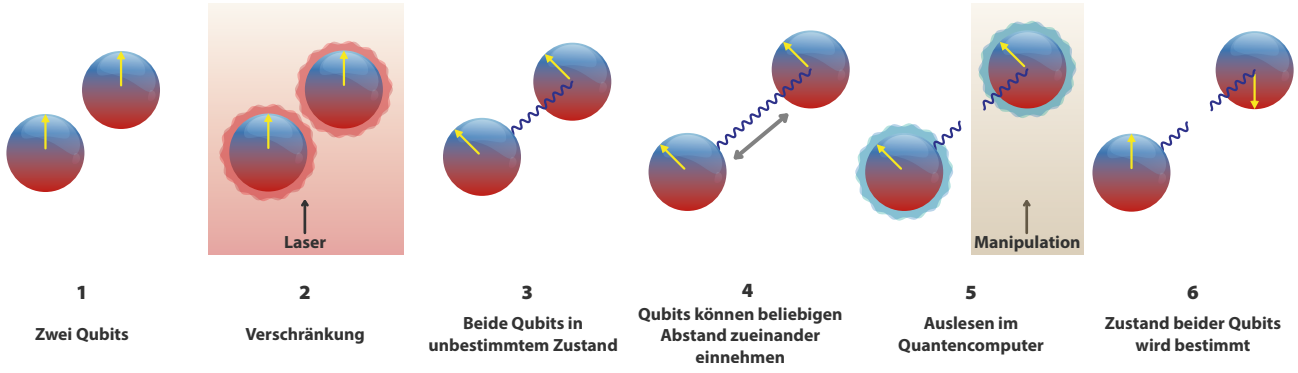



***Abb. 5 Schematische Darstellung der Verschränkung von Qubits.*** | Quelle der Vorlage: VectorMine auf shutterstock.com

Es ist nicht gänzlich ausgeschlossen, dass die oben genannten Skeptiker*innen Recht behalten und einige der mit Quantencomputern verbundenen Versprechungen länger – oder gar für immer – auf sich warten lassen werden. Aber angesichts der in nur knapp drei Jahrzehnten gemachten Fortschritte, der bereits existierenden Prototypen und Spezialanwendungen, der Investitionen und nicht zuletzt dem weltweiten Aufwand von Talent und Zeit scheint die hier im Raum stehende Frage doch eher eine des »Wann«, nicht des »Ob« zu sein.

Legt man diese Annahme zugrunde, ergeben sich im Falle der Kryptoanalyse weitreichende sicherheitspolitische Ableitungen. Sämtliche sensible Kommunikation müsste dann flächendeckend und so schnell wie möglich durch die Umstellung auf quantencomputerresistente Verschlüsselungsverfahren geschützt werden.

## Fazit und Handlungsempfehlungen

Die USA, China, Großbritannien und Indien haben Förderprogramme für Quantentechnologie aufgelegt; die EU betreibt ein »Flaggschiffprojekt« und will Mittel in Höhe von bis zu einer Milliarde Euro bereitstellen. Die Bundesregierung beschloss, auch um sich der durch die Covid-19-Pandemie verursachten Wirtschaftskrise entgegenzustemmen, im Juni 2020 ein Konjunkturprogramm, in welchem ebenfalls Quantentechnologie gezielt gefördert wird. Allein in der laufenden Legislaturperiode sind 650 Millionen Euro vorgesehen. Die Forschung in Europa und insbesondere Deutschland kann – dank der staatlichen Förderung, traditionell guter wissenschaftlicher Ausbildung und zahlreichen bereits bestehenden technologischen Schwerpunktzentren – bisher mit der Weltspitze mithalten.

Im Sicherheits- und Verteidigungsbereich wird sich der eingangs skizzierte Hype um Quantentechnologie, das legen zumindest Erfahrungen mit anderen neuen Technologien nahe, bald fürs Erste wieder legen. Und da soziale und politische Faktoren wie Kultur und Regulierung mit Technologieentwicklung und -anwendung stets in Wechselwirkung stehen, ist ohnehin keine lineare Entwicklung zu erwarten.

Zugleich hat aber diese Studie gezeigt, dass Abwarten keine Option ist und wichtige Fragen schon jetzt adressiert werden müssen. Daraus ergeben sich drei Empfehlungen für das kurz-, mittel- und langfristige Ausloten von Handlungsoptionen.

- Quantencomputerresistente Kryptographie wird zum Standard werden. Das Bundesverteidigungsministerium sollte jetzt planen und abschätzen, wie lange das Implementieren entsprechender Verschlüsselungsverfahren in seinem Geschäftsbereich dauern würde. Tritt ein Durchbruch bei Quantencomputern – und somit das Ende der klassischen Verschlüsselung – vor dem Abschluss dieses Prozesses ein, dann hat dies desaströse Auswirkungen auf eingestufte Informationen. Zu bedenken ist dabei: Auch bis dato womöglich bereits von der Gegenseite gesammelte, wenn auch noch verschlüsselte Daten müssten fortan als kompromittiert gelten.

- Mittelfristig sollte die Bundeswehr – in nationalem Rahmen, aber auch mit Partnern in EU und NATO sowie mit Einrichtungen für angewandte Forschung und der Industrie – systematisch durchspielen, was Durchbrüche im Feld der Sensorik militärisch konkret bedeuten könnten. Welche neuen Fähigkeiten wären mit einzelnen Anwendungen für einen potenziellen Gegner verbunden, welche eigenen würden womöglich obsolet? Was wären die Implikationen für Planung, Beschaffung und Interoperabilität? Welche rüstungskontroll- und exportpolitischen Hebel könnten entwickelt werden? Szenario-Workshops bieten ein mögliches Format für solche Überlegungen.

- Langfristig und in breitem gesellschaftlichem Rahmen sollte darüber nachgedacht werden, was ein Durchbruch im Bereich des Quantencomputers menschheitsgeschichtlich bedeuten würde. Das Ende der klassischen Verschlüsselung ist, wie oben gesehen, nur eine mögliche Konsequenz. Auch Pharmazie und Materialwissenschaften könnten durch die Verfügbarkeit von Quantencomputern revolutioniert werden, um nur zwei weitere Beispiele zu nennen. Insbesondere aber der Fortschritt im aktuell dank maschinellem Lernen bereits boomenden Feld der Künstlichen Intelligenz[4] dürfte weiter beschleunigt werden, was leistungsfähige Simulationen und die Optimierung zahlloser Verfahren erlauben würde. In der internationalen Forschergemeinde ist vor diesem Hintergrund bereits eine Diskussion um »Quantenethik« in Gang gekommen: Welcher rechtlichen, politischen und sozialen Rahmenbedingungen bedarf es, um den womöglich existenziellen Risiken des Quantenzeitalters zu begegnen?

4 Unter Künstlicher Intelligenz wird hier die Vielzahl unterschiedlicher computerbasierter Techniken und Verfahren zur Automatisierung von Aufgaben verstanden, die bisher die Anwendung menschlicher Intelligenz erforderten.

Metis

**IMPRESSUM**

**Herausgeber**

Metis Institut
für Strategie und Vorausschau
Universität der Bundeswehr München
metis.unibw.de

**Autor**

Dr. Frank Sauer
metis@unibw.de

**Creative Director**

Christoph Ph. Nick, M. A.
c-studios.net

**Bildnachweis**

Titel: IBM Q Quantum Computer. | Quelle: flickr.com/photos/ibm_research_zurich/; Credit: Graham Carlow

**ISSN-2627–0587**