19. Wahlperiode

Deutscher Bundestag
Ausschuss Digitale Agenda

Wortprotokoll
der 11. Sitzung

Ausschuss Digitale Agenda
Berlin, den 6. Juni 2018, 16:00 Uhr
11011 Berlin, Konrad-Adenauer-Str. 1
Sitzungssaal: PLH E.300

Vorsitz: Hansjörg Durz, MdB

Tagesordnung - Öffentliche Anhörung

Einziger Tagesordnungspunkt **Seite 08**

Öffentliches Fachgespräch
zum Thema "Quantencomputer"

Mitglieder des Ausschusses

	Ordentliche Mitglieder	Stellvertretende Mitglieder
CDU/CSU	Beermann, Maik Durz, Hansjörg Hauer, Matthias Heilmann, Thomas Kemmer, Ronja Sauer, Stefan Schipanski, Tankred	Biadacz, Marc Friedrich (Hof), Dr. Hans-Peter Kühne, Dr. Roy Nick, Dr. Andreas Schön, Nadine Steineke, Sebastian Whittaker, Kai
SPD	Esken, Saskia Herzog, Gustav Korkmaz, Elvan Mohrs, Falko Zimmermann, Dr. Jens	Bartol, Sören Gerster, Martin Kelber, Ulrich Klingbeil, Lars Stadler, Svenja
AfD	Cotar, Joana Kamann, Uwe Schulz, Uwe	Bühl, Marcus König, Jörn Wiehle, Wolfgang
FDP	Höferlin, Manuel Schulz, Jimmy	Brandenburg, Mario Sitta, Frank
DIE LINKE.	Domscheit-Berg, Anke Sitte, Dr. Petra	Movassat, Niema Pau, Petra
BÜNDNIS 90/DIE GRÜNEN	Christmann, Dr. Anna Janecek, Dieter	Bayaz, Dr. Danyal Rößner, Tabea

19. Wahlperiode

Deutscher Bundestag

Sitzung des Ausschusses Digitale Agenda (23. Ausschuss)

Mittwoch, 6. Juni 2018, 16:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
CDU/CSU		**CDU/CSU**	
Beermann, Maik		Biadacz, Marc	
Durz, Hansjörg		Friedrich (Hof) Dr., Hans-Peter	
Hauer, Matthias		Kühne Dr., Roy	
Heilmann, Thomas		Nick Dr., Andreas	
Kemmer, Ronja		Schön, Nadine	
Sauer, Stefan		Steineke, Sebastian	
Schipanski, Tankred		Whittaker, Kai	
SPD		**SPD**	
Esken, Saskia		Bartol, Sören	
Herzog, Gustav		Gerster, Martin	
Korkmaz, Elvan		Kelber, Ulrich	
Mohrs, Falko		Klingbeil, Lars	
Zimmermann Dr., Jens		Stadler, Svenja	

Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339

ÖH.

19. Wahlperiode

Sitzung des Ausschusses Digitale Agenda (23. Ausschuss)
Mittwoch, 6. Juni 2018, 16:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
AfD		**AfD**	
Cotar, Joana		Bühl, Marcus	
Kamann, Uwe		König, Jörn	
Schulz, Uwe		Wiehle, Wolfgang	
FDP		**FDP**	
Höferlin, Manuel		Brandenburg, Mario	
Schulz, Jimmy		Sitta, Frank	
DIE LINKE.		**DIE LINKE.**	
Domscheit-Berg, Anke		Movassat, Niema	
Sitte Dr., Petra		Pau, Petra	
BÜ90/GR		**BÜ90/GR**	
Christmann Dr., Anna		Bayaz Dr., Danyal	
Janecek, Dieter		Rößner, Tabea	

ÖH.

Tagungsbüro

Deutscher Bundestag

Sitzung des Ausschusses Digitale Agenda (23. Ausschuss)
Mittwoch, 6. Juni 2018, 16:00 Uhr

	Fraktionsvorsitz	Vertreter
CDU/CSU		
SPD		
AFD		
FDP		
DIE LINKE.		
BÜNDNIS 90/DIE GRÜNEN		

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	Fraktion	Unterschrift
KOCH ZECH	SPD	
Pialluhn	B90/Gr	
Dr. HERRMANN	AfD	
LIENING	CDU/CSU	
F. SARTORI	SPD	
K SHOAIB	FDP	

Ministerium bzw. Dienststelle (bitte in Druckschrift)	**Name** (bitte in Druckschrift)	**Unterschrift**	**Amtsbezeichnung**
BMWi	Schmidt-Holtmann		ORRin
BMWi	Marco-Alexander Bret		MdI
BMI	Peter Franke	Franke	TB'er

Deutscher Bundestag

Liste der Sachverständigen
Öffentliche Anhörung
am Mittwoch, 06. Juni 2018,16.00 Uhr im Saal E.300 PLH

Anwesenheitsliste Sachverständige

Name	Unterschrift
Dr. Stephan Ritter	
Prof. Dr. Frank Wilhelm-Mauch	
Prof. Dr. Marian Margraf	
Prof. Dr. rer. nat. Hendrik Bluhm	
Prof. Dr. Dr. h.c. Johannes Buchmann	
Prof. Dr. Stephanie Wehner	
Prof. Dr. Winfried Hensinger	

Einziger Tagesordnungspunkt

Öffentliches Fachgespräch zum Thema: "Quantencomputer"

Der **Vorsitzende** Hansjörg **Durz** (CDU/CSU): Ich darf Sie nun bitten, die Plätze einzunehmen. Ich begrüße Sie alle ganz herzlich zur 11. Sitzung des Ausschusses Digitale Agenda, zur öffentlichen Anhörung zu dem Thema „Quantencomputer".

Ich begrüße ganz herzlich die Mitglieder des Ausschusses, die Mitarbeiter des Ausschusssekretariats und all diejenigen, die unsere öffentliche Anhörung verfolgen. Ganz herzlich begrüße ich auch die geladenen Sachverständigen, die uns das Thema heute näher bringen werden. Ich darf ganz herzlich begrüßen

Herrn Dr. Stephan Ritter,
Herrn Prof. Dr. Frank Wilhelm-Mauch,
Herrn Prof. Dr. Marian Margraf,
Herrn Prof. Dr. Hendrik Bluhm,
Herrn Prof. Dr. Dr. h.c. Johannes Buchmann,
Frau Prof. Dr. Stephanie Wehner und
Herrn Prof. Dr. Winfried Hensinger.

Herzlich Willkommen bei uns im Ausschuss. Vielen Dank, dass Sie heute da sind.

Wir widmen uns in dieser ersten öffentlichen Anhörung des Ausschusses Digitale Agenda in der 19. Wahlperiode den Quantencomputern. In der Forschung sind Quantencomputer nicht ganz neu. Aber nach mehr als zwanzig Jahren Entwicklung und den ersten Laborexperimenten erreichen uns die Quantencomputer und ihre Anwendungen mittlerweile fast wöchentlich in den Schlagzeilen, zumindest in der technikbezogenen Presse, aber auch darüber hinaus. Zudem wird insbesondere ein Wettlauf zur Realisierung von Quantencomputern mit sehr namhaften Hauptakteuren beschrieben. Dies spiegelt die reale und rasante Entwicklung auf diesem Gebiet wider. Grund genug, dass sich der Ausschuss Digitale Agenda des Deutschen Bundestages mit diesem Thema befasst. Es geht unter anderem darum, auf welchem Stand der Entwicklung wir uns aktuell befinden bis hin zu den möglichen Anforderungen an die Politik. Dazu wollen wir uns heute umfassend informieren und von den Experten Informationen erhalten.

Bevor wir mit den Statements beginnen, möchte ich auf verschiedene organisatorische Abläufe hinweisen: Die Sachverständigen halten zu Beginn ein fünfminütiges Statement. Laut Vereinbarung der Obleute von heute Nachmittag erhält jeder Abgeordnete die Möglichkeit, zunächst zwei Minuten lang Fragen zu stellen. Die Fragen werden gesammelt, und die Sachverständigen haben dann die Möglichkeit, darauf zu antworten. Sie sollten sich möglichst auf fünf Minuten beschränken. Sollte es bei diesem komplexen Sachverhalt länger dauern, haben wir dafür auch Verständnis, aber fünf Minuten sollte der Richtwert sein.

In den dann folgenden Fragerundenwollen wir es ebenso handhaben: Zwei Minuten Fragezeit für die Abgeordneten und die entsprechende Antwortzeit für die Experten. Es wird ein Wortprotokoll angefertigt. Die Anhörung wird durch das Parlamentsfernsehen zeitversetzt um eine Stunde übertragen. Der Stream ist später über die Mediathek des Deutschen Bundestages abrufbar. Weitere Aufnahmen während der Sitzung gibt es auch; ein Kamerateam begleitet derzeit vier Abgeordnete des Deutschen Bundestages, darunter auch Frau Dr. Petra Sitte. Im Ergebnis soll ein Dokumentarfilm entstehen, der 2020 im RBB ausgestrahlt werden soll. Das ist schon sehr in die Zukunft gerichtet. Wer weiß, wo wir dann bei den Themen stehen, die wir heute diskutieren. Die Mikrofone bitte ich jeweils für den Wortbeitrag einzuschalten und danach wieder auszuschalten. Soweit die organisatorischen Hinweise. Ich darf nun die Sachverständigen um ihre Eingangsstatements bitten.

SV **Dr. Stephan Ritter**: Vielen Dank, Herr Vorsitzender, vielen Dank meine Damen und Herren Abgeordnete für die Einladung. Quantencomputer sind faszinierend. Sie nutzen die Gesetze der Physik auf kleinsten Skalen für eine neue Art des Rechnens. Diese verlangt neue Algorithmen, aber insbesondere auch revolutionäre neue Hardware. Es müssen quantenmechanische Systeme, wie einzelne

Atome und einzelne Ionen, die lange Zeit nicht einmal beobachtet werden konnten, unter vollständige Kontrolle gebracht werden. Nur so können sie als Quantenbits eingesetzt werden.

Quantenbits sind das Äquivalent eines klassischen Bits für einen Quantencomputer. Weil die Zustände dieser Quantensysteme so fragil sind, muss diese exotische Hardware nahezu perfekt von der Umgebung isoliert werden. Gleichzeitig möchte man aber ihre Zustände mit höchster Präzision manipulieren. So wird plausibel, warum selbst die derzeit größten universellen Quantencomputer aus noch nicht mehr als 50 Qubits bestehen. Aber die physikalischen und technologischen Herausforderungen anzunehmen ist lohnend, weil Quantencomputer mit einigen Berechnungen und Aufgaben prinzipiell viel besser klarkommen als herkömmliche klassische Computer. Vereinfacht gesagt: Kapitulieren Sie nicht, wenn das zu berechnende System groß wird. Damit rücken die Berechnungen einiger Fragestellungen in den Bereich des Möglichen, deren Anwendungsbereich von herausragender Bedeutung ist. Eine effiziente Lösung von Optimierungsproblemen nutzt in der ökonomischen Modellierung und in der Logistik, sie hilft bei der Steuerung des Verkehrsflusses und beim autonomen Fahren. Die Simulation von Quantensystemen, wie Molekülen und deren Dynamik, ist für die Entwicklung neuer Medikamente, neuer Materialien und die energieeffiziente Synthese, beispielsweise von Stickstoffdünger, wichtig. Maschinelles Lernen würde beschleunigt, weil künstliche Intelligenz mit Quantencomputern schneller trainiert werden kann. Auch Muster- und Spracherkennung sowie die Datenbanksuche würden von Quantencomputern profitieren. Die Begeisterung über diese fantastischen potenziellen Anwendungen darf uns nicht vergessen lassen, dass es noch viele technologische, aber auch einige strukturelle Herausforderungen gibt.

Hierzu gehören die Aus- und Weiterbildung hochqualifizierter Arbeitskräfte. Zurzeit ist das Wissen über Quantencomputer hauptsächlich in relativ kleinen Arbeitsgruppen an Universitäten oder anderen Einrichtungen der Grundlagenforschung vorhanden. Dies sieht man nicht zuletzt auch an den heute hier vertretenen Sachverständigen, die, außer mir, alle an Universitäten arbeiten. Dort fehlt häufig die Möglichkeit für die Entwicklung von Produkten, die auch Anwender ohne Expertise im Bereich der Quanten-Hardware nutzen können. In Unternehmen, die größere Produktentwicklung eher stemmen können, fehlt hingegen oft noch das Wissen über die Quantentechnologien. Auch wenn sich das langsam zu ändern beginnt, ist es eine schwierige Herausforderung. Es gibt allerdings eine Vielzahl von Firmen, die Teilkomponenten anbieten, die für die Entwicklung im Betrieb eines Quantencomputers benötigt werden: Vakuumtechnik, Kryostaten, Hochfrequenztechnik, Messtechnik und Laser sind nur einige Beispiele. In Deutschland sind in diesem Bereich vor allem viele kleine und mittlere Unternehmen, wie TOPTICA Photonics, aktiv. Sie arbeiten seit Jahren eng mit Forschern zusammen und besitzen daher die notwendige Expertise und innovative Produkte. Weil der gesamte Markt noch klein und aufgrund der Vielzahl verschiedener technologischer Ansätze auch noch hoch spezialisiert ist, müssen hier finanzielle Anreize, etwa durch die Übernahme von Entwicklungskosten, geschaffen werden.

Glücklicherweise ist die Entwicklung von Quantencomputern ganz eng mit anderen Quantentechnologien verknüpft, von denen einige deutlich früher Marktreife erreichen werden. Beispiele sind Sensoren und Uhren mit höherer Genauigkeit. Quantennetzwerke sind nicht nur essenziell für die Vernetzung von Quantencomputern, sondern sie können auch die Kryptographie revolutionieren. Diese Synergien und die damit verbundenen wirtschaftlichen Chancen sollten nicht ungenutzt bleiben.

Die Europäische Kommission und das BMBF haben das erkannt und mit dem Flaggschiff-Programm zu Quantentechnologien bzw. der deutschen Initiative für Quantentechnologien „QUTEGA“ sehr gute Förderprogramme aufgelegt.

Auch durch die Schaffung von Märkten für Quantentechnologien, beispielweise über die Nachfrage von Quantenkryptographie-Systemen, kann der Staat eine wichtige Rolle einnehmen. Ein weiterer Baustein zum Erfolg ist die internationale Kooperation. Die schnellsten Fortschritte erzielt man bei einer solchen Mammutaufgabe wie dem Quantencomputer durch Zusammenarbeit und Partnerschaften, und zwar über Grenzen zwischen verschiedenen Fachdisziplinen, zwischen Wissenschaft und Wirtschaft sowie über Ländergrenzen hinweg.

Auch der kommerzielle Erfolg ist abhängig von Partnerschaften mit den besten internationalen Akteuren und einem offenen globalen Markt. Ich hoffe, dass diese öffentliche Anhörung auch zu einem breiteren Verständnis, einer breiteren Diskussion des Themas führt. Ein gutes und realistisches Verständnis der Chancen und Herausforderungen in der Öffentlichkeit sollte entstehen. Dabei darf nicht vergessen werden, dass der Quantencomputer ein langfristiges Ziel des riesigen Gebiets der Quantentechnologien ist. Diese werden kommen und wir sollten die Chance nicht verstreichen lassen, davon wirtschaftlich und gesellschaftlich zu profitieren.

SV **Prof. Dr. Frank Wilhelm-Mauch**: Vielen Dank. Es ist mir eine große Ehre und ein großes Vergnügen, hier zu diesem Zeitpunkt über unser Gebiet berichten zu dürfen. Der Zeitpunkt ist sehr interessant. Quantum Computing gibt es in der Wissenschaft als abstraktes Forschungsgebiet schon sehr lange mit einer kleinen Community. Ich selber arbeite auf diesem Gebiet seit achtzehn Jahren und es gibt einige, die noch deutlich länger dabei sind. Aber wir haben die meiste Zeit über hypothetische Computer oder auch über einzelne Bauelemente geredet. Seit etwa vier Jahren ist die Idee eines programmierbaren Computers tatsächlich greifbar. Sie können sich in der Cloud kostenlos daran versuchen. Seit etwa einem Jahr gibt es auch ökonomisches Interesse von Firmen, die wissen wollen, was diese neue Technologie bringt.

Das geht im Augenblick alles sehr schnell. Selbst ich, als theoretischer Physiker und Grundlagenforscher darf jetzt gemeinsam mit Firmen Doktorarbeiten betreuen, was normalerweise ein Privileg der Ingenieure ist. Als mein Postdoc Geld besorgen wollte, um einen Business-Plan zu schreiben, hatte er bereits Kunden. Er hat daher diese Phase übersprungen und gleich sein Spin-off gegründet. Tatsächlich hat sich sogar in der letzten Stunde etwas geändert. In dieser Zeit haben wir erfahren, dass die europäische Flaggschiff-Initiative sich dafür entschieden hat, wen sie in der ersten Runde fördern möchte. Ich bin sehr froh darüber, dass sich das von mir koordinierte Konzept des Konsortiums durchgesetzt hat. Deshalb sehen Sie mich auch ein wenig derangiert.

Eine solche Situation führt aber oft auch dazu, dass manchmal Nachrichten kommen, die übertrieben sind. Man könnte auch von einer Blase sprechen. Deshalb habe ich mir in meiner Stellungnahme Mühe gegeben, immer zu sagen, wo die Quantenbeschleunigung bewiesen ist und wo man noch spekuliert. Beschleunigung heißt hier nicht die nächstschnellere Clock frequency (Taktfrequenz), sondern es bedeutet, es werden Aufgaben für den Computer zugänglich, die vorher unzugänglich waren. Ich glaube, wenn man sich auf das konzentriert, was man weiß, und dann noch auf das hofft, an dem man gerade arbeitet, ist das Gebiet vielversprechend genug, um etwas zu erreichen. Sie sehen uns auch in einem Stadium, das vielleicht der klassischen „Computerei" der 50er Jahre ähnelt. Damals liefen Computer in Großrechenzentren. Sie waren empfindlich und die Anwendungen, die man kannte, Kryptologie und Entwicklungswerkzeug, waren auch hauptsächlich Anwendungen, mit denen man im Alltag tatsächlich wenig zu tun hatte.

Auf dieser Basis beurteilen wir das gerade, vor allem als Technologie im Bereich des High-Performance Computing (HPC). Durch die neuen Benutzer, auch Interessenten aus der Industrie, kann sich das natürlich ändern. Möglicherweise sieht meine Stellungnahme irgendwann so aus, wie die Stellungnahme des früheren IBM CEOs Thomas J. Watson, der angeblich gesagt hat, es

gäbe einen Weltmarkt für fünf Computer. Deshalb haben wir hier eine Momentaufnahme, basierend auf dem derzeitigen Wissensstand.

So, wie wir schnell aus der Grundlagenforschung kommen, ist natürlich die internationale Kooperation für uns eine ganz wichtige Sache. Wir brauchen einen offenen Austausch von Ideen und Konzepten, einschließlich des Austauschs gelegentlicher Misserfolge, um wirklich als Community weiterzukommen. Das ist wichtig, auch im Hinblick auf Dinge, die wir in Deutschland tun können. Wir sehen im Augenblick Anbieter von außerhalb der EU, die große Plattformen erstellen und die im Augenblick noch sehr offen sind. Ich hoffe, dass die offen bleiben. Aber man kann sich nicht sicher sein. Es ist wichtig, eine davon unabhängige Plattform zu haben, um offene Standards zu haben, um zu wissen, was dort wirklich passiert und um die Software nah an der noch unvollkommenen Hardware entwickeln zu können.

Wenn wir anschauen, welche Initiativen es in anderen Ländern gibt, gibt es einige Singularitäten, insbesondere in den USA. Ein interessanter Referenzpunkt in der EU ist möglicherweise Schweden. Dort wurde gerade ein Programm für eine Plattform im Wert von 100 Mio Euro aufgelegt. Es gibt vorbildliche Programme in der Schweiz und auch in Großbritannien. Ich glaube, es ist wichtig, dass wir dorthin kommen, dass wir hier vor allen Dingen die Technologie und das Engineering, das wir brauchen, um weiterzukommen, entwickeln. Das ist in der Tat jenseits von Universitäten.

Das Allerwichtigste sind aber gut ausgebildete Leute. Es ist wichtig, dass die Menschen, die Quantencomputer einmal nutzen werden, jetzt ausgebildet werden und in der Industrie sind, damit sie das in ihrer neuen Umgebung gut umsetzen können. In der Innovationsforschung redet man oft von einer Spannweite von etwa zehn Jahren. Da geht es vor allen Dingen jenseits unserer kleinen engen Community um den zukünftigen Quanteningenieur, die zukünftige Quanteningenieurin, den zukünftigen Lehrer oder die zukünftige Informatikerin, die genau die richtige Quantenphysik kennen müssen, damit wir hier interdisziplinär und bis hin zu realen Computern weiterkommen.

SV **Prof. Dr. Marian Margraf**: Auch ich möchte mich für die Einladung bedanken. Meine Arbeitsgruppe und ich kümmern uns in erster Linie um das Thema IT-Sicherheit. Wir haben bereits viel darüber gehört, was Quantencomputer alles leisten können. Das betrifft die IT-Sicherheit leider ein bisschen negativ, denn wir wissen, wenn es irgendwann Quantencomputer gibt, dann können die de facto alle kryptographischen Verfahren, also gerade die asymmetrischen Verfahren, die wir heute einsetzen, brechen. Es würde uns auch nicht helfen - was zurzeit das Übliche ist -, die Schlüsselmengen deutlich zu vergrößern. Das klappt da leider nicht. Wir kennen seit Mitte der 90er-Jahre Quantenalgorithmen, die ziemlich große Auswirkungen auf diese Kryptographie haben.

Das Problem ist, dass praktisch alle unsere Internetkommunikationen oder auch Kommunikationen über VPNs (Virtual Private Network) auf diesen asymmetrischen Verfahren, die gebrochen werden können, basieren. Daher muss man jetzt schon die Zukunft vorbereiten, entsprechende andere Algorithmen zu entwickeln. Da gibt es einige Ideen. Aber wovor ich warnen möchte ist, sich damit nicht zu viel Zeit zu lassen. Die meisten Experten gehen davon aus, dass Quantencomputer 2030 in einer anständigen Größe existieren. Da hat man jetzt noch zwölf Jahre Zeit. Aber seit Snowden wissen wir, dass viel Internetkommunikation von den amerikanischen Geheimdiensten aufgenommen wird und damit nachträglich entschlüsselt werden kann, sobald es Quantencomputer gibt.

Ich plädiere dafür, in die sogenannten quantencomputerresistenten Kryptoverfahren deutlich mehr Forschungsinitiative, also viel mehr Finanzmittel, zu investieren. Es gibt gewisse Ideen, wie man das umsetzen kann; bei einigen davon weiß man schon, dass sie sehr sicher sind. Man könnte heute schon Signaturverfahren einsetzen, die auf Hashfunktionen basieren, und

alle Experten gehen davon aus, dass sie sicher sind, aber bei anderen kryptographischen Protokollen - Schlüsseleinigung, Schlüsselaustausch - gibt es noch einige Unsicherheiten. Entweder Unsicherheiten oder wir kennen nur ineffiziente Algorithmen, da muss jedenfalls mehr Forschungsarbeit geleistet werden.

SV **Prof. Dr. Hendrik Bluhm**: Ich bin ebenfalls Experimentalphysiker und arbeite an halbleiterbasierten Implementierungen von Quantencomputern an der RWTH (Rheinisch-Westfälische Technische Hochschule Aachen) und auch am Forschungszentrum Jülich. Ich möchte mich bei dem Ausschuss für die Einladung bedanken. Ich muss vorweg noch betonen, dass der Ursprung meiner Nominierung als Experte nicht unbedingt meine politischen Ansichten widerspiegelt. Dementsprechend freue ich mich, dass mein Erscheinen hier mehrheitlich befürwortet wurde. Ich hoffe, dass wir unabhängig von Parteipolitik einen sachbezogenen Austausch pflegen können. In diesem Sinne jetzt zum Thema.

Ich denke, die Bedeutung der derzeitigen Informationsverarbeitungstechnologie brauche ich nicht weiter zu betonen, die ist hier täglich erfahrbar. Aber trotz der rasanten Entwicklung gibt es Bereiche, Probleme, die noch nicht lösbar sind, jedenfalls nicht praktisch ab einer gewissen Größe.

Das ist die große Versprechung von Quantum Computing, dass einige dieser Probleme, aber eben nicht alle, dann doch lösbar gemacht werden könnten. Das basiert - wie eingangs beschrieben - auf der Verwendung grundlegend neuer Konzepte aus der Quantenmechanik. Man kann sagen, dass ist die größte Revolution der Informationsverarbeitung, seit wir angefangen haben, überhaupt Steinchen zu zählen oder einen Abakus zu verwenden.

Wichtiges Beispiel dazu, das auch zu den am besten erforschten zählt, ist die Simulation von chemischen Prozessen zur Realisierung effizienterer Verfahren: Düngemittelherstellung, CO_2-Bindungen werden genannt. Man könnte Materialien mit besonderen Eigenschaften gezielter entwickeln. Das zeigt, dass eine recht konkrete Perspektive besteht für Anwendungen mit erheblichem gesellschaftlichem und wirtschaftlichem Nutzen.

Wie schon angesprochen, steht das Feld nach etwa zwanzig Jahren Grundlagenforschung, die ursprünglich von reiner Neugier getrieben war, an der Schwelle zur Technologieentwicklung. Es gibt erste Kommerzialisierungsschritte, insbesondere in den USA. Deren Reifegrad wird in Pressemitteilungen oft am Rande des Ehrlichen aufgebauscht. Es ist nicht ganz falsch, aber der Eindruck, der entsteht, ist etwas übertrieben. Man sollte nicht vergessen, dass es in den Details der Umsetzung noch erhebliche Unsicherheiten, Unabwägbarkeiten gibt. Auch die Anwendbarkeit der Systeme, die sich in den nächsten Jahren zeigen werden, ist Gegenstand der Forschung und lässt sich momentan noch sehr schwer einschätzen. Dennoch glaube ich, dass langfristig das Potenzial deutlich gegeben ist. Man darf es eben bloß nicht überbewerten und nicht unbedingt alles glauben, was gehypt wird.

In Europa ist in der Forschung eine sehr hohe Kompetenz vorhanden, aber die Technologieentwicklung ist - nicht zuletzt aufgrund von bislang fehlender oder erst vor kurzem ins Leben gerufener gezielter Förderprogramme - hinter den Aktivitäten in den USA zurückgeblieben. Aber wie schon gesagt, mit dem anlaufenden EU-Flaggschiff und dem Programm der Bundesregierung sind die wesentlichen Weichen gestellt, dies zu ändern. Ich bin gespannt zu sehen, wie das anläuft.

Wichtig ist nun, dass diese Projekte auch zielführend umgesetzt werden, und zwar mit einer langfristigen Perspektive. Dabei ist vor allem wichtig, nicht nur die Forschung voranzutreiben, sondern auch an den Industrietransfer zu denken, an primär lokal agierende Unternehmen in Deutschland und Europa. Eine Schwierigkeit dabei ist, dass die vornehmlichen Unternehmensstrategien, insbesondere Großindustrie und Halbleiterindustrie, eher risikofern und auf kurzfristige Profite ausgerichtet

sind, so dass das kein Selbstläufer sein wird. Das erfordert gemeinsame Anstrengung von Politik, Wissenschaft und der Industrie.

In diesem Sinne werden wir eine konkrete Anwendung für allgemeine Technologien mit sehr langfristigen und risikobehafteten Entwicklungspotenzial haben und daher sollte vielleicht darüber nachgedacht werden, ob man nicht Industrieprojekte auch zu Vollkosten fördern könnte, um eben dort gezielt das Know-how aufzubauen. Derzeit ist das, soweit ich weiß, durch die zuwendungsrechtlichen Rahmenbedingungen nicht möglich. Aber ich glaube, ich bin hier an der richtigen Adresse, um das vielleicht zu ändern, wobei das auch mit EU-Recht zu tun hat. Ein ganz konkretes Beispiel dazu: Vor etwa zehn Jahren haben wir die ersten Anfänge des jetzt sehr sichtbaren Programms von IBM noch belächelt als improvisierte Slights. Jetzt ist das eine der sichtbarsten und größten industriellen Aktivitäten. Die hat, in der Zwischenphase zumindest, ganz massiv von vollkostengeförderter Forschungsförderung durch die amerikanische Regierung profitiert. Das geht meines Wissens in der Form in Europa derzeit nicht.

Zum Stichwort Europa: Auch eine effektive europäische Zusammenarbeit ist sehr wichtig, weil nur auf dieser Basis die Kompetenz gebündelt und eine kritische Masse erreicht werden kann. Oft wird gefragt, wie profitiert Deutschland, wenn viel Geld in die Forschung gepumpt wird. Ich glaube, es ist durchaus möglich, dadurch Kompetenz zu binden und nach Europa zu holen; und das angesprochene Projekt, das Kollege Frank Wilhelm-Mauch koordiniert, ist ein sehr gutes Beispiel dafür, wie genau das geschehen kann. Zum Schluss möchte ich noch Folgendes sagen: Obwohl mir persönlich die Hardware-Entwicklung sehr am Herzen liegt, ist es noch viel wichtiger, Software zu fördern, um keine Abhängigkeit von amerikanischen Firmen herbeizuführen. Es wäre noch viel fataler, Computer importieren zu müssen und diese gar nicht nutzen zu können. Auch hier muss ein Förderprogramm entsprechend Akzente setzen.

SV **Prof. Dr. Dr. h. c. Johannes Buchmann:** Vielen Dank für die Einladung. Sehr geehrte Abgeordnete, ich möchte etwas zu dem Zusammenhang zwischen Quantentechnologie und Computersicherheit sagen. Ich bin Professor für Informatik und Mathematik an der TU Darmstadt. Ich beschäftige mich seit fünfzehn Jahren mit den kryptographischen Verfahren, die auch noch sicher sein sollen, wenn es mal die Quantencomputer gibt.

Das Thema Quantentechnologie und Computersicherheit hat zwei Aspekte: Zum einen ist Quantentechnologie eine große Bedrohung für die gegenwärtige Computersicherheit. Zum anderen ist Quantentechnologie eine große Chance für neue Schritte in der Computersicherheit. Internetsicherheit hängt von der sogenannten Public-Key-Kryptographie ab. Wenn Sie beispielsweise Ihr Homebanking machen, wollen Sie, dass niemand den Pin sieht. Oder wenn Sie eine neue App auf Ihr Smartphone laden, wollen Sie keine Schadsoftware. Damit das garantiert wird, ist die Public-Key-Kryptographie wichtig.

Die Quantencomputer können die Public-Key-Kryptographie, die wir heute kennen, komplett brechen. Wenn es morgen Quantencomputer gibt, ist unsere gesamte Internetsicherheit in Gefahr. Daraus folgt, dass man etwas machen muss. Wir haben gehört, es kommt bald, aber keiner weiß, was „bald" heißt. Also muss man schon heute etwas machen. Die Sachen, die heute vertraulich sein sollen für die nächsten zwanzig Jahre, sind es nicht mehr in dem Augenblick, wo es die Quantencomputer gibt. Also: Heute anfangen!

Wir können das Problem lösen. Es gibt eine Menge Forschung. Wir haben auch selber dazu beigetragen. Dazu könnte ich in der Befragung gerne mehr sagen; was die Perspektiven sind. Ich will noch ein paar Minuten etwas zur Chance sagen: Digitalisierung ist ubiquitär, also alles wird digitalisiert. Zum Beispiel Genomdaten, Gesundheitsdaten etc. Wir brauchen sehr langfristigen Schutz, solange wie die Menschen leben, oder darüber hinaus, denn ihre Kinder haben so ähnliche Gene wie sie selbst. Sollen wir

das schützen? Das können wir technologisch heutzutage mit der Kryptographie, die wir haben, nicht. Aber die Quantenkryptographie kann einen Beitrag dazu leisten, in Kooperation mit der Informatik, Systeme entwickeln, die richtig langfristig sicher sind. Wir haben in Darmstadt einen von der Deutschen Forschungsgemeinschaft geförderten Sonderforschungsbereich, der sich mit dem Thema „langfristige Sicherheit" als ganz essentielles Thema beschäftigt - und da wird die Quantentechnologie eine große Rolle spielen. Es gibt entsprechende Experimente und es gibt Dinge im Vorfeld. Das wollte ich Ihnen auch als Ausschuss ans Herz legen, wenn ich mir erlauben darf, das zu sagen. Damit möchte ich meine Stellungnahme abschließen.

SVe **Prof. Dr. Stephanie Wehner:** Sehr geehrter Herr Vorsitzender, sehr geehrte Abgeordneten, sehr geehrte Damen und Herren, kurz zu meiner Person: Ich bin Professor am Institut QUTech an der Technischen Universität Delft/Holland. Ich bin auch Roadmap Leader, also Leiter der Abteilung für Quantennetzwerke im Quanteninternet und Quantum-Computing-Bereich. Das sind sowohl Professoren als auch Ingenieure. Ich vertrete die wissenschaftliche Gemeinschaft in Holland in dem Quantum Community Network im Flagship. Ich bin auch sehr froh, sagen zu können, dass ich Koordinatorin der Quantum Internet Alliance Project in Europa bin, bei dem Dr. Stephan Ritter und ich an Quantennetzwerken zusammenarbeiten. Aufgrund meiner Einladung stehe ich Ihnen gerne zur Verfügung zu Fragen über Quantenkommunikation und Quantenkryptographie. Ich beantworte aber auch gerne Ihre Fragen über Quantum Computing im Allgemeinen oder über das Institut QUTech in Holland.

Was ist Quantenkommunikation? Unter Quantenkommunikation versteht man das Versenden von Quantenbits, also Qubits über Abstände. Das ist das Analog für die Datenübertragung von heute. Das kann man über Glasfaser machen, also die, die sich jetzt schon in der Erde befinden.

Was kann man damit machen? Quantennetzwerke haben eine ganze Reihe von Anwendungen. Die bekannteste davon ist wohl Quantenkryptographie oder Quantum Key Distribution, bei der man einen Schlüssel austauscht für die sichere Datenkommunikation und die Sicherheit gewährleistet, selbst wenn der Angreifer einen Quantencomputer besitzt. Andere Anwendungen von Quantenkommunikation sind zum Beispiel Password Identification, das Synchronisieren von Uhren und auch der sichere Zugang zu Quantencomputern, die weit weg sind. Das kann ich später noch näher erklären.

Quantenkommunikation ist auch interessant auf kleinen Abständen, nämlich indem man Quantencomputer miteinander verbindet, um einen größeren Quantencomputer zu bauen. Das ist analog zu einem Computing Cluster im klassischen Computer. Was ist der heutige Stand? Anders als beim Quantum Computing ist Quantenkommunikation teilweise schon kommerziell erwerbbar. Man kann ein Paket kaufen, das Quantum Key Distribution macht und auf einen Abstand bis ungefähr einhundert Kilometer anwenden. Hier ist die Schwierigkeit, eine Kommunikation über längere Abstände zu führen und auch mehr Anwendungen zu unterstützen als nur Quantum Key Distribution.

Im akademischen Bereich hat man schon einige Tests durchgeführt. Beispielsweise hat China via Satelliten über eine Distanz von 1.203 Kilometern eine Verbindungen zwischen zwei Orten in China hergestellt. Allerdings nicht deterministisch, d.h., man kann es noch nicht für die sichere Kommunikation gebrauchen. Um längere Abstände auf dem Boden herzustellen, muss man etwas bauen: einen Quantum Repeater - und den gibt es noch nicht. Alle Quantennetzwerke, die man heute im Internet findet - wenn Sie Quantennetzwerke googeln - sind welche, bei denen man die 100 Kilometer langen Stückchen aneinandergeklebt und deshalb keine End-to-end-Security hat.

Was sind die Bestrebungen außerhalb Deutschlands? In China gibt es sehr große Bestrebungen in diesem Bereich von

Quantentechnologie mit einem Umfang von 10 Mrd. Euro. Das meiste davon ist investiert in Hefei. Ich weiß nicht genau, was davon im Quantenkommunikationsbereich liegt. Allerdings sind die Efforts dort sehr extensiv. China engagiert sich mit diesem Experiment auch sehr in der Weltraumforschung mit Satelliten sowie auf der Erde im Bereich Repeaters. Ich schätze, dass China im Weltraum vorne liegt, und wir auf der Erde. Es gibt auch etliche Industrie, die diese Schachteln macht, also Content Key Distribution, die die Anwendungen selber machen. Zum Beispiel in Japan Toshiba, NEC, Mitsubishi und in Europa ID Quantique. Es gibt kleine Testnetzwerke, die diese 100 Kilometer langen Stückchen aneinanderkleben. Aber ansonsten gibt es bis jetzt noch nichts.

In den Niederlanden haben wir den Plan, dass wir 2020 ein Netzwerk bauen, das mehr kann als Quantum Key Distribution, nämlich das kleine Quantencomputer in verschiedenen Städten miteinander verbindet.

Was erwartet man als Timeline? Das ist schwer einzuschätzen. Ich denke, dass es wahrscheinlich möglich ist, innerhalb von fünf Jahren sternförmige Netzwerke zu machen, die die Glasfiberinfrastruktur besser nutzen als die Point-to-point Connections. Long Term Repeaters ist natürlich eine Frage der EU Scientific Research Agenda. Man geht davon aus, dass man innerhalb von sechs Jahren Milestone-Experimente für den Proof of Principle (Machbarkeitsbeweis) im Labor durchführen und dann innerhalb von zehn Jahren mehrere Stücke aneinander außerhalb des Labors demonstrieren kann.

Man kann vieles nennen, das wichtig ist für die Weiterentwicklung. Ich kann mich meinen Kollegen nur anschließen, dass eine starke Zusammenarbeit zwischen verschiedenen Fachbereichen der Wissenschaft als auch zwischen dem akademischen und dem industriellen Bereich sehr wichtig ist. Ich möchte einen Punkt hervorheben: Ich denke, dass es wichtig ist, selbst kleinen Entwicklern - beispielsweise einem Softwareentwickler - zu ermöglichen, ein Softwareprodukt zu entwickeln für Quantennetzwerke. Das wäre sehr nützlich für die Entwicklung. Es ist aber so, dass Quantentechnologie sehr teuer ist und nicht jeder Zugang dazu hat. Einer meiner Vorschläge: Vielleicht sollte man darüber nachdenken, wie man ein Testbed oder Quantentechnologie mehreren Leuten zugänglich machen kann, die diese zur Entwicklung nutzen können.

SV **Prof. Dr. Winfried Hensinger**: Vielen Dank für die Einladung. Ich freue mich sehr, hier zu sein. Ich bin Direktor des Sussex Centre for Quantum Technologies und Leiter der Sussex Ion Quantum Technology Group an der Universität Sussex. Ich leite dort ein Team von 30 Wissenschaftlern und wir sind dabei, dort einen Quantencomputer zu bauen. Vielleicht erzähle ich Ihnen erstmal etwas zu meinem Hintergrund:

Ich war seit 20 Jahren nicht mehr in Deutschland und habe in Australien, Amerika und in den letzten 13 Jahren in England gearbeitet. Ich bitte Sie, mein „rostiges" Deutsch zu entschuldigen.

Lassen Sie mich damit anfangen: Was ist eigentlich die Quantenphysik? Einstein betrachtete die Quantenphysik als gespenstisch. Da gibt es die Möglichkeit, dass ein mechanisches Objekt an zwei Orten gleichzeitig ist. Es kann also sein, dass Sie hier im Ausschuss sitzen und gleichzeitig zu Hause einen Kaffee trinken. Das gibt es wirklich in der Quantenphysik. Leider haben wir das noch nicht mit Menschen geschafft, aber mit Atomen funktioniert es. Man kann wirklich ein Atom an zwei Orten gleichzeitig haben. 30, 40 Jahre haben die Quantenphysiker das eigentlich gar nicht glauben können. Einstein hat es nicht glauben können, dass solche Sachen überhaupt funktionieren. Es wurden viele Experimente gemacht.

Vor circa 20 Jahren haben sie es einfach glauben müssen, denn alle diese Experimente haben immer wieder gezeigt, dass die Quantenphysik wirklich funktioniert und stimmt. Da haben sich die Quantenphysiker überlegt, ob es vielleicht möglich ist, diese Effekte, diese Phänomene, auszunutzen, um eine Maschine zu bauen, die manche Probleme lösen kann, wenn also auch der schnellste Supercomputer Millionen von Jahren

benötigen würde, um das berechnen zu können. Das klingt alles wunderbar. Aber leider ist das Problem, dass es unglaublich schwierig ist, solche Quantenphänomene zu kontrollieren in dem Sinne, wie man es braucht, um einen Quantencomputer zu bauen. Seit vielen Jahren haben Physiker versucht, das zu schaffen. Ein Quantencomputer würde wahrscheinlich als eine der größten technischen Errungenschaften zählen, weil es so unglaublich kompliziert ist, diese Quantenphänomene zu bändigen.

In den letzten paar Jahren hat sich herauskristallisiert, dass bei zwei physikalischen Systemen die Fehlerraten gering genug sind, um solche Maschinen bauen zu können. Eins dieser Systeme sind supraleitende Qubits. Das ist ein sehr tolles System und es wurden fantastische Fortschritte gemacht. Der Grund, weswegen ich mich dann entschieden habe, nicht an diesem System, sondern an Ion-Systemen zu arbeiten, ist, dass man die supraleitenden Qubits bis 273 Grad Celsius, also fast bis zum absoluten Nullpunkt, kühlen muss. Die Ionen funktionieren bei Zimmertemperatur oder mit ganz leichter Kühlung.

Ist es einfacher einen Quantencomputer mit Ionen zu bauen? Nein, überhaupt nicht! Da gab es immer noch riesige Probleme, sowas zu schaffen. Eins, von diesen Problemen ist gewesen, dass man, um logische Operationen in einem Quantencomputer bauen zu können, für jedes Qubit zwei Laserstrahlen braucht. Um die richtig interessanten Probleme zu lösen, bräuchte man wohl Millionen oder Milliarden von Laserstrahlen. Da können Sie sich vorstellen, eine Maschine zu bauen, bei der man Millionen oder Milliarden Laserstrahlen auf einzelne Atome ausrichten müsste, wäre natürlich eine ganz schöne Herausforderung.

Wir hatten uns lange darüber Gedanken gemacht und dann vor zwei Jahren eine neue Methode entwickelt, bei der wir keinen Laserstrahl mehr brauchen, um solche Operationen auszuführen, sondern wir legen Spannungen in einem Mikrochip an, um dann solche logischen Operationen durchzuführen. Daraufhin, ein Jahr später, haben wir zusammen mit Wissenschaftlern von Google, der Universität Siegen und vielen anderen Universitäten einen Bauplan verfasst. Mit diesem Bauplan haben wir gezeigt, dass es jetzt wirklich möglich ist, einen großen leistungsfähigen - da heißt es dann wirklich Millionen oder Milliarden von Qubits - Quantencomputer zu bauen. Das bedeutet nicht, dass es einfach ist. Man muss wirklich eine ingenieurwissenschaftliche Meisterleistung vollbringen, um sowas hinzukriegen. Es ist überhaupt nicht einfach. Dann ist natürlich auch die Politik gefragt, denn sowas benötigt einen Rieseneinsatz von Menschen und Mitteln. Ich glaube, die Möglichkeiten sind eben so fantastisch, dass es sich wirklich lohnt, eine solche Maschine zu bauen.

Der **Vorsitzende**: Vielen Dank. Nun besteht die Möglichkeit der Fragen. Ich beginne mit der CDU/CSU-Fraktion, Abg. Beermann, bitte.

Abg. **Maik Beermann** (CDU/CSU): Ich bin mit einer geringen Vorstellung in diese Anhörung gekommen und hatte Sorge, dass ich nach den Meinungen und Statements der Experten nicht unbedingt verstehe, was konkret mit Quantum Computing gemeint ist bzw. was Sie konkret machen. Aber Sie haben das aus meiner Sicht wirklich eindrucksvoll rübergebracht, so dass wir da auf jeden Fall schon auf einem neuen Level sind. Besten Dank! Sie haben aber auch deutlich gemacht, welche Herausforderungen für die Zukunft vorhanden sind.

Oftmals ist es so, dass man der Politik im Bereich der Digitalisierung häufig vorwirft, eine Legislaturperiode zu spät dran zu sein mit dem, was man tun. Vielleicht gelingt es uns tatsächlich, bei diesem Thema anders vorzugehen.

Ich höre heraus, dass wir - ich will nicht sagen, komplett in den Kinderschuhen stecken - noch sehr am Anfang dieser speziellen, neuen und dennoch wichtigen Technologie sind. Ich stelle meine Fragen an Prof. Bluhm und Prof. Wilhelm-Mauch. Sie haben in Ihren Ausführungen bereits darauf hingewiesen, dass Förderprogramme wichtig sind und dass diese auch politisch begleitet werden sollten. Meine Anmerkung ist

aber zudem, dass ich persönlich, als Politiker im Deutschen Bundestag, auch den Anspruch habe, dass wir bei bestimmten Technologien weltweit federführend sind. Daher meine Frage: Was kann Politik konkret noch tun, um dieses Thema zu begleiten und das anzustrebende Ziel zu erreichen? Und zwar in einer Art und Weise, dass wir in Deutschland, aber vielleicht auch aufgrund der Vernetzung in Europa, an der Weltspitze stehen? Wie können wir eine zukunftsfähige deutsche Technologie schaffen oder Vorreiter bei dieser Technologie werden?

Abg. **Dr. Jens Zimmermann** (SPD): Ich empfand es auch als einen sehr spannenden Einstieg in die Debatte. Ich habe ein bisschen an Fusionsreaktoren - das ist wahrscheinlich böse, das bei Ihnen zu sagen - gedacht. Aber ich habe den Eindruck, das geht alles schneller bei Ihnen. Ich möchte Prof. Wilhelm-Mauch und Prof. Heusinger eine relativ simple Frage stellen: Ich habe verstanden, dass es erste Formen von Quantencomputern gibt, dass ein großes amerikanisches Unternehmen erwähnt worden ist und dass das Unternehmen schon etwas anbieten kann. Meine Frage ist, für Leute, die sich nicht jeden Tag damit beschäftigen: Wo befinden wir uns genau? Was ist das, was aktuell verfügbar ist? Wie ist das von den Fähigkeiten her anzusehen, was ist das und was kann das? Was ist der Maßstab und wo wollen Sie hin? Erster Quantencomputer im Jahr 2030 ist in Ihren Eingangsstatements genannt worden. Sie haben von Plattformen gesprochen. Was ist das eigentlich genau? Aber im Prinzip ist die Frage relativ simpel: Wo stehen wir aktuell und wo ist das im Vergleich zu dem, wo Sie hin wollen?

Abg. **Uwe Schulz** (AfD): Ich habe viel gelernt. Ich habe mir alle Ihre Unterlagen angeschaut, habe mir die Nummer für Nummer nebeneinander gelegt und habe dann auch noch ein wenig im Internet recherchiert, und war etwas betroffen - Herr Prof. Buchmann, bei Ihnen war es ganz besonders deutlich - , als Sie in Ihrem Vortrag ausführten, dass wir ein echtes Sicherheitsproblem haben. Ich denke, das muss noch näher beleuchtet werden im Laufe der Zeit. Denn irgendwann überrennt uns eine Nation oder jemand mit einem Quantencomputer und unsere Sicherheitsmechanismen sind ausgehebelt.

Herr Prof. Hensinger, Sie haben das Wort nicht benutzt, aber es kam zum Vorschein - der Brain Train in Deutschland. Sie sind selbst ein Brain Trainer. Sie sind weggegangen, sind sehr lange nicht mehr in Deutschland gewesen. Das ist auch ein Riesenthema, das wir in diesem Ausschuss unbedingt stressen müssen. Meine spezielle Frage, zu der ich in Ihren Ausführungen, die sehr wertvoll waren, keine Antwort gefunden habe, geht an Dr. Ritter.

Sie sind für ein Unternehmen tätig. Wie sieht es aus mit der Technologieabsicherung im Falle Quantencomputer? Gibt es Patente? Gibt es Länder, die besonders viele Patente einheimsen? Wie sieht es aus mit Patenten zur Technologieabsicherung in Sachen Quantencomputer?

Abg. **Manuel Höferlin** (FDP): Vielen Dank für die Ausführungen. Ich verstehe bei Quantencomputern eher unterdurchschnittlich viel, weil es mir einfach - wie Sie so schön sagen - unvorstellbar ist. Ich kämpfe immer noch etwas damit, aber es ist hochinteressant und wir lernen gerne. Ich möchte zwei Punkte ansprechen, Professor Buchmann.

Die Kryptographie von heute ist vorbei. Die gute Nachricht ist, Kryptographie von morgen ist machbar. Wir haben derzeit in einer WSI-Studie (Wirtschaft- und Sozialwissenschaftliches Institut) den Entwicklungsstand zu Quantencomputern beleuchtet bekommen. Dort wurde ein Punkt nicht berücksichtigt und vielleicht können Sie uns dazu etwas sagen. Dort gibt es ein Forschungsergebnis von dem Hersteller D-Wave, der bereits Grundlagen oder Teile von einer Technik entwickelt hat, die, sobald sie noch ein bisschen mehr Qubits verarbeiten können, möglicherweise - so habe ich es verstanden - sehr bald RSA-Schlüssel knacken. Wir hatten verschiedene Zeithorizonte gehört, fünf Jahre, sechs Jahre, vielleicht geht das auch schneller. Für mich ist die spannende Frage, wie schnell wir sein werden, um eine neue Art von Kryptographie

zu denken und vorzubereiten, damit wir nicht - wie das oft geschieht - dann, wenn etwas passiert, wieder Jahre brauchen, um eine Gegenstrategie zu entwickeln. Der schlimmste Fall wäre, es gibt einen Quantencomputer und wir erfahren davon aus der Presse.

Der zweite Punkt ist: Halten Sie die Ansätze, wie sie bisher zur Technikfolgenabschätzung gemacht wurden, für ausreichend? Wie und was kann man machen? Was würden Sie uns als Gesetzgeber empfehlen, vielleicht auch der Regierung, die wir dann gerne auch mit Haushaltsmitteln unterstützen können, damit man dort frühzeitig die Technikfolgenabschätzung so gestaltet, dass wir da zumindest zeitlich gleichziehen. Ich will gar nicht sagen, dass wir als Politiker der Entwicklung vorgreifen wollen. Aber zumindest wollen wir nicht so weit hinterher hinken.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ich habe eine Frage an Professor Wehner. Ich möchte gerne wissen, wie Politik dazu beitragen kann, dass die Fortschritte im Bereich Quantum Computing am Ende nicht nur der Wirtschaft zugutekommen, sondern wie man sicherstellt, dass auch gemeinwohlorientierte Entwicklungen eine Chance haben. Das ist deshalb schwierig, weil es eine sehr teure Technologie ist, gerade jetzt am Anfang werden viele Dinge entwickelt und patentgeschützt. Wie weit spielt da zum Beispiel Open Access als Strategie eine Rolle, die wir generell gut finden und vertreten, wenn irgendwo Fördergelder hineinfließen.

Wie kann man die Möglichkeiten der Quantentechnologie nicht nur denen mit viel Geld zur Verfügung stellen, sondern auch kleinen Startups, Einzelpersonen usw., um Chancengleichheit herzustellen?

Meine zweite Frage geht auch an Professor Wehner. Was ist vorstellbar an Veränderungen für Forschung und Wissenschaft, wenn Simulationen mit Quantencomputern möglich wären. Wir haben schon einzelne Beispiele gehört. Aber mich würde noch interessieren, in welchen Bereichen das außerdem denkbar wäre. Wo könnte es Beschleunigungen, Durchbrüche oder Wege geben, die nur mit Quantencomputer vorstellbar oder denkbar sind?

Abg. **Dieter Janecek** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank und mein Lob für Sie alle, dass Sie mit einer solchen Leidenschaft uns das Thema „Quantum Computing" nahgebracht haben und die Begeisterung bei mir und wahrscheinlich auch bei den anderen für das Thema wecken. Wir sind am Anfang. Herr Höferlin hat es gesagt, vielleicht ist es die Chance, dass wir eine Technologie im Frühstadium in Deutschland zielgerichtet mitbegleiten und fördern. Andere sind schon dran. Aber wir hätten noch die Möglichkeit in die Führung zu gehen. Das wäre eine Herausforderung, die ich zumindest gerne annehmen würde.

Meine Fragen gehen beide an Professor Hensinger. Die erste Frage betrifft ein für uns in der Politik immer sehr relevantes Gebiet, nämlich das Anwendungsgebiet. Frau Domscheit-Berg hat es auch schon angesprochen. Die Vorstellung, dass man die Proteinentfaltung besser verstehen und damit Demenz heilen könnte, dass Quantencomputer ein besseres Verständnis von chemischen Reaktionen liefern könnten, das sind Versprechungen oder Szenarien, die uns geschildert werden. Können Sie darauf eingehen und uns verdeutlichen, wo Herausforderungen und vielleicht auch Risiken sind, die uns begegnen können? Wir haben demnächst die Enquete-Kommission „Künstliche Intelligenz", wo das Thema Quantencomputer sicher auch von der Seite hereinspielen wird, in dem Zusammenspiel, was wir in der Zukunft alles mit Daten machen können.

Die zweite Frage, die wir alle hier im Raum angesprochen haben, das ist die Frage der Kryptographie. Ich verstehe es so, dass es mit den Möglichkeiten des Quantum Computing ab einem bestimmten Zeitraum neue Möglichkeiten der Verschlüsselungen gibt, die dann vielleicht auch neue Chancen sind. Das ist natürlich erstmal zu definieren und zu implementieren. Aber gleichzeitig ist die gesamte Kryptographie - im Prinzip bis 1990 rückwirkend - hinfällig. Das ist ein gewaltiges Szenario, und keines, was mir gefällt. Wie gehen wir damit um?

Der **Vorsitzende**: Wir kommen zu den Antworten der ersten Runde. Die Fragen von Herrn Beermann gingen an Professor Bluhm und Professor Wilhelm-Mauch. Ich bitte darum, die fünfminütige Redezeit im Blick zu behalten.

SV **Prof. Dr. Hendrik Bluhm**: Zu der Frage, was die Politik tun kann, um daraufhin zu wirken, dass Deutschland in Zukunft vielleicht ein Technologievorreiter ist: Zunächst muss man ehrlicherweise sagen, das wird aus dem jetzigen Start heraus ein Uphill Battle. Denn die amerikanischen Unternehmen sind früher eingestiegen und massiver als irgendeine deutsche oder europäische Forschungsgruppe, teilweise auch mit niederländischen Gruppen zusammen. Aber ich glaube, wenn man das richtig und vor allen Dingen europäisch gemeinsam angeht, dann hat man noch eine Chance. Eine Möglichkeit ist zum Beispiel, sehr offen vorzugehen, Richtung Open Access, um eine bessere Zusammenarbeit zwischen den Gruppen zu schaffen. Das geht leichter im akademischen als im industriellen Umfeld.

Ich habe ein paar Sachen überlegt, die ein Forschungsprogramm liefern sollte. Das sind die Eigenschaften, die teilweise nicht ganz trivial umzusetzen sind, aber es gibt auch gute Konzepte.

Zum einen muss man technologieorientiert strategische Schwerpunkte setzen. Wenn man das den Grundlagenforschern, die gerne neue Ideen entwickeln, überlässt, kommt da schnell ein „Zoo" raus. Man braucht eine Kraft, die das alles zusammenhält, die aber auch eine Fachkompetenz hat und die Leute dort abholt, wo sie sind. Man könnte zum Beispiel einen emeritierten Experten einstellen, der solch ein Programm koordiniert. Das räsoniert auch mit dem Gedanken aus dem BMBF. Darüber hinaus muss man aber auch die Grundlagenforschung sinnvoll einbinden, um neue Ideen aufzugreifen, gezielt Lösungen auf die mehr grundlagenorientierten Fragestellung zu entwickeln und die Community zu bilden. Sinnvoll erscheint mir, neue Leute aufzunehmen, um die Gruppe der Experten zu vergrößern.

Eine kritische Masse ist ganz wichtig, das wäre der europäische Zusammenhalt. Sie brauchen einen langfristigen Planungshorizont. Das kann kein Dreijahresprojekt sein, sondern muss mindestens auf zehn Jahre ausgelegt sein. Wenn das gut läuft und sich die Technologie positiv entwickelt, lohnt es sich, daraufhin zu investieren. Damit das klappt, sind zentrale Infrastrukturen wichtig. Das Thema hat bei mir Sympathie, eben aus dem Forschungszentrum kommend, weil es eine Spezialität ist, das zu betreiben und effektiv mit der dezentralen universitären Forschung zu verknüpfen.

Dann ist es ganz wichtig, Instrumente zur Verfügung zu stellen, um einerseits ein lokalagierendes Industrieunternehmen an das Thema heranzuführen und zu ermutigen, einzusteigen. Das ist gerade in den großtechnologie-lastigen Bereichen, wie Halbleitertechnologie, sehr schwierig, weil das nicht ganz so gut zu den Unternehmensstrategien passt, wie der von Intel, die von vornherein im Halbleiter-Performance-Bereich unterwegs sind.

Es gibt eine Prozessorfertigung in Dresden, ich war auch gerade zufällig bei Infineon Technologies Dresden GmbH, einem der größten Fertigungsstandorte der Infineon Technologies AG. Ich würde sagen, da sollte man gemeinsam mit geeigneten Instrumenten versuchen, die Unternehmen heranzuführen und zu ermutigen, auch einmal größere Sachen, die in der Zukunft liegen, anzugehen.

Zu dem Thema Start-ups: Ich glaube, es gibt eine deutsche Start-up-Szene, es gibt gute Förderungsinstrumente. Die sehen aber alle so aus, als sollte man eine konkrete Geschäftsidee haben, die sich relativ kurzfristig umsetzen lässt. Förderungsinstrumente, die Projekte mit höherem Risiko fördern, wären vielleicht auch interessant.

Noch ein paar Details zur europäischen Zusammenarbeit: Wenn man sich zusammenschließt und Infrastrukturen oder Zentren in Deutschland aufbaut, kann es gelingen, die ganze Kompetenz, die in Europa vorhanden ist, zu vernetzen und gegebenenfalls deutschen Unternehmen zugänglich zu machen. Und natürlich auch dem gesamten System in Europa, und daraus könnte durchaus eine Chance

entstehen, national führend zu sein. Wenn man sich die Programme anschaut, haben diese durchaus ein im europäischen Rahmen konkurrenzfähiges Volumen. Insofern haben wir gute Chancen, wenn man das richtig angeht.

SV **Prof. Dr. Frank Wilhelm-Mauch**: Eine Sache, die wir schon im Kleineren im europäischen Umfeld gesehen haben, ist, wie viel ein klares Bekenntnis zum Quantum Computing und zur Quantentechnologie bringt. Als das Flaggschiff angekündigt wurde, war allen klar - auch Universitätsleitungen, die immer auf viele Stimmen hören müssen -, Quantentechnologie ist nicht nur eine Mode, über die die Physiker gerade reden. Das ist ernst zu nehmen! Das ist wichtig! Da kann man einsteigen.

Das Interesse der Industrie wurde durch die Ankündigung getriggert. Das Quanten-Flaggschiff hat uns geholfen, bevor der erste Euro geflossen ist. Ich glaube, ein solches Bekenntnis müsste in Deutschland aber auch noch etwas anderes beinhalten. Wer sich heute auf den Weg einer wissenschaftlichen Karriere nach der Promotion macht und in Quantum Computing wirklich mithalten muss, darf sich nicht diversifizieren, sondern sich darauf konzentrieren. Das zeichnet auch die starken akademischen Gruppen in anderen Ländern aus. Das ist etwas, was das deutsche Hochschulsystem einem nicht immer nahelegt.

Wenn ich die Zahl der Physikfachbereiche in Deutschland zähle und mir, 15 Jahre jünger, überlegte, wie viele Professuren in Quantum Computing ausgeschrieben sind, würde ich sagen, ich diversifiziere mein Programm, damit ich hier und dort berufbar bin. Das geht auf dem Niveau von Grundlagenforschung mit wenigen Qubits, aber auf einem höheren Niveau ist das sehr schwierig. Das hat mich selbst biographisch zu einem Karriereumweg durch Kanada geführt. Es war eine schöne Erfahrung, aber ich glaube, ein Bekenntnis mit einer Perspektive der nichtuniversitären, aber öffentlichen Großforschung, mit Quantum Computing als Priorität, wäre eine gute Sache.

Wir sehen, dass in den USA Firmen mit sehr tiefen Taschen, die auch teilweise im Bereich Super Computing kommerziell tätig sind, so etwas alleine stemmen. Die haben wir hier nicht. Aber wir haben durchaus Forschungseinrichtungen bei Helmholtz, bei Leibnitz und etwas grundlegender bei Max-Planck, die in der Lage sind, den langen Atem, die Perspektive, auch mit dauerhaften Anstellungen für Wissenschaftlerinnen und Wissenschaftler, durchaus hinzubekommen. Die können auch ein Katalysator sein, sehr früh Anwender anbinden und dort den richtigen Kompass und die richtigen Perspektiven schaffen. Das wäre meines Erachtens das Richtige. Denn, wie Winfried Hensinger schon gesagt hat, in den Grundlagen sind wir in Deutschland enorm stark. Wenn wir Pionierarbeiten schauen, wenn wir auf Teilnahme an internationalen und globalen Forschungsprogrammen schauen, haben wir da eine sehr starke Stellung. Aber diese ganzen Ingenieursaufgaben, die für eine Karriere in der Physik zu spezialisiert sind, aber noch nicht im Profil der Ingenieurausbildung vorhanden sind, erfordern einen langen Atem. Da kann meines Erachtens die nichtuniversitäre Großforschung - ich sage das in dem vollen Bewusstsein, dass ich an einer Universität bin, die nichtuniversitäre Großforschung also meine Konkurrenz ist - einen sehr wichtigen Beitrag als Katalysator leisten, mit dem Verständnis und der Geduld ausgestattet, dass der Gewinn nach der Investition vieler Euros möglicherweise noch eine gewisse Zeit braucht. Das wäre ein wichtiger Wunsch.

Der **Vorsitzende**: Die Fragen von Herrn Dr. Zimmermann gingen auch an Herrn Professor Wilhelm-Mauch und Herrn Professor Hensinger.

SV **Prof. Dr. Frank Wilhelm-Mauch**: Es gab die Frage, wie weit wir sind und wie die Situation mit den Plattformen ist.

Zunächst zu den Plattformen: Auch hier ist die Lage mit der Geschichte des klassischen Computers, sozusagen im Deutschen Museum, vergleichbar. Der hat auch einen Weg gemacht, vom elektromagnetisch arbeitenden Relais über Röhren zu Transistoren. In dieser Suchphase sind wir jetzt auch ein bisschen. Mehrere Leute von uns glauben, den integrierten Schaltkreis zu

haben. Aber ich denke, keiner würde sagen, dass der Ansatz des anderen jetzt völlig von der Hand zu weisen wäre. Das ist das, was wir mit Plattformen meinen. Da gibt es welchen, die ähneln Atomuhren. Das ist eine oberflächliche, aber nicht ganz falsche Analogie. Es gibt welche, die ähneln relativ stark den Halbleitercomputerchips. Die von mir favorisierte supraleitende Plattform hat eine etwas entferntere Ähnlichkeit.

Wir wollen das mit den tiefen Temperaturen handhabbar, zuverlässig und problemlos machen. Es sieht so aus, dass Tieftemperaturtechnik von Rechenzentren und von Super-Computing-Zentren von Technikern zuverlässig betrieben werden kann. Das ist keine Geheimwissenschaft mehr.

Wo sind wir? Da gibt es den Begriff der Quantum Supremacy oder das Quantum Advantage. Das beschreibt einen sehr akademischen Meilenstein, der sagt, der Quantencomputer ist jetzt so groß, dass kein klassischer Supercomputer der Welt den noch simulieren kann. Also in der idiosynkratrischen Anwendung der Simulation seiner selbst schlägt er alle Supercomputer. Das ist ein ganz wichtiger Zwischenmeilenstein. Wir glauben, dass dabei etwa 50 Qubits - wieviel genau, kommt darauf an, wen man fragt - erreicht werden, wenn die nur sehr geringe Fehlerraten haben. Deshalb kündigen so viele Unternehmen 50 Qubits an.

Der nächste Schritt wird sein, mit ein wenig größeren Systemen unter den verschiedenen geplanten Anwendungen etwas zu machen, was tatsächlich nützlich ist. Der ganz große Favorit - hier kommt es auch wieder darauf an, wen man fragt -, von dem wir glauben, dass die Größenordnung von 100 Qubits interessante Dinge macht, ist die Simulation von Molekülen und Materialien. Das ist deshalb interessant, weil die Übersetzung der Algorithmen relativ einfach ist. Es ist deshalb interessant, weil wir auf eine informierte Industrie treffen, nämlich auf die theoretischen Abteilungen von Chemieunternehmen, die bei Super Computing auch Experimenten offen gegenüberstehen. Die auch Investitionskosten in der Entwicklung haben, die Quantum Computing interessant erscheinen lassen. Da gibt es im Augenblick ein gewisses Rennen darum, welches das größte Molekül ist, das ich mit 100 Qubits simulieren kann, und ist das etwas, was klassisch nicht mehr geht. Wir lesen gerade die Vermerke darüber. Das ist etwas, was man auch im Ergebnis sehen kann. Man sieht sozusagen das Molekül, das entwickelt wurde. Für Unternehmen interessant, weil man natürlich, wenn man vorne dabei ist, auch einen Wettbewerbsvorteil haben kann.

Danach, deshalb hören Sie von uns manchmal sehr unterschiedliche Zahlen, kommt eine sehr schwierige Angelegenheit, nämlich die Fehlerkorrektur. Quantencomputer sind sehr viel fehleranfälliger als klassische Computer. Klassische Computer sind in dem Sinne eine gewisse Anomalie. Man kann diese Fehler aktiv korrigieren. Das braucht aber Overhead (einen Mehraufwand) und das braucht Zeit. In den augenblicklichen Schätzungen, die wir auch in der BSI-Studie sehen - dann sind wir tatsächlich bei Millionen von physikalischen Qubits -, wird es auch kryptographisch spannend. Eine wichtige Aufgabe in der Forschung ist in dem Bereich des nichtfehlerkorrigierten Quantencomputers - der halt wenig Fehler macht, aber nicht beliebig wenig -, den Anwendungsbereich immer weiter zu vergrößern.

SV **Prof. Dr. Winfried Hensinger**: Zu der Frage, wo stehen wir gerade: Im Moment bauen wir Prototypen des Quantencomputers. An der University of Sussex bauen wir jetzt eine Maschine mit nur ein paar Qubits, an der wir aber zeigen können, dass die Technik funktioniert. Die Maschinen sind aber nicht dazu da, irgendwelche interessanten Probleme zu lösen, sondern eigentlich nur, um die Technologie zu zeigen und auch um zu sehen, was vielleicht nicht funktioniert oder aus anderen Gründen der Weiterentwicklung bedarf. Es gibt ungefähr fünf oder zehn Quantencomputer auf der Welt, in unterschiedlichen Formen, die supraleitenden Qubits und die Ionen-Qubits sind da weit vorne. Dann gibt es das Konzept der Quantum

Supremacy. Da geht es wirklich darum, zum ersten Mal zu zeigen, dass ein Quantencomputer etwas machen kann, was ein klassischer Computer nicht machen kann.

Für mich war die Quantum Supremacy nie so interessant, weil man da zwar unglaublich wissenschaftliche Probleme löst, die aber nicht unbedingt eine richtige Anwendung haben. Sondern man beweist einfach nur wissenschaftlich, dass ein Quantencomputer besser ist als ein klassischer Computer. Für mich war es interessanter, in die Zukunft zu schauen und dann die Technologie so weiterzuentwickeln, dass wir zu den riesigen Qubit-Zahlen kommen können. Da rede ich wirklich von Millionen oder Milliarden von Qubits. Da wird es wichtig, dass man eine Technologie hat, die das leisten kann. Für mich war es immer eine Entscheidung, nicht so große Herausforderungen an die Kühltechnik stellen zu müssen. Bei den Ionen ist es auch möglich, dieses Modular zu bauen.

Aber wo wollen wir hin? Und was müssen wir machen, um dahin zu kommen? Das Wichtigste ist, dass wir die Technik entwickeln, um solche große Maschinen zu bauen. Das kann dann nicht mehr in der Universität stattfinden. Doktoranden können mit vielen Kabeln an einem Experiment herumhantieren, um so ein Ding zu bauen, aber man kann damit keine Maschine bauen, die vielleicht Millionen Qubits hat. Das muss man industriell produzieren. An meiner Universität sind wir gerade dabei, eine Firma aufzubauen. Das heißt nicht, dass ich nicht mehr Professor bin, meine Arbeitsgruppe läuft weiter. Aber wir brauchen auch eine Firma, um diese Module zu produzieren. Das sind Halbleitermodule, die müssen ähnlich, wie bei Intel, produziert werden, um die vielen Ionen zu halten. Es ist natürlich wahnsinnig wichtig, solche industrielle Fertigung aufzubauen, damit wir dann wirklich diese großen Maschinen produzieren können.

Wie gesagt, im Moment haben wir überall auf der Welt circa 50 oder 70 Qubits. Die Leute arbeiten daran und sind dabei, wirklich tolle Sachen zu machen. Aber der nächste Schritt ist, diese Maschinen zu bauen, damit wir zu viel größeren Zahlen von Qubits kommen können. Dann können wir anfangen, die richtig interessanten Probleme zu lösen, und anfangen, Moleküle zu simulieren. Die andere Herausforderung, die wir haben, ist die Fehlerkorrektur. Eine Möglichkeit, mit den Fehlern zu arbeiten, ist, sie einfach kleiner und kleiner zu machen. Viele Arbeitsgruppen arbeiten in diese Richtung. Aber was wir gesagt haben ist, wir wollen jetzt eine Maschine bauen, die auch interessante Probleme lösen kann. Deshalb gehen wir in die andere Richtung und sagen, wir haben mehr und mehr Qubits. Dann können wir nämlich auch mit dem jetzigen Fortschritt der Technik überlegen, solche Maschinen zu bauen, und die würden auch dementsprechend groß sein. Da sind ingenieurwissenschaftliche Meisterleistungen gefragt, um das zu erreichen.

Zur Zeitskala: Den Prototypen bauen wir in etwa eineinhalb Jahren. Wir denken, dass wir diesen Zeitrahmen brauchen. Es läuft gut und wir sind vielleicht ein bisschen schneller. Dann fangen wir an, eine große Maschine zu bauen, die auch dazu dienen kann, einige der interessanten Probleme zu lösen. Dazu kann ich nachher noch etwas mehr sagen.

Der **Vorsitzende**: Die Frage von Herrn Schulz ging an Herrn Dr. Ritter.

SV **Dr. Stephan Ritter**: Zur Frage der Technologiesicherung und wie steht es mit Patenten, ein interessantes Thema: In Deutschland sind wir spitze bezüglich Publikationen, Anzahl von Forschern, in der Grundlagenforschung und Expertisen zu diesem Thema. Bezüglich der Patente sind wir nicht so gut aufgestellt. Ich war selbst 15 Jahre in der Grundlagenforschung und kann daher aus meiner persönlichen Perspektive ein bisschen dazu berichten.

Das hat damit zu tun, dass die Quantencomputer und Quantentechnologien allgemein in der Grundlagenforschung angesiedelt sind. Der Grundlagenforscher, wenn er etwas Neues realisiert, verstanden oder entdeckt hat, hat schon als nächste Idee, was er besser machen möchte. Er hat eigentlich kein großes Interesse daran, den aufwendigen Weg der Patentierung oder

Technologiesicherung zu gehen. Das ist, wenn er an einem Grundlagenforschungsinstitut angestellt ist, im Zweifel auch gar nicht seine vornehmliche Aufgabe. Das zeigt, warum Patente gerade in dem Bereich zurzeit noch relativ wenige existieren.

Ein anderer Grund ist, dass man Technologie erstmal besitzen muss, um sie sichern zu können. Das heißt, bevor wir darüber reden, was es alles an Technologie bezüglich des Quantencomputers zu sichern gibt, müssen wir das bestehende erstmal erforschen. Auf diesem Weg sind wir in der Grundlagenforschung zurzeit.

Ein anderer Aspekt ist, dass derjenige, der technologisch vorne ist und führt, sich Märkte als erster erschließen kann. Das heißt, die Patentsicherung oder die Sicherung des Wissens ist sicherlich ein Aspekt. Ein anderer ist, dass derjenige, der in der Entwicklung früh dabei war und eine führende Stellung einnimmt, im Zweifel auch die Entwicklungsschritte machen kann, die dann später am Markt relevant sind.

Herr Bluhm hatte schon darauf hingewiesen, dass die Situation bezüglich Start-ups in Deutschland nicht so stark ist. Das hat sicherlich auch mit der geringeren Verfügbarkeit von Venture Capital in Deutschland bei Start-ups zu tun. Da ist man in Amerika einen Schritt weiter.

Bezüglich der Technologiesicherung möchte ich auf die Schlüsseltechnologien eingehen, die wir nicht vergessen dürfen. Es gibt ganz viele Firmen, die entwickeln Technologien, die zwar keine Quantentechnologie ist, aber die essentiell nötig ist, damit man Quantencomputer bauen kann. Da sind wir in Deutschland wirklich sehr stark. Da läuft es typischerweise so ab, dass ein Forscher kommt und sagt, er braucht ein neues Gerät, um seinen Quantencomputer weiterzuentwickeln. Dann sagt der Vertrieb in der Industrie, dass man ein ganz tolles neues Produkt habe mit unerhörten Spezifikationen. Dann sagt der Wissenschaftler, dass er es noch eine Nummer besser brauche. Das ist die typische Situation. Das ist gut. Das bringt beide Seiten voran, sowohl die Seite der Quantencomputer-Entwickler als auch die Seite derer, die Schlüsseltechnologien entwickeln. Das passiert natürlich ganz häufig in der Industrie. Da weiß man, wie man eine Technologiesicherung durchzuführen hat.

Ein Aspekt, den ich noch ergänzen möchte, ist das Thema Quantentechnologien als Ganzes. Man darf nicht vergessen, dass man die Möglichkeiten, die wir bei der Entwicklung von Quantencomputern jetzt kennen, auch auf andere Anwendungsfelder ausdehnen kann. Da gibt es ganz viele gegenseitige Synergien. Da gibt es Entdeckungen, die gemacht werden im Bereich des Quantum Computing, die zum Beispiel zur Verbesserung von Uhren genutzt werden können. Wir haben schon von der Nähe von optischen Uhren und gewissen Ansätzen zu Quantum Computing gehört. Es gibt zum Beispiel die Idee, dass man ein einzelnes Ion, das als beste Uhr dient, mit Hilfe eines Quantenlogikgatters, also eines Elements aus dem Quantum Computing, ausliest, um das Ion möglichst wenig zu stören, damit die Uhr möglichst gut durchläuft. Das ist jetzt nur ein Beispiel von vielen, das man benennen könnte. Ich möchte betonen, dass ich es für sehr wichtig halte, dass dieser Bereich als Ganzes gesehen wird.

Der **Vorsitzende**: Die Frage von Herrn Höferlin ging an Herrn Professor Buchmann.

SV **Prof. Dr. Dr. h.c. Johannes Buchmann:** Sie haben im Zusammenhang mit dem D-Wave Computer die Frage nach dem Zeithorizont gestellt.

Ich glaube, die Physikerkollegen können mehr zu dem D-Wave Computer sagen als ich. Ich glaube, man kann sagen, dass die Technologie, die dort verwendet wird, jedenfalls nicht das ist, was die Kollegen hier am Tisch entwickeln.

Zu dem Zeithorizont möchte ich ein Gedankenexperiment nennen. Wie wäre es denn, wenn wir in Deutschland sagen würden, die deutsche IT ist quantencomputerresistent. Also, dass wir eine Strategie machen und uns vornehmen, dass deutsche IT-Technologie, Industrie 4.0 - der Begriff ist in Deutschland geprägt worden und inzwischen weltweit bekannt - soll hinsichtlich der Sicherheit dieser Systeme quantencomputerresistent sein. Wenn man von

einem solchen Gedanken ausginge, könnte man eine Strategie entwickeln von den Verfahren bis zu der Integration in die Produkte und käme auch zu einem Zeitplan.

Vielleicht ein Wort zu der Frage, wieweit wir in den Grundlagen sind: Das National Institut of Standards and Technology in den USA hat im vergangenen Herbst eine Ausschreibung erarbeitet, wo Leute quantencomputerresistente Kryptographie vorschlagen konnten. Da liegen jetzt circa 70 Vorschläge vor. Das heißt, es gibt Material. Wir können es machen und wir können damit beginnen. Wenn man eine solche Strategie machen würde, würde man sagen, das stärken wir erstmal. Wir sagen, die jungen Leute, die sich mit diesen Themen beschäftigen, werden gleich zusammengeschaltet mit den Unternehmen, die dann die Anwendungen haben.

Wenn heute ein Auto in Deutschland produziert wird, hält das sehr lange, und die Kryptographie darin können Sie nicht so leicht austauschen, weil die in der Hardware ist. Das heißt, man würde mit der Automobilindustrie sprechen oder mit anderen Zulieferern, wie Bosch zum Beispiel, und fragen, wie können wir es schaffen, die Geräte, die in diesem Kontext Industrie 4.0 gemacht werden, quantencomputerresistent zu entwickeln. Ich denke, wenn wir da eine Strategie aufbauen würden - Deutschland steht auch für Sicherheit -, dann hätten wir eine sehr gute Chance, hier nach vorne zu kommen.

Technikfolgenabschätzung hängt eng damit zusammen. Sie haben gefragt nach dem Stand der Technikfolgenabschätzung. Ich glaube, bis jetzt bezieht sich das, was man Technikfolgenabschätzung nennt, nicht auf diesen Bereich. Das heißt, wenn man eine solche Strategie machen würde, müsste man das begleiten von der Technikfolgenabschätzung, die sagen würde, was passiert, wenn wir jetzt nicht schnell genug handeln. In welchem Zeitraum müssen wir fertig sein und ähnliches. Ich glaube, das wäre eine sehr günstige Ergänzung.

Der **Vorsitzende:** Die Fragen von Frau Domscheit-Berg gehen an Frau Professorin Wehner.

SVe **Prof. Dr. Stephanie Wehner:** Es gibt zwei Fragen: Wie kann Quantentechnologie dem Gemeinwohl zugutekommen und welche Rolle spielen Patente darin. Ich denke, dass es wichtig ist, Quantentechnologie schon im sehr frühen Stadium für die Allgemeinheit zugänglich zu machen. Dies kann beispielsweise geschehen im Rahmen von Testbed oder einem Quantenrechenzentrum, in dem Leute den Quantenrechner benutzen können, oder auch im Netzwerkbereich, wo sie Zugang haben zu dem Netzwerk. Ich denke, dass es dafür viele Gründe gibt. Der erste ist, dass die Allgemeinheit es benutzen und davon lernen kann. Es ist ein sehr nützliches Instrument zur Ausbildung von Leuten, die diese Technologie verwenden können. Es gibt auch eine Möglichkeit, dass viele Leute dafür dann Software entwickeln.

Ich denke, wenn Sie klassische Computer oder ein klassisches Netzwerk anschauen - natürlich ist die Hardware sehr wichtig - aber das, was es am Schluss schließlich für den Benutzer möglich macht, diese Technologie einzusetzen, ist die Software, die diese Hardware benutzt. Wir können nicht vorhersehen, welche Anwendungen es sein werden, die die Leute gerne ausführen möchten. Ich denke, das Internet ist groß geworden, indem sehr viele Leute Software dafür entwickelt haben. Das können Privatpersonen sein, können Open Source sein, können aber auch Sachen sein, die von Firmen als Software-Package angeboten werden. Das ist das, was es wirklich nützlich macht. Deshalb denke ich, dass es wichtig ist, ein Testbed zu kreieren, zu dem die Leute Zugang haben. Das kann im Ausbildungsbereich liegen oder auch gekoppelt sein, wie zum Beispiel im Start-up-Investment, wo man selbst einer Einzelperson, die Software entwickeln möchte, die Möglichkeit dafür gibt.

Es ist so, dass es diese Instrumente, die Quantum Key Distribution machen, jetzt schon auf dem Markt gibt. Wenn man darauf eine andere Software installieren würde, könnte man damit nicht nur Quantum Key Distribution machen, sondern sogar Identification. Deshalb halte ich das für sehr nützlich.

Zu den Patenten: Natürlich kann man über Patente eine sehr allgemeine Diskussion führen. Ich möchte mich auf den Quantenbereich beschränken. Ich bin am QuTech. Wir haben eine Partnerschaft mit Microsoft. Microsoft hat ein eigenes Labor bei uns im Gebäude. Wir haben auch eine Partnerschaft mit Intel. Das heißt, Chips, die bei uns am QuTech entworfen werden, werden in der Intel-Fab fabriziert und kommen dann wieder zurück zu uns. Das ist sehr nützlich, weil man sich davon erhofft, sehr homogene Chips herzustellen. Ich hoffe, dass es klar ist, dass in diesem Bereich selbst jetzt schon sehr viele Patente geschrieben werden, auch für Sachen, die es noch gar nicht gibt, also Designs.

Man sollte sich darüber im Klaren sein, dass im internationalen Bereich, gerade auch in den USA, sehr viele Patenten kreiert werden, die möglicherweise bestimmte Leute in der Zukunft vor Herausforderungen stellen. Patente in diesem Bereich müssen nicht unbedingt schlecht sein. Aber man muss klarstellen, dass damit schon bestimmte Herausforderungen verbunden sind. Wir möchten gerne ein Quantennetzwerk bauen. Wir können das aber auch nur machen mit Partnern wie TOPTICA, die dafür - weil wir immer hohe Ansprüche haben an die Laser - Neuentwicklungen machen müssen. Wir möchten auch in fünf oder zehn Jahren noch neue Laser von TOPTICA bekommen. Also, nicht alle Patente müssen schlecht sein. Es ist aber klar, denke ich, Akademiker schreiben normalerweise keine Patente, es ist schwierig und es kostet Zeit. Man muss sich im Klaren darüber sein, dass ein Patent auch Geld kostet, nämlich, um es zu behalten. Daher ist es wichtig, auch in Europa im akademischen Bereich Leuten zu helfen und Förderungen einzurichten.

Zu der Frage über die Anwendungen von Simulationen auf dem Quantencomputer: Quantencomputer können Quantensimulationen ausführen. Man könnte sich vorstellen, dass in der Zukunft sehr viele Experimente, die jetzt im Chemielabor durchgeführt werden - wenn ich beispielsweise ein neues Material testen möchte, - nicht erst als ein langwieriges Experiment durchgeführt werden müssen, sondern auf dem Quantencomputer erst einmal als eine Simulation ausgeführt wird. Dann kann man das Material vielleicht ausschließen. Wenn man einen guten Kandidaten gefunden hat, möchte man es noch verifizieren. Aber ich denke, dass Quantencomputer eine große Rolle spielen können, um solche Probleme in der Zukunft ganz anders lösen zu können, indem man es durch das Labor auf dem Quantencomputer laufen lässt.

Der **Vorsitzende**: Von Herrn Janecek gingen die Fragen an Herrn Professor Hensinger.

SV **Prof. Dr. Winfried Hensinger**: Es ging um die Anwendungsgebiete und Herausforderungen für einen Quantencomputer. Ich fange am besten an zu beschreiben, wieso ich denke, dass Quantencomputer ganz speziell und anders sind als andere Computer. Da komme ich zurück zur Quantenmechanik. Die Quantenmechanik ist eine unglaublich starke Theorie, die wirklich alles beschreibt. Die Quantenmechanik beschreibt chemische Reaktionen, sie kann beschreiben, wie die Leitung in Supraleitern funktioniert, ob Material stark, zugleich aber auch leicht ist. Die Quantenmechanik ist eine unglaublich fantastische Theorie. Es gibt nur leider ein Problem, und das ist, dass konventionelle Computer die Probleme der Quantenmechanik gar nicht lösen können, weil die nicht genug Rechenleistung haben. Deswegen müssen wir jetzt im Chemielabor stehen, um Reaktionen durchzuführen, Pharmafirmen müssen Produkte ausprobieren, weil man die Ergebnisse nicht berechnen kann. Die Computer heutzutage können das gar nicht. Da haben wir eine Riesenmöglichkeit durch den Quantencomputern. Die Quantencomputer können es schaffen, chemische Reaktionen so zu simulieren, wie sie eigentlich funktionieren. Nicht nur chemische Reaktionen, es können auch biologische Reaktionen sein, zum Beispiel die Proteinentfaltung. Man könnte herausfinden, ob es möglich ist, einen Zimmertemperatur-Supraleiter zu bauen. Da können Sie sich vorstellen, was das heißen würde für die Energiekosten.

Darum setzt man so viel Hoffnung in die Quantencomputer, weil die Quantencomputer die Quantenmechanik simulieren können. Dann gibt es noch das Gebiet der Quantenalgorithmen, also die Quantensoftware. Dazu muss ich sagen, es ist nicht so, dass ein Quantencomputer ein schneller Computer ist, überhaupt nicht. Ein Quantencomputer funktioniert komplett anders als ein konventioneller Computer. Da kann man argumentieren, dass ein Quantencomputer in parallelen Universen rechnet. Da können Sie sich vorstellen, dass Windows oder Apple nicht die Software ist, die sowàs produzieren kann. Man muss für jede Anwendung einen neuen Algorithmus schreiben. Es gibt Optimierungsalgorithmen und Suchalgorithmen und vieles mehr, aber wir sind gerade erst am Anfang.

Einer meiner Kollegen hatte mir erzählt, vor drei Jahren schien es fast unmöglich zu sein, eine Professur in der Entwicklung der Quantenalgorithmen zu bekommen. Damals wussten die Leute noch nicht so richtig, ob man überhaupt solche Computer bauen könnte. Sprich, das Feld ist gerade erst am Anfang. Um das richtig zu verstehen, ist ein Vergleich mit den konventionellen Computern in den 40er-Jahren am besten. In den 40er-Jahren gab es schon konventionelle Computer und man kann auch argumentieren, dass diese Computer den Zweiten Weltkrieg beendet haben.

Als ich in den 80er-Jahren tippen gelernt habe, habe ich das noch auf einer Schreibmaschine gelernt, weil in den 80er-Jahren die Computer noch nicht so einfach verfügbar waren. Aber irgendwann kamen sie dann. So ähnlich ist es jetzt mit den Quantencomputern. Es wird erst ein paar Anwendungen geben, aber dafür muss Software entwickelt werden. Es wird ganz langsam passieren. Man sollte keinem Wunderheilern glauben und denken, dass, sobald wir den ersten Quantencomputer haben, auch alle Anwendungen sofort verfügbar seien. Es ist viel Arbeit, langfristige Arbeit, und es muss gemacht werden. Ich denke, da sind sich hier alle Experten am Tisch darin einig, dass die Möglichkeiten auch heute schon wunderbar erscheinen, wir aber trotzdem erst am Anfang sind. Da würde ich keine Zukunftsprognose geben wollen.

In der zweiten Frage ging es um die Kryptographie. Leider ist es so, dass, wenn es einen Quantencomputer gibt, alle Daten, die mit der regulären RSA-Kryptographie verschlüsselt wurden, sofort lesbar sein werden. Dagegen können wir nichts machen. Das Gute ist, dass die ersten Quantencomputer, die sowas machen können, wahrscheinlich erst in zehn oder fünfzehn Jahren verfügbar und außerdem sehr teuer sein werden. Da muss man sich genau überlegen, ob die Daten es wert sind, sie auf diese Art zu knacken. Da gibt es bestimmt auch bessere Möglichkeiten. Aber wie die anderen Kollegen hier schon gesagt haben, ist es unglaublich wichtig, jetzt an Software zu arbeiten, um dann eben auch Verschlüsselungen zu finden, die quantencomputerresistent sind. Das muss nicht einmal die Quantenkryptographie sein, es gibt auch klassische Verschlüsselungsprotokolle, die angewendet werden könnten, die zumindest heute so erscheinen, dass ein Quantencomputer sie nicht knacken kann.

Der **Vorsitzende**: Wir kommen zur zweiten Runde. Ich darf die Kolleginnen und Kollegen aus terminlichen Gründen bitten, die Fragen kurz zu fassen. Bei den Antworten bitte ich die Experten, sich zu beschränken.

Abg. **Tankred Schipanski** (CDU/CSU): Eine Frage an Herrn Professor Wilhelm-Mauch habe ich: Sie haben von dem BMBF-Flaggschiff gesprochen, dem europäischen Flaggschiff-Programm. Können Sie Zahlen nennen, wie hoch die Volumina sind, die da gebraucht werden, was Sie an Fördermitteln bekommen - wir haben verschiedenste Förderlinien.

Die zweite Frage geht an Herrn Professor Bluhm: Sie haben die Start-ups angesprochen und dass sich da noch zu wenige ausprobieren. Wo sehen Sie Möglichkeiten für Start-ups oder junge Unternehmen, sich mit dieser Technologie am Markt zu platzieren?

Abg. **Gustav Herzog** (SPD): Vielen Dank für die

guten Antworten. Wenn ich eine flapsige Bemerkung mache, dann deshalb, weil ich meine Sorgenfalte auf der Stirn etwas überspielen will. Ich habe den Eindruck, wir werden mit dem Quantencomputer die Probleme lösen, die wir ohne ihn gar nicht hätten. Meine Frage geht an Herrn Professor Markgraf: Was können wir denn heute schon oder in der nächsten Zeit tun, um unsere Daten zu schützen? Wird es sinnvoll sein, möglichst viel zu löschen, damit man sie nicht mehr entschlüsseln kann? Oder wird es nicht unsere Aufgabe sein, Instrumente zu schaffen, um die heutigen Daten mit einem Quantencomputer so zu verschlüsseln, dass sie der Quantencomputer nicht mehr entschlüsseln kann? Was können wir tun? Wir haben jetzt die Verantwortung. Sie haben uns gesagt, es wird schwierig werden, also müssen wir heute die Fragen stellen und sie geben uns die Antworten.

Abg. **Uwe Kamann** (AfD): Auch von meiner Seite aus: Herzlichen Dank. Ich könnte Ihnen stundenlang zuhören, wobei ich immer strubbeliger werde. An Herrn Professor Buchmann geht meine erste Frage und die zweite an Frau Professorin Wehner. Technologie ist faszinierend, aber als solches immer ein Selbstzweck. Wir sind, wenn ich das richtig verstanden habe, in einer Zeitachse, in der wir von zehn bis zwanzig Jahren reden, bis wirklich echte Anwendungen durchgeführt werden können oder sich auch der Nutzen realisierbar zeigt. Können Sie uns, als Politik, Empfehlungen geben, was wir heute oder in den nächsten Jahren schon tun können, damit wir - Technologieführer zu werden wird schwierig, nachdem, was ich gehört habe - eine der führenden Gesellschaften in Europa oder in Deutschland sein können? Was können wir als Politiker tun, um unser Land nach vorne zu bringen?

Meine zweite Frage an Frau Professor Wehner: Glauben Sie und stimmen Sie mit mir darin überein, dass die Quantentechnologie und die Nutzung der Quantentechnologie die Welt etwas näher zusammenbringt?

Abg. **Mario Brandenburg** (FDP): Ich habe eine Frage an Herrn Professor Wilhelm-Mauch: Sie haben gesagt, vor vier Jahren war die Idee greifbar und seit einem Jahr ist sie ökonomisch. Gibt es in der jetzigen Entwicklung etwas, was wir aus der klassischen Halbleiterindustrie kennen, sowas wie das Mooresche Gesetz? Dass wir sagen, da gibt es ein lineares Wachstum. Oder gibt es am Tag X eine Explosion der Qubits, um das planbar zu halten?

Frage zwei geht an Herrn Dr. Ritter: Was können wir, als Politik, als Leitplanke setzen oder an Richtung vorgeben, damit Sie als Vertreter der Wirtschaft sagen, das hilft entweder mir oder anderen Unternehmen und Start-ups, um schnellstmöglich in diesem Bereich weiterzukommen?

Abg. **Dr. Petra Sitte** (DIE LINKE.) Ich weiß nicht genau, an wen ich diese Frage stellen soll. Unlängst ist bei einer Podiumsdiskussion zu KI gesagt worden, wenn Quantencomputer dazu kommen, wird die Welt eine andere sein. Wenn Technologien nicht verstanden werden, und wir versuchen jetzt gerade als Politiker halbwegs, irgendeine Ahnung zu kriegen, was da gerade läuft, werden auch Befürchtungen offenkundig. Deshalb ist mir in diesem Zusammenhang eine Aussage von Klaus Töpfer eingefallen: „Demokratiefähigkeit von Technologien". Was können wir tun, um an der Stelle pro aktiv zu handeln, um genau das zu gewährleisten und die gesellschaftliche Sensibilität für den Einsatz dieser Computer zu realisieren?

Meine zweite Frage lautet: Was machen Quantennetzwerke mit dem Internet mit der Architektur von heute, wie beispielsweise Darknet usw.? Was erwartet uns da unter Umständen? Ich weiß nicht genau, an wen ich diese Fragen stellen soll. Vielleicht kann sich jemand melden.

Abg. **Dieter Janecek** (BÜNDNIS 90/DIE GRÜNEN): Ich beschränke mich auf eine Frage an Professor Hensinger zur Energiebilanz und zur Herausforderung, das alles zu begreifen. Sie haben beschrieben, dass superleitende Qubits und Ionen-Qubits teilweise auf den absoluten Nullpunkt von -273° Celsius gekühlt werden. Jetzt habe ich sogleich den Link zur Blockchain im Kopf gehabt, die auch als vielversprechende

Technologie angepriesen wurde und dann, beim Bitcoin zumindest, in der Massenverbreitung zu gigantischen Energieverbräuchen geführt hat, die nicht mehr nachhaltig und darstellbar sind. Jetzt schließt sich die Frage an: Welchen Aufwand betreiben Sie pro Rechenleistung. Das ist das Spiel der Zukunft. Wir werden viel Rechenleistung brauche, gleichzeitig Moore's law, und auf der anderen Seite kommen Sie mit der Quantentechnologie. Haben wir dann ein Szenario mit gigantischen Energieverbräuchen zu erwarten oder laufen Sie dagegen?

Der **Vorsitzende**: Wenn wir in der Zeit bleiben wollen, was wir auch müssen, dann bleibt für die Antwortzeit nur eine Minute.

SV **Prof. Dr. Frank Wilhelm-Mauch**: Um Zahlen zu nennen für die vier Anwendungssäulen der Quantentechnologien: Die Europäische Union hat 1 Mrd. Euro in einem Zehnjahresprogramm ausgelobt. Es finden Diskussionen in anderen Förderinstrumenten statt, wonach speziell im Bereich Quantum Computing ein vergleichbarer Betrag drauf gelegt werden soll.

Das schwedische Programm, das in einer Institution den Bau eines Quantencomputers fördert, hat ein Volumen von 100 Mio. Euro über zehn Jahre. In den gerade ausgelobten Flaggschiff-Projekten wurde pro Entwicklungsprojekt das Budget für drei Jahre auf 10 Mio. Euro limitiert. In unserem Fall ist das nur möglich, weil sehr viele Leistungen, die wir in der Forschung brauchen, aus Bordmitteln der Teilnehmer, insbesondere aus Schweden und der Schweiz, getragen werden und budgetneutral sind. Unser Gesamtaufwand ist wahrscheinlich ein Vielfaches. Das Ziel ist es, da auf der 50 bis 100-Qubit-Ebene konkurrenzfähig zu sein.

Was die USA in Unternehmen und teilweise auch im sicherheitsrelevanten Bereich investiert, ist nicht öffentlich. Ich glaube, da wird insgesamt eine Programmgröße von 200 Mio. USD pro Jahr geschätzt, von Leuten, die das beruflich schätzen.

SV **Prof. Dr. Hendrik Bluhm**: Zu den Start-ups hinsichtlich der Chancen und Möglichkeiten: Es gibt relativ viele Start-ups, schon zwei, drei aus Deutschland, aber auch weltweit, die im Bereich Software unterwegs sind. Es sind geringe Anfangsinvestitionen. Man kann in die Beratung gehen und sehen, was ein Unternehmen damit machen kann. Es stellt sich die Frage, ab wann und zu welchen Bedingungen es ist sinnvoll, Testsysteme oder Zugang zu Testsystemen zu erwerben, um dort eine Plattform zu bieten. Das ist eine Frage, die wir uns in Jülich und auch im Austausch mit dem BMBF immer wieder stellen. Darüber kann man noch weiter diskutieren.

Im Hardware-Bereich ist Rigetti Computing ein interessantes Beispiel; vor etwa drei Jahren gegründet mit 70 Mio Venture Capital. Ich frage mich immer, geht das hier? Wenn nein, wieso nicht. Das ist wahrscheinlich eine Mischung zwischen falscher Mentalität, fehlenden Leuten, die das wirklich angehen, und fehlendem Venture Capital. Ich wäre froh, wenn ich dazu bessere Antworten hätte. Weiterhin sehe ich gewisse Möglichkeiten im Design, Know how, Design Tools, um hier voranzukommen. Simulationssoftware, wie sie auch Herr Wilhelm-Mauch selbst in der Forschungsgruppe entwickelt. Wir sind da auch aktiv und prüfen, ob das nicht ein Bereich wäre, der relativ kleine Einstiegsinvestitionen hat und trotzdem gewisse Technologiekompetenz aufbauen lässt.

Weiterhin frage ich mich, ob es nicht sinnvoll wäre, mehr Forschung durch Start-ups zu ermöglichen und zu fördern, also zuzulassen, dass sich eine Unternehmenskultur entwickelt und ganz gezielt Forschungsprojekte dominant oder in Zusammenarbeit mit Unternehmen an Start-ups zu vergeben. Aber eben so, dass nicht gleich ein Produkt oder ein konkreter Profitgedanke dahinter stehen muss. Ob man das will, ist sicher eine politische Frage. Aber ich finde, das ist ein interessanter Gedanke.

SV **Prof. Dr. Marian Margraf**: Was können wir tun? Ich habe in meinem Eingangsstatement zwei verschiedene Szenarien kurz erklärt. Für Geheimnisse, die jetzt nur kurzfristig vertraulich sein müssen, besteht noch kein großer Handlungsbedarf. Wenn wir in zehn bis zwölf Jahren die Quantencomputer haben, schon. Aber

wenn ich heute Online-Banking mache, ist nicht relevant, ob das in zehn Jahren geknackt werden kann.

Ich bin zuversichtlich, dass wir deutlich weiterkommen werden. Ich erinnere mich, dass ich mit diesem Thema Post-Quantum Cryptography vor drei Jahren angefangen habe. Da war ich auf einigen Podiumsdiskussionen und die Leute haben die Augen gerollt und gedacht: „Jetzt kommt der Markgraf wieder mit diesem Thema und dabei haben wir ganz andere Themen." Mittlerweile kommt die Industrie tatsächlich auf uns zu. Nicht nur wegen der Forschungsprojekte, wir haben einige Industriepartner, die uns konkret fragen, wie sie ihre Industrieprojekte umsetzen sollen. Da geht es in erster Linie ganz formal um Migrationskonzepte: Wie kann ich meine heutigen Krypto-Geschichten zukünftig ändern. Das BSI nennt das Krypto-Agilität. Da muss man sich häufig überlegen, wie setze ich später die neuen Krypto-Algorithmen ein. Dafür bräuchte ich schon einen Update-Prozess, der auch quantencomputerresistent ist. Ich habe vorhin gesagt, wir haben Signaturverfahren, die können das. Im letzten Schritt müssen wir uns jetzt überlegen, wie konkret kann man Schlüsseleinigungsverfahren einsetzen und welche sind das, damit das funktioniert. Ich bin zuversichtlich. Die kommen auf uns zu und wollen konkret mit uns zusammenarbeiten.

SV **Prof. Dr. Dr. h.c. Johannes Buchmann:** Es wurde gefragt, was man machen kann. Ich komme auf das zurück, was ich eben schon gesagt habe. Man setze ein Gremium aus Wissenschaftlerinnen und Wissenschaftlern sowie Vertreterinnen und Vertretern aus der Industrie zusammen, die sollen eine Strategie entwickeln, wie wir deutsche IT quantencomputerresistent machen können. Am besten anhand eines konkreten Beispiels. Das ist meine Antwort dazu.

Ich möchte noch kurz etwas zu Quantencomputern und KI sagen: Ehrlich gesagt ist KI für sich genommen schon so ein relevantes Thema und da werden so dramatische Sachen passieren, dass wir dabei das Thema Quantencomputer ignorieren können. Es wird dadurch nicht viel dramatischer. Man muss das sehr nötig diskutieren. Aber ob es dann Quantencomputer gibt oder nicht, ist jetzt nicht so spielentscheidend.

Sie haben auch gefragt wegen Quantencomputer und Internet. Ehrlich gesagt, bei der Quantentechnologie, wie ich sie heute verstehe, haben Quantenkommunikation und Internet wenig miteinander zu tun, weil das Punkt-zu Punkt-Verbindungen sind. Das ist noch echte Zukunftsmusik.

SVe **Prof. Dr. Stephanie Wehner:** Ich beantworte drei Fragen. Ich fange an mit dem Internet: Es ist natürlich so, dass es im Moment noch keine großen Quantennetzwerke gibt. Aber natürlich ist das Ziel beim Quantencomputer, sie zu bauen.

Zur Architektur: Es steht noch nicht fest. Das ist übrigens auch ein interessantes Forschungsthema, wo auch gerade die Informatik viel dazu beitragen kann.

Zu Technologie als Selbstzweck: Es ist natürlich so, dass es zum Beispiel Quantum Key Distribution, eine Methode des sicheren Schlüsselaustauschs, der auch beweisbar sicher ist gegen Attacken von einem Quantencomputer, als Punkt-zu-Punkt gibt. Ich denke, dass es innerhalb von fünf Jahren möglich sein wird, vielleicht einen Großraum wie Berlin an ein Sternnetzwerk anzuschließen.

Wie sollte man sich auf die Zukunft vorbereiten? Natürlich gibt es hier viele Aspekte, die auch schon erwähnt wurden. Ich denke, dass es wichtig ist, früh strategische Entscheidungen zu treffen, unabhängig von den Mitteln, die eingesetzt werden können. Das gilt gleichermaßen im Hardwarebereich, im Softwarebereich, in der Ausbildung und bei der Entwicklung neuer Start-ups. Und die Industrie benötigt den Zugang zu weiteren wissenschaftlichen Entwicklungen.

Zum Abschluss zu der Frage, wie kann die Quantentechnologie die Leute näher zusammenbringen: Ich denke, dass die Menschen eine natürliche Tendenz haben, näher zusammenzukommen. Das Interessante ist, was Menschen machen, wenn man ihnen Zugang

ermöglicht. Wir haben einen Simulator released (freigegeben) für unser Quantum-Internet Demo-Netzwerk und einen Programmierwettbewerb durchgeführt, wo jemand QuT-Chat geschrieben hat. Offenbar ist der Wunsch, dass es in der Zukunft ein quantenverschlüsseltes WhatsApp gibt. Gerade deshalb ist es wichtig, Menschen einen Zugang zu geben. Man sieht auch ganz neue und originelle Ideen, die dadurch entstehen.

SV **Prof. Dr. Frank Wilhelm-Mauch**: Zur Frage nach Extrapolation und Mooresches Gesetz: Als federführender Autor der BSI-Studie war ich sehr froh, dass das BSI nicht darauf bestanden hat, dass wir dazu etwas schreiben, weil es dafür noch relativ früh ist. Aber mit der Reifung der Technologien sehen wir, dass man für Fortschritt meistens keinen wissenschaftlichen Durchbruch mehr benötigt, sondern einfach konsistentes Engineering und eine große Menge von schrittweisen Innovationen. So, dass ich denke, dass es kontinuierlich weitergeht. Aber es gibt neben der Dimension der Größe, wo jetzt alle den 50 Qubits-Meilenstein erreichen wollen, auch die Dimension der Fehlerrate. Ich erwarte, dass wir auf dem Plateau zwischen 50 und 100 Qubits eine Weile bleiben werden und dann der Fortschritt zunächst an der Fehlerrate und der Länge des benutzbaren Quantenalgorithmus erkennbar sein wird, bevor wir wieder größer werden. Gordon Moore hatte tatsächlich drei Datenpunkte. Wir haben tatsächlich im Moment nur zwei.

SV **Dr Stephan Ritter**: Zu Leitplanken und wie man wirtschaftlich weiter kommen könne: Die Flaggschiff-Programme sind sicherlich auf einem sehr guten Weg. Ich glaube, dass wir Leuchtturmprojekte brauchen. In der nächsten Phase idealerweise unter Führung von Industriepartnern, weil die besser wissen, wie eine Überführung in Produkte möglich ist, im Bereich der Quantentechnologie und allgemein. Eine Standardisierung kann helfen, gerade für Schlüsseltechnologien, weil dann die Anbieter der Schlüsseltechnologien wissen, auf was sie hin entwickeln müssen und nicht für jede Nachfrage einen zersplitterten Markt bedienen müssen.

Die Vollkostenförderung ist angesprochen worden von Herrn Bluhm. Das ist ganz wichtig. Der Staat kann sicherlich durch Nachfrage Märkte schaffen. Das passt sehr zu dem, was Stephanie Wehner erwähnt hat. Wenn man zum Beispiel Teststrecken für Quantenkryptographie oder offen zugängliche Hardware für Quantum Computing schafft, auf denen jeder arbeiten kann, sind die Teststrecken und offen zugänglichen Geräte auch Entwicklungsprojekte für beteiligte Firmen, die einen kleinen aber soliden Markt darstellen.

Der **Vorsitzende**: Auf die Frage von Frau Dr. Sitte hat sich Herr Professor Wilhelm-Mauch gemeldet.

SV **Prof. Dr. Frank Wilhelm-Mauch**: Ein Aspekt zur Anwendung in der künstlichen Intelligenz ist, dass einige der Quantenalgorithmen, speziell im Optimierungsbereich, wo das Benchmarking noch nicht abgeschlossen ist, durchaus ein Teil sind, die in vielen Anwendungen in der künstlichen Intelligenz tief unten im Maschinenraum sitzt. Das kann durchaus Auswirkungen haben und es gibt auch direkte KI-Anwendungen. Aber die künstliche Intelligenz beruht immer auf der Analyse enorm großer klassischer Datenmengen, also Big Data eben. Das bedeutet, wenn ich eine Perlenschnur aufmache, wenn ich denke, dass bestimmte Dinge in der Entwicklung von Quantencomputern erreicht werden können, ist die Dimension, die für diese wirklich disruptive Anwendung in der künstlichen Intelligenz erreicht werden wird, sehr weit weg. So, dass ich mich der Idee anschließe, dass die Politik sich grundsätzlich mit der künstlichen Intelligenz auseinandersetzen sollte und dann auch für Quanten gewappnet sein wird.

SV **Prof. Dr. Winfried Hensinger**: Ich möchte noch sagen, wie bei allen Technologien kann man einen konventionellen Computer dazu verwenden, wunderbare Sachen in Krankenhäusern zu machen oder aber auch einen Sprengkopf einbauen. Letztendlich gesehen ist bei der Förderung von allen Technologien wichtig, dass wir sie verstehen und dass wir sie fördern. Deswegen ist es sehr wichtig, dass die Förderung nicht nur im militärischen Bereich, sondern generell frei passiert und frei gefördert wird. Deswegen ist es auch so wichtig, dass die

Quantentechnologie und die Quantencomputer hier in Europa genauso gefördert werden wie zum Beispiel in China. Da ist es wirklich wichtig zu sehen, dass in vielen Ländern das Investment in Quantum Computing sehr viel größer ist als in Europa, hundertmal größer als in ganz Europa. Da kann man sich vorstellen, wenn das so weitergeht, was dann auch mit der Technologie passiert. Und deswegen denke ich, das ist ganz wichtig anzumerken.

Zu der Frage von Herrn Janecek: Als Physiker muss ich erstmal antworten, dass der Vorteil der Quantencomputer darin liegt, dass man eigentlich mit einem Quantencomputer. keine Leistung verbraucht Aber als Physiker, der einen Quantencomputer baut, muss ich dann wiederum sagen, dass alle Ansätze, einen Quantencomputer zu bauen, einen riesigen Energieverbrauch haben, vor allem am Anfang. Wie gesagt, man benutzt Quantencomputer nicht für Zwecke, wo ein konventioneller Computer ausreicht, sondern man benutzt Quantencomputer nur, wenn es keine andere Möglichkeit gibt. Wenn man damit wirklich ein Problem lösen kann, das man sonst nicht lösen kann. Ja, diese Maschinen werden einen unglaublichen Stromverbrauch haben. Aber man muss sehen, was es dann ersetzt, beispielsweise jahrelange Forschung in einem Chemieunternehmen. Und das würde viel mehr Energie verbrauchen als unter Umständen den Quantencomputer ein paar Tage oder Monate laufen zu lassen.

Der **Vorsitzende**: Zum Abschluss darf ich Ihnen allen ganz herzlich dafür danken, dass Sie Rede und Antwort gestanden haben und dass Sie uns diese komplexen Thematiken ein Stück näher gebracht haben - auch wenn, wie vorher schon angeklungen, viele neue Fragen entstanden sind. Aber das liegt am Thema. Wir haben einen tieferen Einblick bekommen und dafür gilt Ihnen unser herzliches Dankeschön.

Ich darf mich auch bei den Kolleginnen und Kollegen bedanken, bei allen Anwesenden hier im Saal, denjenigen, die die Sitzung mitverfolgt haben. Natürlich gilt auch allen, die für den reibungslosen Ablauf der Sitzung sowie für die Technik und die Übertragung gesorgt haben, ein herzliches Dankeschön. Ihnen allen wünsche ich einen schönen Abend.

Die nächste Sitzung findet am 8. Juni 2018 um 8:00 Uhr hier im Paul-Löbe-Haus, im Raum E.300, statt.

Die Sitzung ist geschlossen.

Schluss der Sitzung: 18:00 Uhr

Hansjörg Durz, MdB
Stellvertretender Vorsitzender