

Prof. Dr. Winfried Hensinger
Professor of Quantum Technologies
Director, Sussex Centre for Quantum Technologies
Head, Sussex Ion Quantum Technology Group

1 June 2018

Stellungnahme zum Fragenkatalog zur öffentlichen Anhörung „Quantencomputer“ des Ausschusses Digitale Agenda am Mittwoch den 6. Juni 2018

1) Wie ist der Stand von Forschung und Technik auf dem Gebiet des Quantencomputing?

1.1 Für viele Jahre erschien es unklar ob solche Maschinen wirklich gebaut werden können da die dafür gebrauchte Kontrolle von Quantensystemen an der Grenze des machbaren erschien. In den letzten Jahren haben entscheidende Durchbrüche in der Forschung dazu geführt dass wir heute davon ausgehen dass solchen Maschinen wirklich gebaut werden können. Zum Beispiel haben wir im letzten Jahr eine Studie in dem renommierten Fachzeitschrift *Science Advances* veröffentlicht in der wir zeigen wie ein leistungsfähiger Quantencomputer gebaut werden kann (<http://advances.sciencemag.org/content/3/2/e1601540>, <https://www.nature.com/news/physicists-propose-football-pitch-sized-quantum-computer-1.21423>).

1.2 Viele physikalische Systeme wurden untersucht ob diese als Grundlage für den Bau von Quantencomputern benutzt werden können. Zwei Systeme haben großen Erfolg gezeigt. Ionen Qubits und supraleitende Qubits sind bei weitem die vielversprechendsten Systeme. In beiden Systemen wurden Fehlerraten erreicht die klein genug sind, dass ein Quantencomputer gebaut werden könnte. Supraleitende Qubits müssen aber fast bis zum absoluten Nullpunkt gekühlt werden (-273C), während Ionen Qubits nur leicht (-200C) oder gar nicht gekühlt werden müssen. Während dieser Unterschied für sehr kleine Quantencomputer nicht so wichtig ist, könnte die benötigte Kühlung nahe des absoluten Nullpunkt für supraleitende Qubits bei großen und leistungsfähigen Quantencomputern (die viele Millionen Qubit benötigen) ein großes Problem werden da es fast unmöglich ist eine ausreichende Kühlleistung bei so niedrigen Temperaturen zu erzielen. Auch gibt es noch keine modularen Designs für Quantencomputer mit supraleitenden Qubits was wiederum bedeutet das wirklich leistungsfähige Quantencomputer so nicht gebaut werden können. Deswegen hat es in letzter Zeit einen starken Trend zu der Entwicklung von Ionen Quantencomputern gegeben wo es realistischer erscheint große und leistungsfähige Quantencomputer zu bauen. So setzt die englische Regierung fast vollständig auf die Entwicklung von Ionen Quantencomputern und Google Ventures hat kürzlich in den Aufbau einer Firma für den Bau von Ionen Quantencomputern investiert.

1.3 Einen einstündigen populärwissenschaftlichen Vortrag den ich dazu am US Department of Energy gegeben habe finden Sie hier:

<https://www.youtube.com/watch?v=fccSQHBssi0&feature=youtu.be>

Einen kurzen Film über meine Forschungsgruppe finden Sie hier:

<https://www.youtube.com/watch?v=naqHy5MAYXw>

Einige relevant populärwissenschaftlichen Artikel finden Sie hier:

[Nature](#), [Financial Times](#), [PC Authority](#), [BBC](#), [Sky News Tonight With Dermot Murnaghan](#), [VICE](#), and [Daily Mail](#)

2) Welche Position haben im internationalen Vergleich Deutschland und Europa? Wer ist – im nationalen und im internationalen Vergleich – Vorreiter auf dem Gebiet des Quantencomputing, hinsichtlich Grundlagenforschung, anwendungsorientierter Forschung, technischer Entwicklung, sowie der Entwicklung möglicher Geschäftsmodelle? Welche Unternehmen/Akteure sind besonders hervorzuheben?

Welche Position haben China und die USA (Welche Ausprägungen der Technologie sind wo verbreitet?) Sollte die internationale Zusammenarbeit auf diesem Gebiet – z.B. im Bereich der Forschung, der industriellen Anwendung oder der Herstellung von QC – gestärkt werden?

2.1 England hat vor einigen Jahren das Potential von Quantencomputern erkannt und ein Ökosystem zur zielgerichteterrichteten Entwicklung der Quantencomputer geschaffen mittels des ‚National Quantum Technology Program‘. Weltweit wurde dieser Schritt als bahnbrechend erkannt und viele Länder versuchen nun ähnliche Programme aufzubauen. Durch dieses Program hat England seine führende Rolle auf diesem Gebiet weiter ausgebaut.

2.2 In Amerika wird ein grosser Teil der Forschungsgelder von Behörden verwaltet, die stark zielgetriebene Forschung vorantreiben. Dieses Model hat zum Beispiel zur Erfindung des Internets geführt. Ueber dieselben Behoerden wird auch die Entwicklung von Quantencomputern seit vielen Jahren finanziert, was zu grossen Erfolgen gefuehrt hat. Deswegen haben die USA eine fuehrende Rolle auf diesem Gebiet erzieht.

2.3 Andere Länder haben vor kurzem die Chancen von Quantencomputern erkannt und haben in grossen Stil in die Entwicklung von Quantencomputern investiert. Dazu gehoeren zum Beispiel die Niederlande, Oestereich, Canada und Australien.

2.4 China hat im Moment noch keine fuehrende Rolle auf diesem Gebiet. Das wird sich aber mit grosser Wahrscheinlichkeit bald aendern, da China intensiv in die Entwicklung von Quantencomputern investiert und effektive Kollaborationen mit internationalen Partnern aufbaut.

2.5 Deutschland's Role in Bereich der Entwicklung der Quantencomputer ist leider eher unbedeutend. Die Gründe dafür sind vielfältig. Im Bereich der Quantencomputer wurde relativ wenig investiert und es gibt wenig oder keine nationale Koordination. Das akademische System ist relativ regide was zum Abgang vieler Forscher in andere Laender, wie England und Amerika, geführt hat. Es gibt aber einzelne Gruppen die durchaus das Potential haben wichtige Beiträge bei der Entwicklung von Quantencomputern zu liefern, zum Beispiel die Gruppen von Ferdinand Schmidt-Kaler in Mainz und Christof Wunderlich in Siegen. Die Forschungsfoerderung in Deutschland macht es diesen Gruppen aber schwer sich an Forschungsprojekten in anderen Laendern effektiv zu beteiligen.

Prof. Dr. Winfried Hensinger, Professor of Quantum Technologies

Sussex Centre for Quantum Technologies | University of Sussex | Pevensey 2 Building | Brighton BN19QH | United Kingdom

T +44 (0)1273 877672 M+44 (0)7717113421 | w.k.hensinger@sussex.ac.uk

www.sussex.ac.uk/physics/igt

2.6 Gegenwaertig fehlt die Moeglichkeit weitgehend mit deutschen Gruppen zusammenzuarbeiten da es keine binationale Forschungsförderungsmöglichkeiten gibt. Zwar gibt es die Möglichkeit der Förderung über die EU. Hier muss man aber mehrere Laender involvieren, die Förderung ist auch nicht flexibel genug und viel zu gering in der Förderungshöhe um signifikante Fortschritte zu machen. Ausserdem ist die Gesamthöhe der Fördermittel so klein, dass die Erfolgsraten auch viel zu klein sind um einen wirklichen Unterschied zu machen. Bilaterale Forschungsabkommen mit anderen Ländern, zum Beispiel England, würden effektive Zusammenarbeit erlauben und würden dazu beitragen, Deutschland's Role in der Entwickluing von Quantencomputern zu stärken.

2.7 Das EU-Flagship in Quantum Technologies ist ein guter Anfang, aber der gesamte Förderungsrahmen ist viel zu klein um effektiv zur Entwicklung von Quantencomputern beizutragen. Die Förderung für Quantencomputing im EU Flagship fuer die naechsten drei Jahre beträgt €27M für ganz Europa. Dieser Betrag ist viel zu klein um Quantencomputer effektiv zu entwickeln und verteilt sich auf so viele Forschungsgruppen sodass der zu erwartente Vortschritt klein sein wird. Der Bewilligungsmechanismus für diese Gelder sollte auch mehr flexibler und fokussiert gestaltet werden um den Fortschritt dieser Technik zu beschleunigen. Beispiele einer effektivieren und gezielten Foerderung gibt es zum Beispiel bei manchen amerikanischen Behoerden, zum Beispiel IARPA, DARPA und ARO.

2.8 Ob Deutschland die Möglichkeit hat eine führende Rolle in der Entwicklung von Quantencomputern einnehmen kann, hängt weitgehend davon ab, ob sich der Staat sich dazu entschliesst diese Technologie gezielt zu fördern. Die jetzige Förderung dieser Technik in Deutschland ist ungenügend.

3) Welche möglichen gesellschaftlichen Chancen oder gesellschaftlichen Herausforderungen sehen Sie durch Quantencomputing? Welche Auswirkungen können Sie auf unser tägliches Leben haben? Ergeben sich spezielle Herausforderung, sobald diese Computer marktreife und entsprechende Verbreitung erlangen? Welche ökologischen Chancen oder Risiken bieten sich durch den Einsatz von Quantencomputing (z.B. Thema Green IT)?

3.1 Quantencomputer bieten die Möglichkeit manche Probleme zu lösen, wofuer auch die schnellsten Supercomputer Millionen Jahre brauchen wuerden. Die Auswirkungen der Entwicklung von Quantencomputern auf unser Leben könnte ähnlich sein, wie die Entwicklung von konventionellen Computern.

3.2 Quantencomputer brauchen neuartige Software, sogenannte Quantenalgorithmen. Diese muessen genauso entwickelt werden wie die Hardware. Zur Zeit gibt es nur wenige Wissenschaftler mit Erfahrung auf diesem Gebiet. 1944 gab es weltweit ungefaehr 5 konventionelle Computer und 50 Fachleute die diese programmieren konnten. Die Lage im Gebiet der Quantencomputer ist heute ähnlich, mit ungefähr 5 Quantencomputern weltweit und ungefaehr 50 Forschern die Quantenalgorithmen entwickeln können. Die ersten Anwendungsgebiete von konventionellen Computern lagen in den vierziger Jahren beim Codebrechen und der Berechnung der Bahnen von Projektilen. Die gezielte Entwicklung von konventionellen Computern hat dann zu den vielen Anwendungen von konventionellen Computern geführt die wir heute kennen. Bei Quantencomputern erwarte ich eine ähnliche Entwicklung. Machine Learning ist eine Anwendung wo schon klar ist das Quantencomputer eine wichtige Rolle spielen können. Es ist auch wahrscheinlich das bestimmte Optimierungsprobleme auf Quantencomputern gelöst werden können, was zum Beispiel folgenschwere Auswirkungen auf den finanziellen Sektor haben könnte.

Prof. Dr. Winfried Hensinger, Professor of Quantum Technologies

Sussex Centre for Quantum Technologies | University of Sussex | Pevensey 2 Building | Brighton BN19QH | United Kingdom

T +44 (0)1273 877672 M+44 (0)7717113421 | w.k.hensinger@sussex.ac.uk

www.sussex.ac.uk/physics/igt

3.3 Die Quantentheorie gibt uns die Möglichkeit die Welt um uns vollständig zu verstehen, ob es da um chemische Reaktionen geht, Eigenschaften von Materialien, Prozesse in biologischen Systemen oder die Entwicklung von neuen Medikamenten. Konventionelle Computer sind aber nicht leistungsvoll genug um solchen Probleme ausrechnen zu können da die gebrauchte Rechenleistung für genaue Berechnungen auch die Möglichkeiten der größten Supercomputer übersteigt. Deshalb müssen Wissenschaftler Näherungen benutzen damit solche Berechnungen auf konventionellen Computern überhaupt durchgeführt werden können. Diese Näherungen führen aber dazu dass man viele Dinge einfach nicht ausrechnen kann. Quantencomputer können solche Berechnungen exakt ausführen da deren Funktionsweise auf der Quantentheorie beruht. Das heißt dass man plötzlich manche Dinge genau berechnen kann, die unmöglich auf einem konventionellen Computer zu berechnen wären. Es gibt einige Beispiele die die Bedeutung dieser Fähigkeit zeigen. Es gibt Anhaltspunkte das ein Quantencomputer uns helfen kann Proteinfaltung zu verstehen. Das wiederum könnte uns helfen Demenz heilen zu können. Auch könnten Quantencomputer ein besseres Verständnis von chemischen Reaktionen liefern und so zur Entwicklung neuer Medikamente beizutragen. Quantencomputer könnten auch bei der Entwicklung neuer Materialien helfen.

3.4 Es ist sehr wahrscheinlich dass Quantencomputer neue Möglichkeiten schaffen, die es bisher nicht gab und damit massiven Einfluss auf gewisse Industriesektoren haben werden. Das wiederum könnte bedeuten das Firmen die Anwendungen auf solchen Maschinen entwickeln und diese dann anwenden die Konkurrenz vom Markt drängen könnten. Das könnte dann ähnlich verlaufen wie es mit Google's Suchalgorithmen passiert ist, dessen Existenz andere Suchmaschinen vom Markt gedrängt hat.

3.5 Es ist noch viel zu früh um die wichtigsten Anwendungen von Quantencomputern abschätzen zu können da wir erst am Anfang der Entwicklung dieser Technologie stehen.

4) Sehen Sie zum jetzigen Zeitpunkt regulatorische Anforderungen? Sehen Sie – legislativen und nicht-legislativen – Handlungsbedarf der Politik? Gibt es voraussichtlich einen Handlungsbedarf zum „Thema Dual Use“?

4.1 Es ist wichtig die Entwicklung von Quantencomputern genau zu folgen um abschätzen zu können wann Regulierung notwendig sein wird. Im Moment gibt es nur Prototypen deren Leistung immer noch kleiner ist als die von konventionellen Computern. Deswegen erachte ich Regulierung im Moment als noch nicht notwendig. Das wird sich aber ändern wenn leistungsfähigere Quantencomputer gebaut werden.

5) Welche Projekte und Erkenntnisse der Technikfolgenabschätzung existieren bereits für den Bereich des Quantencomputing?

5.1 Es gibt hierzu nur spekulative Studien da das Feld der Anwendungsforschung noch ganz am Anfang steht. Ich habe hierzu ein Kapitel in einem populärwissenschaftlichen Buch geschrieben. ‚What's Next?: Even Scientists Can't Predict the Future – or Can They?‘ ist erschienen bei Profile Books (2017) (https://www.amazon.de/Whats-Next-Science-Fascinating-Future/dp/1781258953/ref=tmm_pap_title_0?encoding=UTF8&qid=1527945210&sr=1-1).

6) Welche besonderen Leistungen und Eigenschaften erwarten Sie von Quantencomputern? Welche Aufgaben könnten Quantencomputer erfüllen? Welchen Nutzen können sie generieren? In der Folge: Welche – wissenschaftlichen und ggf. gesellschaftlichen - Herausforderungen und Probleme können mit Quantencomputing gelöst werden?

6.1 Ich erwarte Anwendungen in vielen Wirtschafts und Wissenschaftsbereichen. Der Einfluss von Quantencomputern könnte in vielen Aspekten unseres täglichen Lebens eine große Rolle spielen. Eine genaue Abschätzung ist aber genauso unmöglich wie es 1940 unmöglich war die wichtigsten Anwendungen von konventionellen Computern abzuschätzen. Technologieabschätzungen mit einer Zeitspanne von mehr als 5 Jahren sind schwierig oder unmöglich und es ist sehr wichtig dass auch so einzuschätzen. Mit Sicherheit werden Quantencomputer nicht alle Probleme lösen können, vor allem nicht in einer frühen Phase ihrer Entwicklung. Mehr und mehr Anwendungen werden geschaffen werden, vor allem wenn erste leistungsstarke Maschinen vorhanden sind.

7) Welche Anwendungen sind denkbar? Wie belastbar ist die Annahme einer „Quantum Supremacy“ (auch bezogen auf vereinzelte Anwendungsbereiche) im Vergleich zu klassischen (Super-)Computern? Bitte benennen Sie, zur besseren Verständlichkeit, ggf. Beispiele, falls möglich insbesondere in den Bereichen Klima-/Energie-Forschung, Verkehr, Medizin, Industrie 4.0., Verteidigung. Welche Auswirkungen erwarten Sie von Fortschritten auf dem Gebiet des Quantencomputing auf andere Technologiebereiche (Maschinelles Lernen, Künstliche Intelligenz, Blockchain, Supercomputing, Kommunikation, aber auch Autonomes Fahren etc.)?

7.1 Die Anwendungen dieser Technik werden vielfältig sein. Es ist aber wichtig zu verstehen, dass man einige Zeit investieren muss um geeignete Qantenalgorithmen zu entwickeln die für bestimmte Anwendungen benutzt werden können. Ersten Anwendungen erwarte ich bei Optimierungsproblem, zum Beispiel um eine optimale (aus vielen möglichen) Routen zu finden. Andere erste Anwendungen sehe ich beim Maschinellen Lernen.

7.2 Quantum Supremacy ist eine Entwicklungsstufe für Quantencomputer. Hier kann für ein bestimmtes wissenschaftliches Problem gezeigt werden, dass ein Quantencomputer ein Problem lösen kann das ein konventioneller Computer nicht lösen kann. Quantum Supremacy wird jedoch erst für Problem gezeigt werden die von purer wissenschaftlicher Natur sind und keine praktische Anwendung haben.

8) Welche (technischen) Herausforderungen bestehen? Welcher Zeitrahmen erscheint realistisch, um diese zu überkommen? Wie können Fehlerrate und Qualität der Qbits verbessert werden? Aktuell werden verschiedene Qbit-Implementierungen erforscht - welche hat, Ihrer Meinung nach, das größte Potenzial?

8.1 Die technischen Herausforderungen sind riesig. Erste Quantencomputer existieren heute schon, zum Beispiel in unserem Labor an der University of Sussex, diese sind aber nur Prototypen.

8.2 Der Zeitrahmen für die Entwicklung hängt stark von der Förderung der Forschung in diesem Bereich ab. Man kann aber davon ausgehen dass es in 5-10 Jahren Quantencomputer geben wird die zumindest manche Probleme lösen können die auch nicht auf den schnellsten konventionellen Computern gelöst werden können. Die Zahl der Anwendungen und die Rechenstärke wird dann langsam wachsen wie es bei konventionellen Computern der Fall gewesen ist.

Prof. Dr. Winfried Hensinger, Professor of Quantum Technologies

Sussex Centre for Quantum Technologies | University of Sussex | Pevensey 2 Building | Brighton BN19QH | United Kingdom

T +44 (0)1273 877672 M+44 (0)7717113421 | w.k.hensinger@sussex.ac.uk

www.sussex.ac.uk/physics/igt

8.3 Fehlerraten und Qualität der Qubits sind ein zentrales Thema der Forschung im Bereich der Quantencomputer. Auch hier sind ausreichende Forschungsmittel von kritischer Bedeutung. Die Förderung in diesem Bereich in Deutschland ist unzureichend, vor allem auch im Hinblick auf die Möglichkeit der internationalen Zusammenarbeit auf diesem Gebiet.

8.4 Viele physikalische Systeme wurden untersucht ob diese als Grundlage für den Bau von Quantencomputern benutzt werden können. Zwei Systeme haben großen Erfolg gezeigt. Ionen Qubits und supraleitende Qubits sind bei weitem die vielversprechendsten Systeme. In beiden Systemen wurden Fehlerraten erreicht die klein genug sind, dass ein Quantencomputer gebaut werden könnte. Supraleitende Qubits müssen aber fast bis zum absoluten Nullpunkt gekühlt werden (-273C), während Ionen Qubits nur leicht (-200C) oder gar nicht gekühlt werden müssen. Während dieser Unterschied für sehr kleine Quantencomputer nicht so wichtig ist, könnte die benötigte Kühlung für supraleitende Qubits nahe dem absoluten Nullpunkt bei großen und leistungsfähigen Quantencomputern (die viele Millionen Qubits benötigen) ein großes Problem werden da es fast unmöglich ist eine ausreichende Kühlleistung bei so niedrigen Temperaturen zu erzielen. Auch gibt es noch keine modularen Designs für Quantencomputer mit supraleitenden Qubits was wiederum bedeutet das wirklich leistungsfähige Quantencomputer so nicht gebaut werden können. Deswegen hat es in letzter Zeit einen starken Trend zu der Entwicklung von Ionen Quantencomputern gegeben wo es realistischer erscheint große und leistungsfähige Quantencomputer zu bauen. So setzt die englische Regierung fast vollständig auf die Entwicklung von Ionen Quantencomputern und Google Ventures hat kürzlich in den Aufbau einer Firma für den Bau von Ionen Quantencomputern investiert.

8.4 Erste Konzepte für den Bau eines Ionen Quantencomputers benötigten Laserstrahlen um logische Operationen durchzuführen. Für jedes Qubit hätte man dann zwei Laserstrahlen gebraucht die man mit einer Genauigkeit eines Hundertstels eines Millimeters auf einzelne Atome auszurichten müsste. Mit Millionen oder Milliarden von Qubits müsste man dann ebenso viele Laserstrahlen in einem Quantencomputer einbauen was fast unmöglich erscheint. Vor 2 Jahren haben wir an der University of Sussex eine neue Methode erfunden mit der wir diese Millionen oder Billionen Laserstrahlen mit Spannungen ersetzen können die an einen Mikrochip angelegt werden (<http://www.sussex.ac.uk/news/media-centre/press-releases/id/38093?id=38093>). Das ist dann ähnlich wie die Funktionsweise eines Transistors oder konventionellen Computerchips. Diese Idee vereinfacht den Bau eines leistungsstarken Quantencomputer auf eine dramatische Weise, so dass jetzt möglich erscheint einen leistungsstarken Quantencomputer bauen zu können. Mit dieser Erfindung waren wir in der Lage den ersten Bauplan für einen Quantencomputer mit Millionen oder sogar Milliarden von Qubits zu entwickeln (<http://advances.sciencemag.org/content/3/2/e1601540>, <https://www.nature.com/news/physicists-propose-football-pitch-sized-quantum-computer-1.21423>). Wir werden jetzt einen solchen Quantencomputer bauen.

9) Welche wirtschaftlichen Chancen können aus Fortschritten im Bereich des Quantencomputing entstehen? In welchen zeitlichen Inkrementen rechnen Sie mit Fortschritten? Wann rechnen Sie mit welchen Formen einer Markteinführung? Welche Entwicklungen veranlassen Sie zu der Annahme, dass Quantencomputer in absehbarer Zeit Marktreife erreichen können oder auch nicht erreichen können?

9.1 Quantencomputer benutzen eine fundamental andere Methode Rechnungen durchzuführen. Man könnte sogar argumentieren dass sie parallele Universen benutzen um ihre Rechnungen durchzuführen. Das heißt dass es gut möglich ist dass die Anwendungen dieser Maschinen weit übersteigen was wir uns heute vorstellen können. Auf der anderen Seite ist es nie einfach die Zukunft

vorherzusagen. Ich wär aber schon sehr überrascht wenn diese Maschinen nicht zahllose Industriesektoren revolutionieren werden.

9.2 Die Markteinführung dieser Maschinen wird langsam passieren. Am Anfang wird man diese Maschinen über die Cloud benutzen für ganz bestimmte Anwendungen. Mit der Entwicklung von mehr Quantenalgorithmen wird auch die Zahl der Anwendungen steigen. Ich sehe große Parallelen mit der Einführung von konventionellen Computers. Diese wurden in den vierziger Jahren entwickelt und deren Rechenleistung trug maßgeblich dazu bei den zweiten Weltkrieg zu entscheiden. Die Anwendungen wurden dann immer mehr bis wir alle einen Computer benutzten. Ich könnte mir erste wichtige kommerzielle Anwendungen in 5-10 Jahren vorstellen. Aber die genaue Zeit wird davon abhängen wie gezielt die Entwicklung dieser Maschinen vorangetrieben wird. Hier ist die Politik gefragt ausreichende Förderung zu gewährleisten.

9.3 Die technischen Entwicklungen auf dem Gebiet der Forschung geben mir Vertrauen, dass eine Markteinführung in absehbarer Zeit erfolgen kann. Wie schon in Frage 8 erklärt, vor 2 Jahren haben wir an der University of Sussex eine neue Methode erfunden wo wir Millionen oder Milliarden von Laserstrahlen mit Spannungen ersetzen können die an einen Mikrochip angelegt werden (<http://www.sussex.ac.uk/news/media-centre/press-releases/id/38093?id=38093>). Das ist dann ähnlich wie die Funktionsweise eines Transistors oder konventionellen Computerchips. Diese Idee an den Bau eines leistungsstarken Quantencomputer auf eine solche Weise vereinfacht, dass wir jetzt planen können eine solche Maschine zu bauen.

(<http://advances.sciencemag.org/content/3/2/e1601540>, <https://www.nature.com/news/physicists-propose-football-pitch-sized-quantum-computer-1.21423>).

10) Wird sich Deutschland als wesentlicher Hersteller von Quantencomputing-Hardware etablieren können, oder sollte Deutschland eher die Entwicklung von Systemanwendungen oder Software fördern? Sind für die Herstellung von Quantencomputer kritische Ressourcen erforderlich (vgl. z. B. Thema „Seltene Erden“), die deutsche Hersteller im außereuropäischen Ausland beschaffen müssten?

10.1 Im Moment sehe ich in Deutschland keine Zentren die das Potential hätten einen Quantencomputer selbstständig zu entwickeln. Es gibt aber viele Gruppen die wichtige Beiträge zur Entwicklung eines Quantencomputers leisten könnten. Es gibt in Deutschland experimentelle Physik Gruppen, theoretische Physik Gruppen und Ingenieurwissenschaftliche Gruppen die dazu beitragen könnten den Bau eines Quantencomputers stark zu beschleunigen als Teil einer bi-nationalen Initiative zwischen England und Deutschland. Leider gibt es zurzeit keine entsprechende Förderungsmöglichkeiten. Eine nahe Zusammenarbeit zwischen Deutschland und England würde hier ein riesiges Potential eröffnen und sicherstellen dass Deutschland und England zusammen eine führende Stellung weltweit im Feld des Baus der Quantencomputer erhalten würden. Falls eine solche Zusammenarbeit nicht realisiert werden kann, muss gefürchtet werden dass China und die USA weitgehend Dominanz auf diesem Gebiet erzielen könnten und der High Tech Standort Europa auf dem Gebiet des Baus von Quantencomputern verloren geht.

10.2 Für den Bau von Quantencomputern sind keine kritischen Ressourcen in der Form von Materialien erforderlich. Was hier kritisch ist sind geeignete Wissenschaftler und Ingenieure die die notwendige Expertise haben um den Bau dieser Maschinen voranzutreiben.

10.3 Die Entwicklung von Systemanwendungen und der Software muss am besten zusammen mit

Prof. Dr. Winfried Hensinger, Professor of Quantum Technologies

Sussex Centre for Quantum Technologies | University of Sussex | Pevensey 2 Building | Brighton BN19QH | United Kingdom

T +44 (0)1273 877672 M+44 (0)7717113421 | w.k.hensinger@sussex.ac.uk

www.sussex.ac.uk/physics/igt

der Hardware entwickelt werden. Eine isolierte Entwicklung von entweder Software oder Hardware ist nur bedingt sinnvoll. Deutschland sollte in Software und Hardware Entwicklung investieren. Dies ist auch für die deutsche Industrie von kritischer Bedeutung.

11) Welche Art der (öffentlichen) Förderung und welche weiteren Rahmenbedingungen sind aus Ihrer Sicht erforderlich, um diese Technologie voranzubringen? Wie viele Mittel fließen weltweit in die Forschung und Entwicklung von Quantencomputing, welche Länder und welche Firmen investieren am meisten?

11.1 Falls Deutschland nicht den Anschluss an diese Technologie verlieren will müssen die Investitionen in diese Technologie massiv ausgedehnt werden. Die jetzige Förderung über die DFG ist nicht ausreichend und das DFG Förderungsmodell ist auch nicht für eine zielgerichtete Entwicklung von Quantencomputern geeignet.

11.2 Ich empfehle eine flexible öffentliche Förderung die sich an dem Beispiel der US Behörden IARPA, DARPA oder ARO orientiert. Dabei ist es wichtig bi-nationale Zusammenarbeit mit England (und unter Umständen auch anderen Ländern) einzubeziehen um die Stärken beider Länder in einer solchen Weise zu verbinden um den Bau von Quantencomputern zu beschleunigen.

11.3 Viele hunderte Millionen werden weltweit für den Bau von Quantencomputern ausgegeben. Deutschland steht im Moment weit hinten in der Förderung von Quantencomputern. Viele große Firmen und Venture Kapital Firmen haben in die Entwicklung von Quantencomputern investiert. Beispiele solcher Firmen sind Google, Microsoft, IBM, Airbus und Intel. Es gibt auch eine Reihe von vielversprechenden Startups, zum Beispiel IonQ in den USA. Wir sind gerade dabei ein Startup für die Entwicklung von Quantencomputern in England aufzubauen und würden uns über Kollaborationen mit deutschen Forschungsgruppen und Firmen freuen, da es in Deutschland vielversprechende Expertise gibt.

12) Welche Forschungsstrategie sollte Deutschland bzw. Europa entwickeln, um international anschlussfähig zu bleiben?

12.1 Das EU Quantum Technology Flagship ist ein guter Anfang, aber das Förderungsmodell ist zu unflexibel, zu klein im Förderungsrahmen und orientiert sich viel zu sehr an der traditionellen ‚Blue Sky Research‘ Förderung der EU.

12.2 Wie schon unter 11) beschrieben, ich empfehle eine flexible öffentliche Förderung die sich an dem Beispiel der US Behörden IARPA, DARPA oder ARO orientiert.

12.3 Es ist wichtig binationale Zusammenarbeit mit England (und unter Umständen auch anderen Ländern) zu ermöglichen um die Stärken beider Länder in einer solchen Weise zu verbinden um den Bau von Quantencomputern optimal voranzutreiben. Um das zu ermöglichen sollten gemeinsame Förderungsprogramme geschaffen werden.

12.4 Die Förderung sollte über den Bund und nicht über die Länder erfolgen da somit eine bessere Koordination möglich wäre.

13) Ist die Nutzung der QC-Hardware abhängig von einer neuen Art Software? Falls ja, ist die Forschung und Weiterbildung daran in Deutschland auf internationalem Niveau oder wie müsste nachgebessert werden?

13.1 Quantencomputer benötigen eine neue Art von Software. Die Entwicklung von Quantenalgorithmen an sich kann weitgehend unabhängig von der Quantencomputerhardware erfolgen. Man muss dann aber auch Software entwickeln die es erlaubt solche Quantenalgorithmen auf bestimmter Hardware laufen zu lassen. Unterschiedliche Hardware Plattformen (zum Beispiel Ionen Qubits oder Supraleitende Qubits) haben unterschiedliche Vor- und Nachteile und man kann Software dazu benutzen den Quantencomputer dementsprechend zu optimieren. Vor allem für die frühen Anwendungen von Quantencomputern wird die nahe Zusammenarbeit zwischen Software und Hardware Entwicklung unerlässlich sein, da man dann die Vorteile gewisser Hardware Plattformen dann auch gezielt einsetzen muss.

14) Ab wann werden heute angewendete Verschlüsselungsalgorithmen und Instrumente aus dem Bereich der IT-Sicherheit (z.B. Verschlüsselungstechnologien, Blockchain-Technologien) voraussichtlich unsicher? Bitte schlüsseln Sie die angenommenen zeitlichen Horizonte für möglichst viele Verschlüsselungsalgorithmen und Instrumente einzeln auf. Warum werden die benannten Verschlüsselungsalgorithmen und Instrumente unsicher? Wie kann sichergestellt werden, dass wir rechtzeitig darauf vorbereitet sind

14.1 Die derzeitigen Verschlüsselungsalgorithmen und Instrumente aus dem Bereich der IT-Sicherheit beruhen auf die RSA Verschlüsselung. Um diese zu brechen braucht man einen leistungsstarken Quantencomputer mit Millionen oder Milliarden Qubits. Eine solche Entschlüsselung ist eine der späteren Anwendungen von Quantencomputern da man dafür sehr viele Qubits benötigt. Die Zeit die dafür gebraucht wird eine solche Maschine zu bauen hängt stark von der Förderung der Quantencomputertechnologie ab. Ich wär aber sehr überrascht wenn es solche Maschinen in weniger als 10 Jahren geben würde da die Konstruktion von so leistungsfähigen Maschinen immer noch eine ingenieurwissenschaftliche Meisterleistung darstellt.

14.2 Es wird jetzt im Moment aktiv an alternativen Verschlüsselung Methoden gearbeitet die dann mit jetzt bekannten Quantenalgorithmen nicht mehr gebrochen werden können. Deswegen kann man davon ausgehen das es Verschlüsselungsalgorithmen und Instrumente geben wird die dann auch sicher sind wenn leistungsstarke Quantencomputer gebaut werden. Es ist aber wichtig zu betonen, dass Daten die heute mit RSA verschlüsselt wurden and heute abgefangen worden sind, in 10 Jahren mit Hilfe eines Quantencomputers entschlüsselt werden können, was dann natürlich auch unter Umständen eine Gefahr darstellen kann.

15) Was wird für die Weiterentwicklung von Quantenkryptografie benötigt? Wie können alle notwendigen Fachgebiete in der Wissenschaft bei der Weiterentwicklung von Quantenkryptografie eingebunden werden? Wie können die Entwicklungen der Quantenkryptografie breit zugänglich gemacht werden in Industrie, Ausbildung und für die End User? Wie kann Quantentechnologie auch kleinen Start-ups oder Einzelpersonen zugänglich gemacht werden, um Anwendungen zu entwickeln? Gibt es mögliche Implikationen für den Datenschutz, wenn Quantenkryptografie weit verbreitet ist?

15.1 Die Quantenkryptographie ist schon sehr weit entwickelt und als kommerzielle Technik erhältlich. Manche Banken benutzen solche Technik schon heute. Für die Benutzung dieser Technik braucht man aber spezielle Leitungen, man kann nicht einfach das Internet benutzen. Deswegen ist es wichtig

Prof. Dr. Winfried Hensinger, Professor of Quantum Technologies

Sussex Centre for Quantum Technologies | University of Sussex | Pevensey 2 Building | Brighton BN19QH | United Kingdom

T +44 (0)1273 877672 M+44 (0)7717113421 | w.k.hensinger@sussex.ac.uk

www.sussex.ac.uk/physics/igt

neue Verschlüsselungstechniken zu entwickeln die zwar nicht so sicher sind wie echte Quantenkryptographie, aber den Vorteil haben, auf dem existierenden Internet angewendet werden zu können.

Weiter Information finden Sie auf:

<http://www.sussex.ac.uk/physics/iqt/>

Prof. Dr. Winfried Hensinger, Professor of Quantum Technologies

Sussex Centre for Quantum Technologies | University of Sussex | Pevensey 2 Building | Brighton BN19QH | United Kingdom

T +44 (0)1273 877672 M+44 (0)7717113421 | w.k.hensinger@sussex.ac.uk

www.sussex.ac.uk/physics/iqt