Gösta Fürnkranz

Vision Quanten-Internet

Ultraschnell und hackersicher

EBOOK INSIDE

Springer

Vision Quanten-Internet

Gösta Fürnkranz

Vision Quanten-Internet

Ultraschnell und hackersicher

Springer

Gösta Fürnkranz
Hinterbrühl, Österreich

ISBN 978-3-662-58452-1 ISBN 978-3-662-58453-8 (eBook)
https://doi.org/10.1007/978-3-662-58453-8

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Einbandabbildung: © AndSus/stock.adobe.com
Planung/Lektorat: Lisa Edelhäuser

Springer ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Einleitung

Die Digitalisierung ist längst zum bestimmenden Element unserer Zeit geworden. Ihre zukünftige Entwicklung bietet vielfältige Chancen und Potenziale, die es zu realisieren gilt. Eine sichere digitale Kommunikation ist dabei ein besonders wichtiger Faktor. Um deren Sicherheit langfristig zu gewährleisten, können innovative Technologien eine wesentliche Rolle spielen. Wir beobachten heute eine rasant steigende Zahl unautorisierter Zugriffe und Manipulationen in Kommunikationsnetzen mit wachsendem Schaden für Einzelpersonen, Gesellschaft und Wirtschaft. Die vermehrte Nutzung des Internets öffnet ein gewaltiges Bedrohungspotenzial hinsichtlich krimineller und terroristischer Zugriffe. Vor allem in Hinblick auf die stete Zunahme von Online-Geschäften, die immer stärker voranschreitende systemische Vernetzung sowie den Ausbau des Internets der Dinge werden Fragen der Datensicherheit und -integrität immer wichtiger. Bereits heute diskutierte Schlagworte wie Industrie 4.0,

autonomes Fahren, Wearables oder Smart City sind Vorboten einer voll vernetzten digitalen Gesellschaft, in der es zu einer explosiven Zunahme an Datenmaterial kommen wird. Dieser Entwicklung kann längerfristig gesehen nur mit völlig sicheren Technologien begegnet werden. Die bisherige Sicherheitstechnologie setzt dabei fast ausnahmslos darauf, den Datenzugang bloß zu erschweren. Es gibt jedoch eine Alternative, welche den unbefugten Zugang zu Daten und Informationen aus inhärent physikalischen Gründen komplett unmöglich machen kann: die Quantenkommunikation.

Im Zentrum dieser Entwicklung steht der Begriff Quanteninformation, welcher einen völlig neuen Zugang zur Informationstheorie eröffnet. In der aktuellen IT erfolgen Datenverarbeitung und Transfer ausschließlich auf Basis von Bits und Bytes, also Folgen von Binärzahlen, die definitionsgemäß nur die Ziffern 0 und 1 enthalten. Die Quanteninformation definiert dagegen als Elementareinheit das Quantenbit (Qubit), welches einer Art gleichzeitige Überlagerung von 0 und 1 entspricht. Damit ergeben sich gegenüber dem klassischen Informationsbegriff zwei wesentliche Vorteile: Zum einen können Quantenbits viel mehr Informationen speichern und übertragen als herkömmliche Bits. Zum anderen beinhalten Qubits einen inhärenten Sicherheitsaspekt, der es unmöglich macht, Quanteninformation abzuhören beziehungsweise zu hacken. Dies ist eine völlig neue Funktionalität, die es in der klassischen IT nicht gibt. Klassische Information kann beliebig kopiert und vervielfältigt werden und ist somit automatisch der unautorisierten Weitergabe preisgegeben. Im Fall von Quantenbits ist dies nach heutigem Wissen aus physikalischen Gründen unmöglich.

In den letzten Jahren sind in der Grundlagenforschung eine Reihe wichtiger Prinzipien demonstriert worden, die das hohe Potenzial dieser Technologie unterstreichen.

Die bahnbrechenden Ergebnisse aktueller Experimente stellen einen Meilenstein in der Entwicklung der Quantenkommunikation dar. So konnten beispielsweise Quantenkanäle bereits auf Entfernungen von bis zu 1203 km erfolgreich realisiert werden. Erste Geräte zur Quantenkryptografie werden von einschlägigen Firmen angeboten. Weltweit werden daher erhebliche Anstrengungen unternommen, um die technischen Voraussetzungen für eine globale Verbreitung schaffen zu können Alle diese Maßnahmen zielen darauf ab, die Quantenkommunikation auch über große Entfernungen zu ermöglichen. In letzter Konsequenz ist dafür ein spezielles Quantennetzwerk erforderlich, das als erste Prototypen in Europa; Asien und den USA implementiert wurde. In China und Europa existieren hierzu erste Fördermaßnahmen, welche einschlägig aktive Forschungseinrichtungen und Unternehmen unterstützen. In Fachkreisen wird dieser Entwicklung eine große Zukunft vorhergesagt. Gerade auch der europäischen Forschung (wo diese Technik ihre Wurzeln besitzt) ist es ein zentrales Anliegen, die abhörsichere Quantenkryptografie marktfähig zu machen.

Eine weitere Triebfeder für die Ausbildung eines Quantennetzwerks liegt in der aktuellen Computerentwicklung, welche aus physikalischen Gründen in absehbarer Zeit an eine Grenze stoßen wird. Hinzu kommt die Schwierigkeit, dass es heute schon EDV-Probleme gibt, die selbst von Supercomputern entweder viel zu langsam oder gar nicht sinnvoll bearbeitet werden können. Die Suche nach innovativen Konzepten hat daher in der Computerwelt längst eingesetzt. Der revolutionärste Ansatz besteht im Konzept des Quantencomputers. Das ehrgeizigste Ziel der Quanteninformatik ist die Entwicklung eines technisch nutzbaren Quantencomputers. Das große kommerzielle Interesse der Industrie, allen

voran klangvolle Namen wie Google, IBM oder Microsoft, lassen dieses Ziel realistisch erscheinen. Studien von Morgan Stanley räumen dem Quantencomputer mittlerweile einen hohen Stellenwert ein, selbst Kritiker wie der Informatiker Scott Aaronson stimmen dem zu. Obwohl gegenwärtig noch im juvenilen Stadium, sind die Quantenrechner der möglicherweise einzige Hoffnungsträger, der imstande wäre, die Computerleistung klassischer Rechner noch erheblich zu toppen. Sollte der Quantencomputer einst die Schwelle zur technischen Nutzbarkeit überwinden, stellt er eine umso faszinierendere Vision in Aussicht: Die Kombination aus inhärenter Datensicherheit und der potenziellen Vernetzung von Quantencomputern könnte eines Tages ein Quanteninternet entstehen lassen, das in punkto Sicherheitsaspekt und Verarbeitungsgeschwindigkeit zu einem völligen Paradigmenwechsel führt. Durch die theoretische Fähigkeit von Quantenrechnern, bestimmte Problemstellungen zu bewältigen, die selbst für Supercomputer unlösbar sind, könnte ein solches Quantenhypernet noch ungeahnte Möglichkeiten der zukünftigen Informationswelt bereithalten.

Zur Auslegung des Buchs möchte der Autor folgendes bemerken: Der Autor bedient sich einer bewusst optimistischen Sprechweise, weil die Forschung bereits wichtige Erfolge zu verbuchen hat und es sich lohnt, die Perspektiven und Potenziale des noch so jungen Gebiets der Quanteninformationstechnologie einer breiten Öffentlichkeit aufzuzeigen. Immerhin basieren diese auf wissenschaftlichen Erkenntnissen von fundamentaler Tragweite. Freilich ist die Quantenphysik bis heute eine kontroversiell diskutierte Thematik, die selbst von ihren profundesten Kennern nicht immer verstanden wurde und wird. Gerade in der populärwissenschaftlichen Darstellung stellt es eine besondere Herausforderung dar,

den Drahtseilakt zwischen fachlicher Genauigkeit und Simplifizierung zu meistern. Um Missverständnissen und Fehlinterpretationen vorzubeugen, sei dem Leser empfohlen, das Buch in seiner Chronologie zu lesen, da es eine beinahe durchgängige didaktische Struktur enthält. So werden zahlreiche Begriffe zunächst nur erwähnt, danach immer wieder aufgegriffen und weiter vertieft. Bereits in Teil 1 werden Versuchsanordnungen diskutiert, die eine wichtige Grundlage für spätere experimentelle Anordnungen und Prinzipdarstellungen in Teil 2 und Teil 3 bilden. In manchen Aspekten weicht der Autor bewusst von üblichen Erklärungsmodellen ab, indem er das heute verstärkt diskutierte Konzept Information (im Sinne einer tiefer gehenden physikalischen Entität) explikativ einbringt. Damit nimmt er Anteile an Positionen, wie sie von Instanzen (wie beispielsweise Anton Zeilinger) vertreten werden. In diesem Sinne möchte der Autor umfassend über den aktuellen Stand der Forschung zum Thema Quanteninternet informieren und sich gemeinsam mit dem Leser auf eine faszinierende Zukunftsreise begeben als Vorgeschmack auf eine neue technologische Ära, die einst Realität werden könnte.

Inhaltsverzeichnis

1

Die quantendigitale Zukunft

1.1 Digitale Visionen

Als vor gut 200 Jahren die industrielle Revolution einsetzte, bedeutete sie weltweite Veränderungen. Damit verbunden war eine tief greifende Umgestaltung der wirtschaftlichen und sozialen Verhältnisse, was die Entwicklung von Produktivität, Technik und Wissenschaft stark beschleunigte. Im Nebenaspekt ergaben sich aber auch eine Reihe von gesellschaftlichen Problemen, verbunden mit Arbeiterunruhen, die Regulierungen und soziale Reformen notwendig machten. Nun, im 21. Jahrhundert, steht der Mensch vor einer ähnlich epochalen Veränderung. Während damals die Muskelkraft durch die Dampfmaschine ersetzt wurde, lebt der Mensch nunmehr im digitalen Zeitalter, wo der Mikrochip sich anschickt, die geistige Arbeit zu substituieren. Was in den 1940ern mit der Entwicklung des Computers begann, später die erste Mondlandung ermöglichte, Taschenrechner zum

G. Fürnkranz, *Vision Quanten-Internet,*
https://doi.org/10.1007/978-3-662-58453-8_1

Massenprodukt machte und die ersten Home-PCs boomen ließ, findet seinen aktuellen Höhepunkt in der Ausbildung des Internets und seiner mobilen Endgeräte. Dies markiert gleichzeitig das Informationszeitalter, dessen zukünftige Zielrichtung die totale Vernetzung von jedem mit allem vorsieht. Aktuell verbindet das Internet Milliarden Menschen miteinander, und es soll bald rund 40 Mrd. vernetzte Geräte umfassen. Mit ungeheurer Dynamik öffnet die Digitalisierung ein neues Kapitel der menschlichen Entwicklung. Digitale Infrastrukturen, Produkte und Dienstleistungen verändern Gesellschaft und Wirtschaft. Dieser Übergang zu einer neuen Moderne wird gemeinhin als digitale Revolution bezeichnet – ein Prozess, der längst als nicht abgeschlossen zu betrachten ist. Zumal auch für das Internet der Dinge, wo Zukunftsforscher großes Potenzial in tragbarer Elektronik, Assistenzsystemen, Robotik und Künstlicher Intelligenz sehen. Damit verbunden sind moderne, systemisch vernetzte Produktionsverfahren zur Steigerung von Effizienz und Innovation. Weitere große Umbrüche zeichnen sich in der Mobilität ab, wo die digitale Vernetzung öffentlicher Verkehrsmittel sowie das autonome Fahren im Mittelpunkt stehen.

Wie die Geschichte lehrt, können technologische Entwicklungen ein starker Motor für gesellschaftliche Veränderungen sein – im Positiven wie im Negativen. Neue Technologien haben die Menschheit immer schon vor Herausforderungen gestellt, ihre Handlungsspielräume im Guten wie im Bösen erweitert, das Leben erleichtert wie auch vernichtet. Von der neolithischen bis zur industriellen Revolution war dies das Ergebnis von Fortschritt durch technischen Wandel, wie die Erfindung des Buchdrucks, welche die Wissenschaft und Weltbilder verändert hat. Der digitale Wandel bedeutet erneut Herausforderungen und Gefahren: Lückenlose Überwachung und Einschränkung der persönlichen Freiheit müssen ebenso beachtet werden

wie der Schutz vor Cyberkriminalität oder ethische Fragen rund um den Einsatz von Künstlicher Intelligenz. Dass eine neue Technik massenweise Arbeitskräfte ersetzt, hat bislang jeden technologischen Wandel begleitet. Aber andererseits entstehen auch laufend neue Tätigkeitsfelder. Viele Unternehmen werden sich verändern müssen, um nicht ein Opfer der digitalen Disruption zu werden (Verdrängung bestehender Produkte und Strukturen durch neue Technologien und Systeme). Im Lastenheft der Politik stehen demnach gesetzliche Regulierungen, die moderne Rahmenbedingungen setzen und für soziale Absicherungen sorgen, damit Arbeitnehmer die positiven Potenziale realisieren können.

Der stete Fortschritt in Mikroelektronik und Kommunikationstechnik erweckt die Vision einer umfassenden Vernetzung unzähliger Sensoren und Computer, eingebettet in die persönliche Umgebung. Winzigste Prozessoren, Speicherbausteine und Sensoren mit minimalen Produktionskosten können in viele alltägliche Gegenstände und Geräte implementiert werden. Nicht nur Mikroprozessoren wurden über Jahrzehnte immer kleiner, leistungsfähiger und preiswerter, sondern auch Funksensoren ermöglichen es, Systeme aus der Ferne schnell und billig zu überwachen und zu diagnostizieren. Sie können in großer Anzahl installiert und adaptiert werden, vermeiden teure Kabelverbindungen und lassen sich unsichtbar in Objekte integrieren, die vorher nicht netzwerkfähig waren. Zusammen mit Fähigkeiten zur Ortserkennung erlangen solche drahtlosen Devices eine nie da gewesene Qualität. Die allgegenwärtige Smartphone-Kultur, aber auch Funketiketten oder Chips in Ausweisen und Kreditkarten sind Vorboten einer neuen Ära des „Ubiquitous Computing" („Überallrechnens"). Bereits um 1990 orakelte der Informatiker und Kommunikationswissenschaftler Mark Weiser: „In the 21st century the

technology revolution will move into the everyday, the small and the invisible“ (https://de.wikipedia.org/wiki/Ubiquitous_computing). Als Reaktion wurde in Europa der Begriff „Ambient Intelligence“ geprägt, welcher die digitale Kommunikation alltäglicher Objekte zur Entlastung und Erleichterung des Lebens in den Vordergrund stellt. Dahin gehende Forschungen verfolgen das Ziel, Prozessoren, Sensoren und Funkmodule in einer Weise zu vernetzen, dass sie adaptiv auf die Bedürfnisse der Nutzer reagieren. Dabei soll sich die sichtbare Technik jedoch zurückziehen und nur noch auf unmerkliche Weise wirken. So wird die Anwesenheit verschiedener Personen von Systemen in der räumlichen Umgebung erkannt, um daraufhin individuell und unaufdringlich zu reagieren. Alltagsgegenstände sollen sich so von passiven zu aktiven Objekten verändern und adaptiv auf die Menschen einwirken. Neuartige Schnittstellen wie Sprach- oder Gestenerkennung leisten maßgebliche Unterstützung. Langfristig soll Ambient Intelligence alle Lebensbereiche umfassen. Ein damit ausgestattetes Smart Home der Zukunft erhöht Komfort, Sicherheit und trägt zur automatischen Energieeinsparung bei. Im Bürobereich wird die Arbeitseffizienz verbessert und durch lernfähige Assistenz gesteigert. Im Feld der intelligenten Transportmittel macht Ambient Intelligence den Verkehr sicherer und Ressourcen schonender, ebenso können Sensornetze umfassende Überwachungsaufgaben übernehmen. Freilich gilt es hier das Augenmaß zu bewahren, sonst ist der Normalbürger am Ende dem totalen Monitoring preisgegeben.

Die 5. Generation von Mobilfunkstandards (5G-Ausbau) ist von zentraler Bedeutung für die zukünftige Nutzung des Internets. Datenraten bis zu 10 Gbit/s sowie geringe Latenzzeiten erlauben eine hohe Dichte mobiler Endgeräte. Damit eröffnet sich eine Vielzahl neuer Geschäftsmodelle und Applikationen. Diese „hypervernetzte 5G-Ära“ soll

bereits in den 2020er Jahren über 40 Mrd. vernetzte Endgeräte ermöglichen. Dies schafft eine wesentliche Basis für das Internet der Dinge, welches Ambient Intelligence unterstützt: Geräte stellen demnach Zusatzinformationen im Internet zur Verfügung und kommunizieren miteinander. Kombiniert mit den Bedürfnissen der NutzerInnen können diese Devices automatische Unterstützung leisten. Die Industrie profitiert von besserer Instandhaltung der Maschinen, indem etwa Zustandsinformationen automatisch kommuniziert werden. Eine andere Kategorie betrifft tragbare Geräte am Körper (Wearables); sie können zum Beispiel Vitalparameter aufzeichnen (wie etwa Herzschlag oder Blutdruck) und die Daten an Ärztezentren funken und so die Überwachung des Gesundheitszustands des Patienten aus der Entfernung gestatten. Ebenso können erweiterte und virtuelle Realitäten ungeahnte Impulse vermitteln: Man blendet etwa via Brille visuelle Zusatzinformationen oder Objekte in Echtzeit ein und schafft damit eine interaktive virtuelle Umgebung. Dies bietet theoretisch beliebig viele Anwendungsmöglichkeiten, vom Tourismus über Bildung bis hin zu Handwerk und Bauindustrie. So kann in der Zukunft ein Projekt vor Baubeginn bereits virtuell besichtigt werden oder es werden Arbeitsanweisungen direkt am Objekt eingespielt.

Das Internet der Dinge bildet ebenso die Basis für das autonome Fahren. Eine besondere Challenge, die immer mehr in den Fokus der Fahrzeugindustrie rückt. Es ermöglicht neue Konzepte zur Vernetzung und Optimierung des öffentlichen und Individualverkehrs. Damit verbindet sich mehr Komfort bei gleichzeitig verringerter Umweltbelastung. Unfälle könnten vermieden und Parkplatzprobleme gelindert werden, Staus ließen sich umgehen, nicht zuletzt könnte auch die Zahl aktiver Fahrzeughalter drastisch sinken. Im Moment vorwiegend als Assistenzsystem realisiert, wird sich diese Technologie einst zum

vollautonomen Fahren weiterentwickeln. Der 5G-Ausbau spielt hier eine große Rolle, da sehr viele Fahrzeugdaten in Sekundenbruchteilen übertragen und verarbeitet werden müssen, was die Mobilfunkbetreiber vor gewaltige Herausforderungen stellt. Benötigt wird zentimetergenaues und stets aktualisiertes Kartenmaterial zusätzlich zur simultanen Erfassung der eigenen Position. Weiteres Datenmaterial betrifft etwa Streckenverlauf, Fahrbahnzustand, aktuelle Verkehrssituation, Wetterlage, Fahrmanöver anderer Autos und vieles mehr. Damit entsteht unmittelbar auch ein Kompetenzproblem: Wem gehören diese Daten eigentlich und was darf mit ihnen geschehen? Ein anderer Aspekt betrifft selbstredend Hacker- und Software-Security, welche hier naturgemäß einen sehr fortschrittlichen Standard erreichen muss. Ebenso stellen sich völlig neue juristische Fragen, wie etwa Rechtsansprüche beim Eintreten des Versicherungsfalls. Wäre der „Fahrer" dann von Sanktionen und Haftung gänzlich entbunden? Wer wäre stattdessen verantwortlich?

Mit dem Schlagwort „Industrie 4.0" verbindet man die industrielle Nutzung moderner Informations- und Produktionstechniken, die auf diese Weise verbunden werden sollen. Als Grundlage dafür dienen intelligente und digital vernetzte Systeme. Dies soll eine weitgehend selbstorganisierte Produktion ermöglichen. Menschen, Maschinen, Anlagen und Logistik sowie Produkte kooperieren und kommunizieren dabei direkt miteinander. Diese Vernetzung soll es gestatten, nicht nur einen Produktionsschritt, sondern eine ganze Wertschöpfungskette zu optimieren, wobei alle Phasen im Lebenszyklus des Produkts mit eingeschlossen sind – inklusive Recycling. Oft wird Industrie 4.0 auch als Zukunftsprojekt verstanden, das auf folgenden Prinzipien beruht: einerseits der Vernetzung von Maschinen mit Sensoren, andererseits der Funktionstransparenz, das heißt einer

Erweiterung durch Sensordaten, technische Assistenz und dezentrale Entscheidungen. Dazu sind allerdings viele Herausforderungen zu bewältigen. Grundziel ist dabei, die IT und die Produktionstechnologie miteinander zu verschmelzen. Im Zentrum steht ein sogenanntes cyberphysisches System, das heißt ein Verbund softwaretechnischer Komponenten mit mechatronischen Teilen, die über eine Infrastruktur (zum Beispiel das Internet) miteinander kommunizieren. Auf Basis von Standards und Normen verspricht man sich davon innovative Produkte und Leistungen. Dabei erhalten Daten als „neuer Rohstoff" eine besondere Bedeutung, womit Datensicherheit und Eigentum selbstredend eine Schlüsselrolle spielen.

Die bisherigen Fortschritte in der Computertechnologie sowie die explosiv zunehmende Informationsmenge durch Vernetzung schaffen neue Gesichtspunkte für weitere Fortschritte in der Künstlichen Intelligenz (KI). Längst ist KI ein Thema, das immer mehr in den Fokus von Firmen und Öffentlichkeit rückt. Die Einsatzgebiete sind vielfältig und betreffen u. a. Fertigung, Instandhaltung, Logistik, Vertrieb, Marketing und Controlling, aber auch Suchalgorithmen und vieles mehr. Schon heute sind Computer dazu in der Lage, zusätzlich zu strukturierten Daten auch unstrukturierte Informationen wie Sprache oder Fotos zu verarbeiten. Damit können Zusatzdaten generiert und verarbeitet werden, die bislang nicht zugänglich waren. Zudem gewinnt der Bereich Machine Learning zunehmend an Bedeutung. Computer lernen dabei an jedem einzelnen Fall, was die Fehlerwahrscheinlichkeit immer weiter reduziert und Handlungsabläufe optimiert. Abseits der industriellen Verwendung kann ein Roboter dann auch in wenigen Minuten eine Tumordiagnose stellen. Eines Tages sollen auch Neuroprothesen möglich werden, das heißt, neuronale Teile ersetzen motorische, sensorische oder kognitive Fähigkeiten, die

durch Verletzung oder Krankheit beeinträchtigt wurden. Abseits der klassischen Informatik könnten in der Zukunft innovative Konzepte, wie beispielsweise der Quantencomputer, zu völlig neuen Möglichkeiten und Sichtweisen beim Machine Learning führen. Einige Experten sind der Ansicht, dass Quantenprozessoren das maschinelle Lernen revolutionieren werden. Firmen wie Google, IBM oder Microsoft investieren heute schon in die Vision der Zusammenführung von KI mit Quantencomputing. Auch hier werden natürlich zunehmend ethische Fragen virulent, die bei einer disruptiven Technologie automatisch zu stellen sind. Bei der Einführung von KI in Unternehmen fühlen sich heute schon Mitarbeiter mit der Sorge belastet, dass durch den technischen Fortschritt Arbeitsplätze verloren gehen. Hier ist die Überzeugungsarbeit vom Management gefragt, dass KI in den meisten Fällen erst durch das Zusammenwirken mit dem Menschen ihr volles Potenzial entfalten kann.

Mit intelligenten Stromnetzen und Smart Grids wird zukünftigen Anforderung nach ökonomisch-ökologischer Optimierung Rechnung getragen. Diese erlauben eine direkte Kommunikation zwischen Verbraucher und Netzbetreiber, was für einen Ausgleich von Angebot und Nachfrage im Verteilernetz sorgt sowie den nachhaltigen Umstieg auf erneuerbare Energien fördert. Ein Beispiel ist etwa die Erzeugung von Elektrizität aus Windkraft oder Fotovoltaik, welche natürlichen Schwankungsbreiten unterliegt. Das intelligente Stromversorgungsnetz reagiert darauf adaptiv, indem es das Zusammenspiel von Verbraucher, Erzeuger und Speicher durch digitale Kommunikation so koordiniert, dass die bestmögliche Effizienz gewährleistet ist. Damit wird eine wichtige Voraussetzung für die Vision einer zukünftigen Smart City erfüllt, welche den Einsatz digitaler Technologien für die Nutzung nachhaltiger Quellen in den Vordergrund stellt. Als weitere Maßnahme zur

langfristigen Energie- und Ressourcenschonung wird der 3D-Drucktechnologie eine große Zukunft vorhergesagt. Dieses auch von Konzernen unterstützte Feld wird immer interessanter für komplexe Anwendungen und könnte einst den klassischen Fertigungsprozess ersetzen. Schon heute werden in Asien Häuser gebaut, welche direkt dem 3D-Drucker entstammen. Produktionssysteme werden dadurch dezentral gestellt, wodurch Fertigung und Verbrauch am selben Ort stattfinden. Diskutabel bleibt, welche genauen Auswirkungen dies bei größerer Verbreitung auf Verkauf, Distribution und Transport hätte. Die Steigerung der Wirtschaftlichkeit gilt andererseits gegenüber so manch konkurrierendem Herstellungsverfahren als erwiesen und wächst zudem mit steigender Komplexität der Bauteilgeometrie. Schlagworte wie „Bioprinter" oder „Digital Food" stellen in Aussicht, dass es auf diesem Wege eines Tages zu markanten Innovationen im Gesundheitswesen wie auch in der Nahrungsmittelproduktion kommen mag. Gut vorstellbar auch, dass Online-Shops die Technik nutzen werden, indem der Kunde keine physische Ware mehr erwirbt, sondern einen digitalen Konstruktionsplan downloadet und damit den privaten 3D-Drucker füttert. In jedem Fall geht es dabei um äußerst komplexes Datenmaterial, das es entsprechend zu schützen gilt.

Zukunftsware: Datenschutz und Prozessorleistung

Mit Hinblick auf die ubiquitäre Vernetzungstendenz sowie die genannten Visionen (die nicht der Fantasie des Autors entstammen, sondern bereits breit diskutiert werden) muss unmittelbar einleuchten, dass die digitale Sicherheit in der zukünftigen IT noch viel umfassender gedacht werden muss. Dies betrifft nicht nur das Internet der Kommunikation, sondern ebenso das Internet der Dinge, von dessen allmählicher Omnipräsenz viele Experten überzeugt sind. Schon heute prasseln Hacker- und Lauschangriffe

global gesehen zu Millionen im Sekundentakt herein und verursachen einen gewaltigen wirtschaftlichen Schaden. In einer immer stärker vernetzten Welt kann sich dieses Problem nur potenzieren. Man mag sich gar nicht vorstellen, was das erst für einen künftigen vollautonomen Fahrbetrieb bedeuten kann. Ein gut gezielter Cyberangriff auf das zigtausende Autos steuernde Verwaltungssystem könnte die absolute Katastrophe bedeuten. Selbstredend bedürfen kritische Infrastrukturen, speziell auch im Zusammenhang mit modernen Industriekonzepten, besonderer Schutzmaßnahmen. Ein Grundsatzproblem besteht darin, dass die generierte Datenmenge (die jährlich exponentiell wächst) in der Zukunftswelt exorbitante Ausmaße erreichen wird. Damit steigt nicht nur die Gefahr unautorisierter und krimineller Angriffe ebenso rapide an, sondern es erreicht auch die Menge personenbezogener Daten eine schwindelerregende Größenordnung. Die bereits heute im Internet erzeugte Informationsmenge (um 2020 ca. 200 Exabyte pro Monat) ist viel zu groß und komplex, um konventionell bearbeitet zu werden. Deshalb werden oft große Datenmengen zentral erfasst und miteinander verschränkt (Big Data). Dies kann für viele sinnvolle Zwecke genutzt werden, etwa für Wirtschaft, Finanz und Medizin. Auf der anderen Seite macht die Ansammlung immer größerer persönlicher Datenbestände die Sicherung von Privatsphäre und Datensouveränität zunehmend zur Herausforderung. In einer so hoch vernetzten Welt muss „echte Privacy" deshalb als eine der wichtigsten Forderungen der Gesellschaft gelten – sonst droht am Ende der totale Überwachungsstaat (der sich mancherorts schon abzeichnet).

Wie aktuelle Beispiele zeigen, ist die Weitergabe persönlicher Daten ein florierendes Geschäft, was zur Ignoranz gegenüber gesetzlichen Auflagen motivieren kann. Hier ist generell ein langfristig wirkender Schutz gefragt, der jedoch nicht ausschließlich in Regulierungen bestehen

kann, sondern auch technisch gewährleistet sein muss. Weil Daten generell als das Gold der Zukunft anzusehen sind und deren Analyse und Weitergabe Konzernen viel Geld einbringt, werden logischerweise irgendwann konträre Geschäftsmodelle entstehen. Somit müssen umfassender Cyberschutz und Sicherung der Privatsphäre in der Zukunft als wesentlicher Business-Faktor ernst genommen werden. Ganz wichtig auch: zentrale Datenspeicher, digitale Archive und Datenbankensysteme, in denen jetzt schon sehr viel Material abgelegt wird. Was heute als sicher gilt, muss diesen Anspruch auch noch in 20, 50 oder 100 Jahren erfüllen können. Bei Banken und großen Unternehmen herrscht überwiegend die Meinung vor, dass zwar die heutige Sicherheitstechnik als ausreichend zu betrachten ist, die Vorstellung jedoch, dass am Tag X einmal die Technik nicht mehr standhält, ein gewisses Unbehagen erzeugt. Dazu gilt es klar festzuhalten, dass die aktuelle digitale Sicherheitstechnik ausschließlich auf der Annahme beruht, dass die Rechnerleistung des Angreifers nicht ausreicht, um die benutzte Codierung beziehungsweise die bestehende Firewall zu knacken. Für diese Annahme gibt es jedoch keinen direkten wissenschaftlichen Beweis. Ein Schwachpunkt der heute üblichen Public-Key-Algorithmen (wie RSA oder elliptische Kurven), die etwa für digitale Signaturen oder Schlüsselaustausch verwendet werden, besteht darin, dass sie auf der Schwierigkeit mathematischer Probleme beruhen. Durchbrüche in der Forschung sowie die stete Zunahme der Rechnerleistung können jedoch dazu führen, diese Verfahren zu brechen. Die Grundfrage ist daher: Wie kann man einen langfristigen und nachhaltigen Cyberschutz garantieren, der auch zukünftigen Computerentwicklungen von potenziell sehr großer Leistung standhält?

Es muss daher im Sinne der Gesellschaft sein (nicht nur von Regierungen und Eliten), dass die Wissenschaft

neue Konzepte zum Thema digitale Sicherheit bereitstellt. Die Quantenkommunikation bildet hierzu die ideale Voraussetzung. Dabei geht es insbesondere um den innovativen Ansatz der inhärenten Sicherheit, das heißt um ein System, dessen Wirksamkeit nicht eine Variable der Computerleistung des Angreifers ist, sondern einen physikalischen Mechanismus enthält, welcher die Immunität garantiert. Auf Basis der bisherigen Informationstechnik ist ein physikalisch garantierbares Verfahren jedenfalls nicht möglich. Die Quantenkommunikation bietet dagegen einen Weg, um eine ganz wesentliche potenzielle Sicherheitslücke automatisch zu schließen: Die völlig abhörsichere Datenverbindung zwischen zwei entfernten Punkten. Eine solche Hochsicherheitsverbindung kann entweder direkt von Punkt zu Punkt erfolgen oder durch vertrauenswürdige Knotenpunkte verteilt hergestellt werden. Zusammen mit Methoden der klassischen Sicherheitstechnik vermag sie auch einen bis dato unerreichten Schutz gegen Hackerangriffe sowie den unautorisierten Zugriff auf Datenbanken zu gewährleisten. Diese Technik liegt dem Grundprinzip nach schon fix und fertig in den Schubladen, ist der Marktreife schon sehr nah und harrt nur mehr der nötigen großen Investitionen. Sie ist bereits in asiatischen Testnetzwerken im bis dato größten Maßstab implementiert und könnte bereits in den 2020er Jahren überregionale Verbreitung finden. Sie kann eine wichtige Rolle in lokalen Strukturen wie auch in Backbone-Netzwerken spielen. Da hiermit auch viele kommerzielle Anwendungen verbunden sind, wird letztlich ein globales Hochsicherheitsnetz vorstellbar, das permanent weiterentwickelt wird und so den zukünftigen Sicherheitsanforderungen bestens gewachsen wäre. Schon heute bieten Firmen Sicherheitslösungen auf Basis der Quantenschlüsselverteilung (englisch, QKD) an, welche die traditionelle Kryptografie verbessert. Dabei handelt es sich um

Verteilungs-Appliances kombiniert mit Linkverschlüsslern, die durch optische Fasern miteinander verbunden sind. Zu den typischen Anwendungen zählen sichere LAN-Erweiterungen, Unternehmensumgebungen oder Datencenter-Links. Verbindungsbandbreiten bis zu 10 Gbit/s sowie Reichweiten um die 100 km erlauben den Einsatz in metropolischen Quantennetzwerken. Gut vorstellbar, dass in einiger Zeit viele User ein Quantenmodul zur abhörsicheren Kommunikation in ihrem Computer nutzen.

Auf der anderen Seite impliziert die Projektion in die digitale Zukunft rasant steigende Computerleistungen. Dies nicht nur als Folge der angesprochenen exponentiellen Datenzunahme und der dafür benötigten wachsenden Prozessorleistung, sondern auch in Hinblick auf zukünftige Logistik- und Optimierungsaufgaben. Wie man zeigen kann, gibt es zahlreiche Problemstellungen, die von klassischen Computern entweder gar nicht oder jedenfalls in keinem angemessenen Zeitrahmen gelöst werden können. Ein bekanntes Beispiel ist das Problem des Handlungsreisenden: Die Berechnung des optimalen Routenplans, um eine Reisestrecke möglichst kurz zu halten, stellt traditionelle Rechner vor erhebliche Probleme; gilt es doch, aus hunderten Billionen möglicher Varianten (die schon bei weniger als 20 Städten auftreten) die optimale auszuwählen. Ein damit verwandtes Zukunftsproblem betrifft zum Beispiel die Verkehrsflussoptimierung beim autonomen Fahren. Das Erfassen von extrem vielen Daten mithilfe von Sensoren ist zwar technisch kein Problem, sehr wohl aber die anschließende simultane Berechnung der optimalen Fahrmanöver für alle Fahrzeuge. Auf Basis der herkömmlichen EDV benötigen klassische Computer dafür viel zu lange. Wie erste Simulationen von Quantenrechnern bereits nahelegen, können derartige und verwandte Optimierungsaufgaben mit diesem neuen Konzept wesentlich rascher gelöst werden.

Davon abgesehen existieren zahlreiche weitere logistische Herausforderungen, vor allem aber auch wissenschaftliche Problemstellungen, die mit klassischen Computern nicht sinnvoll oder gar nicht zu bewältigen sind. Auch mit Hinblick auf KI und Machine Learning werden neue Computerkonzepte immer wichtiger. Nicht zuletzt auch deshalb, weil die herkömmliche „Silicium-Revolution" in wenigen Jahren ausgereizt erscheint. Das vielversprechendste Konzept ist hier der Quantencomputer, der wahrscheinlich die einzige Möglichkeit darstellt, die Computerleistung noch wesentlich zu verbessern oder sogar in eine neue Dimension zu führen. So können Quantencomputer zum Beispiel im Bereich der KI die dort auftretenden harten kombinatorischen Optimierungsprobleme viel effizienter lösen. Auch vermögen sie Strukturen aus verrauschten Daten viel schneller zu erkennen und liefern entsprechend neue Gesichtspunkte für Machine Learning. Heute schon zeigt sich, dass gleichsam jede digitale Quantensimulation eines komplexen Problems auf einem Quantensimulator durchgeführt werden kann. Das große Marktpotenzial beweisen IT-Riesen wie Google, Microsoft oder IBM, die bereits Milliarden in diese Technologie investiert haben. VW beispielsweise hat eine Kooperation mit Google geschlossen, um auf Basis von Quantenprozessoren Kalkulationen für Akkus und autonome Fahrzeuge erstellen zu lassen. Quantentechnologien werden daher auch von dieser Seite eine wichtige zukünftige Rolle spielen. Unabhängig vom enormen wissenschaftlichen Wert steht demnach die Entwicklung von technologisch nutzbaren Quantencomputern, respektive einer damit verbundenen Netzwerktechnik im Fokus der Forschung. Während ein QKD-Internet bereits ein fassbares Ziel mit klaren Konturen darstellt (Regierungen und Unternehmen haben schon ihr Interesse artikuliert), muss ein Netzwerk leistungsfähiger Quantenprozessoren

hingegen noch als reine Zukunftsvision gesehen werden. Dabei ist noch nicht einmal klar, welche Funktionalitäten damit eigentlich genau verbunden sein können. Ebenso lässt sich noch nicht abschätzen, in welchem Umfang eine Realisierung physikalisch/technologisch überhaupt möglich ist. Die Gesichtspunkte eines Quanteninternets sind vielfältig und für so manchen Forscher überwiegend noch ein Graubereich. Dennoch geben sich einige Experten heute schon der faszinierenden Spekulation hin, dass auf Basis von Quantentechnologien eines Tages ein unsagbar leistungsfähiges Hypernet entstehen wird, welches in den Parametern Prozessorgeschwindigkeit, Datenrate und Sicherheit völlig neue Maßstäbe setzt. Dabei gilt es explizit festzuhalten, dass der Geschwindigkeitsvorteil eines Quanteninternets nicht etwa auf einen überlichtschnellen Transfer von direkt nutzbarer Information zurückzuführen ist, sondern auf die Tatsache, dass Quantenbits viel mehr Information speichern und übertragen können als herkömmliche Bits. Zwar kann auch ein Quanteninternet nicht schneller als das Licht kommunizieren, sehr wohl aber überlichtschnell koordinieren und synchronisieren, was es bezüglich dieser Eigenschaft einzigartig macht (auf derartige und ähnliche Aspekte wird später noch ausführlich eingegangen). Schließlich würde ein Quanteninternet nicht nur vom Speed-up seiner Quantenprozessoren profitieren, sondern es könnte bei entsprechender Konfiguration auch dazu beitragen, Quantencomputer skalierbar (das heißt um beliebige Qubits erweiterbar) zu machen. Mit Hinblick auf die Anforderungen des Internets der zukünftigen Welt gilt es festzuhalten: Wenn die angedachten Visionen der klassischen IT (die sich ja nicht sofort, sondern in einer schleichenden Revolution vollziehen würden) langfristig sinnstiftend sein sollen, so ist jedenfalls eine „quantendigitale" Begleitung dieser Entwicklung nicht wegzudenken. Nicht zuletzt auch deshalb,

weil Quantencomputer eine theoretische Gefahr für die traditionelle Sicherheitstechnik darstellen und daher auf längere Sicht besondere Verfahren notwendig machen. Ironischerweise beruhen diese Maßnahmen wiederum erheblich auf der Quantentheorie.

1.2 Revolutionäre Quantenphysik

Es war bereits Thema der Alpbacher Technologiegespräche Schon seit vielen Jahrzehnten hat die Quantentechnologie eine revolutionäre Auswirkung auf die Menschheit. Errungenschaften wie Laser, bildgebende Verfahren oder Halbleitertechnologie haben ihre Wurzeln in grundlegenden Gesetzen der Quantenmechanik. Insbesondere resultiert daraus die moderne Computerentwicklung, ohne die ein weltumspannendes Netzwerk wie das heutige Internet gar nicht erst möglich wäre. Nicht so bekannt ist in der Öffentlichkeit der Umstand, dass bereits jedes Smartphone, jeder DVD-Player, aber auch jede Badezimmer-LED als Kind der Quantentheorie anzusehen ist. Die wirtschaftlich hohe Bedeutung der Quantentechnik lässt sich daran erkennen, dass heute schon gut ein Drittel des Bruttosozialprodukts eines Industriestaats durch Produkte erwirtschaftet wird, die auf der Quantentheorie beruhen. Forschungsergebnisse in den letzten Jahren und Jahrzehnten geben Anlass zur berechtigten Hoffnung, dass die Quantentechnik noch viele weitere Facetten bereithalten könnte. Quantentechnologien können in unterschiedlichen Bereichen Anwendungen finden und ermöglichen auf vielen Gebieten Verbesserungen von bestehenden technischen Lösungen. Ebenso eröffnen sie fundamental neue Möglichkeiten und Gesichtspunkte. Abseits der Quantenkommunikation und der Quanteninformatik ist etwa die Quantensensorik von besonderem

Interesse. Obwohl die Quantenphysik eine Wissenschaft der Unbestimmtheiten und Wahrscheinlichkeiten ist, kann sie zu einer noch nie da gewesenen Präzision beitragen: Heutzutage werden klassische Sensoren immer kleiner und präziser gebaut. Allerdings ist bereits jetzt abzusehen, dass damit in Zukunft keine entscheidende Verbesserung in den Parametern Empfindlichkeit und Spezifizität zu erreichen sein wird. Originäre Quantenphänomene wie Superposition oder Verschränkung können jedoch dazu genutzt werden, physikalische Größen wie Druck, Temperatur, Zeit, Lage, Beschleunigung oder aber elektrische, magnetische sowie Gravitationsfelder wesentlich präziser zu erfassen. Dies kann zu vielfältigsten Anwendungen führen wie auch zur Untersuchung fundamentaler wissenschaftlicher Fragestellungen.

Um zu verstehen, wie nahe diese „zweite Quantenrevolution" uns heute bevorsteht, drehen wir das Rad der Zeit zurück, um zu sehen, worin die erste Quantenrevolution bestand: Am Ende des 19. Jahrhunderts wurde manchem Studenten (etwa dem jungen Max Planck!) von einem Physikstudium abgeraten, da man der Meinung war, dass es nichts Wesentliches mehr zu entdecken gäbe. Allerdings zogen, wie es Lord Kelvin (William Thomson) ausdrückte, alsbald „dunkle Wolken" am Physikhimmel auf. Eine solche war zum Beispiel die Strahlung, welche von glühenden Körpern emittiert wird, etwa der Sonne, die uns gleißend weiß erscheint, wenn sie im Zenit steht. Doch weiß kaum jemand, dass sie in erster Linie grün leuchtet. Der physiologische Grund liegt darin, dass die Sonne (so wie jeder Stern) Strahlung mit vielen verschiedenen Wellenlängen abgibt und die menschliche Wahrnehmung den sichtbaren Anteil dieser Mixtur als „weißes" Licht interpretiert. Physikalisch steht hinter dem realen „grünen" Strahlungsmaximum das wiensche Verschiebungsgesetz, welches besagt, dass mit zunehmender

Oberflächentemperatur eines Sterns die Wellenlänge der maximal emittierten Strahlung immer kleiner wird. Ein besonders heißer Stern leuchtet demnach in erster Linie blau, unsere mittelheiße Sonne danach grün, ein kühler Roter Riese wie Beteigeuze im Sternbild Orion vorwiegend im roten Spektrum. Will man allerdings nicht nur das Maximum, sondern die gesamte Energieverteilung eines glühenden Körpers erklären, stößt man mit der klassischen Physik an eine Grenze. Es ist im Rahmen der klassischen Physik nicht möglich, eine Formel zu finden, die mit den ermittelten Messdaten übereinstimmt. Insbesondere käme es nach den Vorhersagen der klassischen Physik zu unendlich großen Termen („UV-Katastrophe"), was definitiv nichts mit der Realität zu tun hat. Erst der deutsche Theoretiker Max Planck fand das sogenannte plancksche Strahlungsgesetz, indem er eine der klassischen Physik grundsätzlich fremde Annahme machte: Danach tauscht das Licht seine Energie nicht in beliebig feiner Einteilung aus, sondern in Klumpen oder Portionen, welche er „Quanten" nannte. Allerdings misstraute Planck seinem eigenen Quantenmodell und hoffte noch lange, dass seine Annahme zugunsten der klassischen Physik wieder verworfen werden könnte – eine Hoffnung, die nie erfüllt wurde. Die Quanten erwiesen sich als fundamental. Diese Erkenntnis entstammte dem damals noch völlig unbekannten Albert Einstein, der durch Planck inspiriert 1905 seine nobelpreisgekrönte Lichtquanten-(Photonen-)Hypothese veröffentlichte. Diese Lichtteilchen werden auch in der zukünftigen Quantentechnik eine ganz entscheidende Rolle spielen. Im Unterschied zu Planck, der zunächst nur den Energieaustausch zwischen Atomen als quantisiert annahm, erweiterte Einstein diese Vorstellung auf das Licht selbst, welches demnach aus diskreten Energiequanten besteht. Auf dieser Basis erfuhr dann erstmals der fotoelektrische