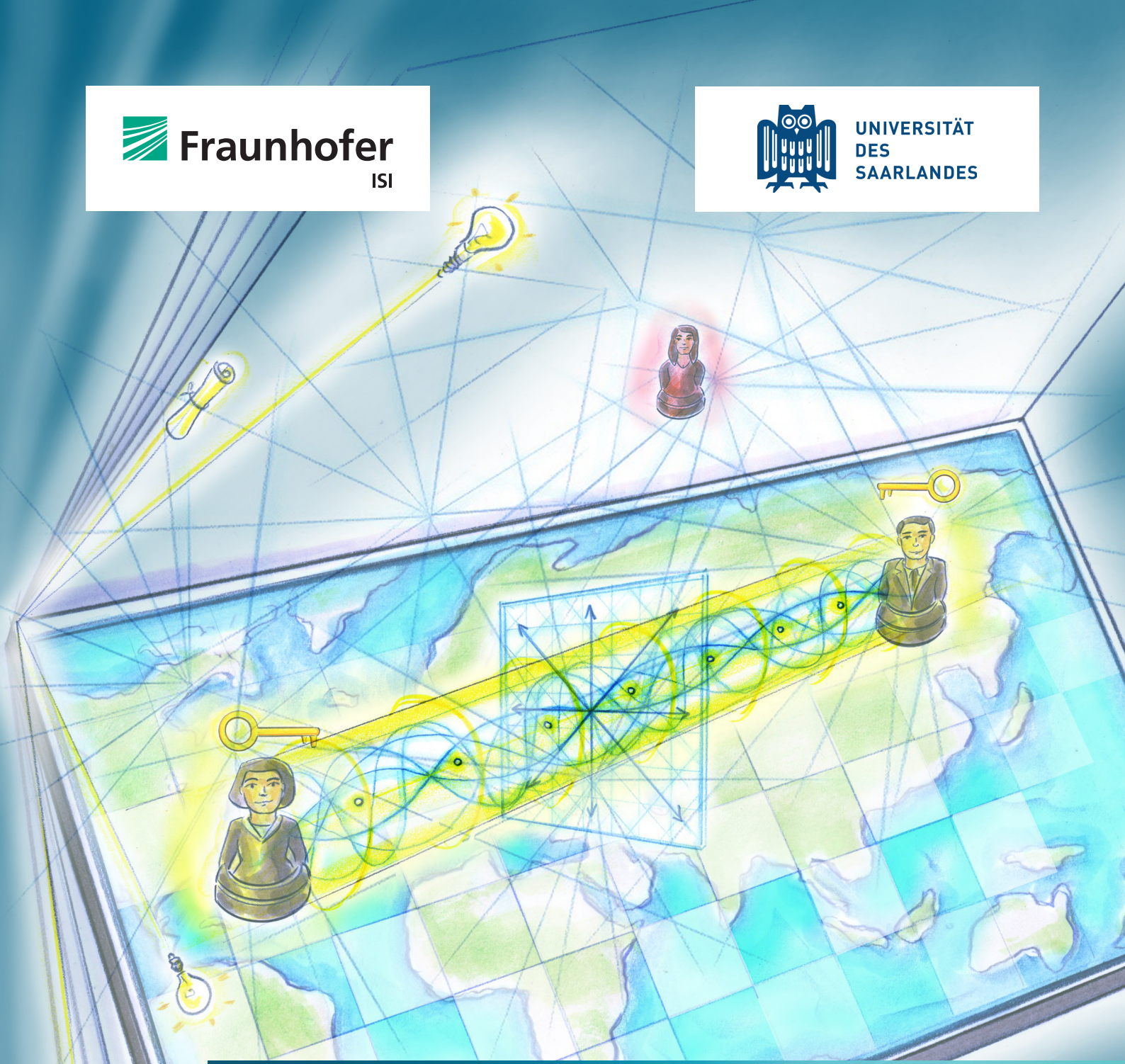
Fraunhofer ISI

UNIVERSITÄT DES SAARLANDES



Juli 2024

Monitoring-Bericht 1 Quantenkommunikation

Impressum

Monitoring-Bericht 1 – Quantenkommunikation

Projektkoordination

Fraunhofer-Institut für System- und Innovationsforschung ISI

Breslauer Straße 48, 76139 Karlsruhe, Deutschland
Dr. Thomas Schmaltz, thomas.schmaltz@isi.fraunhofer.de

Universität des Saarlandes

Fachrichtung Physik, Campus E2 6, 66123 Saarbrücken
Prof. Christoph Becher, christoph.becher@physik.uni-saarland.de

Verantwortlich für den Inhalt

Chie Endo, Fraunhofer ISI, chie.endo@isi.fraunhofer.de
Christoph Becher, Universität des Saarlandes, christoph.becher@physik.uni-saarland.de
Jessica Schmidt, Universität des Saarlandes, jessica.schmidt@uni-saarland.de
Linus Krieg, Physikalisch-Technische Bundesanstalt, linus.krieg@ptb.de
Lukas Weymann, Fraunhofer ISI, lukas.weymann@isi.fraunhofer.de
Saeideh Shirinzadeh, Fraunhofer ISI, saeideh.shirinzadeh@isi.fraunhofer.de
Thomas Schmaltz, Fraunhofer ISI, thomas.schmaltz@isi.fraunhofer.de

Zusammengestellt im Auftrag von

Schirmprojekt Quantenkommunikation Deutschland – SQuaD, gefördert durch das Bundesministerium für Bildung und Forschung BMBF

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Bildnachweis

Deckblatt: Heyko Stöber, Hohenstein

Veröffentlicht

Juli 2024

DOI

doi:10.24406/publica-3284

Inhalt

Zusammenfassung

Sichere Kommunikation ist ein Grundpfeiler freier Gesellschaften und essenziell für den verlässlichen Betrieb kritischer Infrastrukturen. Um diese zu gewährleisten, sind kryptografische Verfahren von zentraler Bedeutung. Durch die Entwicklungen im Quantencomputing können heute verwendete Verschlüsselungsverfahren potenziell in absehbarer Zeit entschlüsselt werden, weshalb dringend "quantensichere" Wege zur Verschlüsselung der Kommunikation benötigt werden. Die aufkommende Technologie der Quantenschlüsselverteilung (QKD), die physikalisch sichere Kommunikation auf Basis quantenmechanischer Prinzipien ermöglicht sowie Technologien die Quantenzustände über längere Distanzen transportieren bzw. austauschen können, werden unter dem Begriff Quantenkommunikation zusammengefasst. Dieser Bericht gibt einen Überblick über die Technologien und Technologiegenerationen der Quantenkommunikation, analysiert Entwicklungen im Bereich der Forschung, Industrialisierung, Testinfrastruktur und des Marktes und diskutiert die Relevanz von technologischer Souveränität in der Quantenkommunikation.

Technologieüberblick nach Generationen der Quantenkommunikation

Die Quantenkommunikation kann systematisch nach Entwicklungsstufen der Technologien in drei Generationen gegliedert werden:

Erste Generation – Quantenschlüsselverteilung nach dem Prepare & Measure-Prinzip:

Qubits werden in verschiedenen zufällig ausgewählten Quantenzuständen präpariert und über Kommunikationskanäle an den Empfänger gesendet werden. Durch geeignete Präparation und Messung der Quantenzustände, wie z. B. der Polarisation der Photonen, und den Austausch gewisser Informationen darüber kann ein sicherer Schlüssel erzeugt werden, der anschließend zur Codierung der eigentlichen Nachricht genutzt wird. Jeder Versuch des Abhörens oder Kopierens durch einen Angreifer führt zu Zustandsänderungen, die von Sender und Empfänger bemerkt werden. Prepare & Measure-QKD stellt bereits heute eine marktreife Technologie für sichere Kommunikation dar. Ein breiter Einsatz wird aber noch durch hohe Kosten sowie ausstehende Sicherheitsbeweise, Zertifizierungen und Zulassungen gehemmt.

Zweite Generation – Quantenschlüsselverteilung mit photonischen Verschränkungsquellen:

Quantenverschränkung, eine spezielle Verknüpfung zwischen quantenmechanischen Teilchen, kann genutzt werden, um sichere Kommunikation zu ermöglichen. Der Ausgangspunkt ist eine Quelle verschränkter Photonen, die zwischen zwei Kommunikationspartnern aufgeteilt werden. Die beiden Kommunikationspartner messen ihr Photon jeweils und können durch den Austausch gewisser Informationen über die Messung ein gemeinsames Schlüsselbit erzeugen oder die Verschränkung der Photonen nachweisen. Ein Abhören bricht unvermeidlich die Verschränkung und wird dadurch erkennbar. Verschränkungsbasierte QKD ist noch nicht so ausgereift wie Prepare & Measure-QKD und erreicht aktuell geringere Schlüsselraten, könnte aber Vorteile für komplexe Kommunikationsnetzwerke bieten.

Dritte Generation – Quantenrepeater mit Verschränkungsverteilung:

Die dritte Generation beschreibt die Entwicklung von Quantenrepeatern, die eine Verschränkungsverteilung über weite Distanzen ermöglichen. Ausgangspunkt ist dabei die begrenzte Reichweite von QKD. Um diese zu erhöhen, wird an Quantenrepeatern geforscht, die Übertragungsstrecken in kürzere Abschnitte aufteilen und durch Verschränkungsaustausch ohne Messung oder Kopie von Quantenzuständen die Reichweite von Quantenverschränkung vergrößern. Die durch Quantenrepeater erzeugten verschränkten Zustände können für verschränkungsbasierte QKD der zweiten Generation und Quantenteleportation über große Distanzen genutzt werden. Letzteres ermöglicht

verteiltes Quantenrechnen und könnte potenziell die Rechenleistung von Quantencomputern steigern. Quantenrepeater tragen damit wesentlich zur Entwicklung zukünftiger Quantenkommunikationsnetze bei und haben hohe gesellschaftliche Bedeutung für IT-Sicherheit und den Schutz kritischer Infrastrukturen. Quantenrepeater sind aktuell allerdings noch Gegenstand der Forschung und noch nicht technologisch ausgereift genug, um eine kommerzielle Anwendung zu ermöglichen.

Ergebnisse des quantitativen Monitorings

Die Zahl der *Veröffentlichungen* zum Thema Quantenkommunikation ist in den letzten 20 Jahren deutlich und kontinuierlich gestiegen, auf fast 2000 im Jahr 2022. Die meisten Publikationen kommen aus China (Publikationsanteil von 33 %), dicht gefolgt von der EU (29 %, Deutschland 7 %) und den USA (16 %). Eine Zitationsanalyse zeigt, dass Publikationen aus der EU durchschnittlich 23-mal zitiert werden, häufiger als Publikationen aus den anderen analysierten Regionen/Ländern. Dies lässt auf eine hohe Relevanz der europäischen Publikationen schließen.

Auch die *Patentierungsaktivitäten* im Bereich der Quantenkommunikation haben in den letzten Jahren stark zugenommen und lagen im Jahr 2021 bei über 200 transnationalen Patentanmeldungen. Die meisten Patentanmeldungen der letzten Jahre kamen dabei aus der EU (Patentanteil von 35 %), gefolgt von den USA (29 %) und China (15 %). Die höchsten Patentaktivitäten verzeichnen Technologieunternehmen, große Telekommunikationsanbieter und Forschungseinrichtungen/Organisationen. Auch wenn die meisten Patentanmeldungen aus der Industrie kommen (ca. 70 %), wird die Technologie weiterhin stark von Forschungsorganisationen vorangetrieben (ca. 30 %).

Die *Analyse von zahlreichen Marktstudien* zum Thema Quantenkommunikation, -kryptografie und QKD deutet auf einen in den nächsten Jahren stark wachsenden Markt hin. Der Median der analysierten Marktschätzungen und -prognosen ergibt einen globalen Umsatz in Höhe von 1,7 Milliarden Euro im Jahr 2023, der bis 2030 auf 5,8 Milliarden ansteigen könnte. Die meisten Studien prognostizieren jährliche Wachstumsraten zwischen 15 und 25 Prozent.

In einer *Analyse der Förderprogramme* in Deutschland und Europa wurden 62 vom BMBF geförderte Projekte im Bereich der Quantenkommunikation identifiziert sowie 57 Projekte bzw. 21 Projekte, die durch die EU-Rahmenprogramme Horizon 2020 (H2020) bzw. Horizon Europe (HE) gefördert werden. Die meisten Projekte beschäftigten sich dabei mit QKD (insb. BMBF und HE), Lichtquellen (BMBF, H2020 und HE) sowie Quantennetzwerken (insb. H2020).

Eine *Analyse der internationalen F&I Strategien* zeigt, dass neben Deutschland und der EU, auch weitere Länder die strategische Wichtigkeit der QCom erkannt und F&E-Programme aufgesetzt haben. Zahlreiche Länder haben hierzu Strategien entwickelt und investieren signifikant in die Quantenkommunikation. Insbesondere China, die USA, das Vereinigte Königreich, Japan und Südkorea sind hier zu nennen.

Um einen *Überblick über die bestehende Testinfrastruktur* zu geben, wird in diesem Bericht eine Karte mit den sogenannten Testbeds für die Quantenkommunikation in Deutschland gezeigt und diese jeweils kurz beschrieben. Der Aufbau von (Test-)Infrastruktur ist von zentraler Bedeutung auf dem Weg zur Industrialisierung und breiteren Anwendung der Quantenkommunikation.

Überlegungen zu Technologiesouveränität

Die Diskussion über die Notwendigkeit der Sicherung der technologischen Souveränität für kritische Technologien in Deutschland und Europa hat in den letzten Jahren an Dynamik gewonnen. Dies gilt insbesondere auch für sichere Kommunikation, da sie nationale Sicherheit, den Schutz von Geheimnissen und Privatsphäre sowie die Integrität von wirtschaftlichen und politischen Prozessen gewährleistet und somit ein fundamentaler Bestandteil der kritischen Infrastruktur einer Nation ist. Im Rahmen dieser Studie wurde die Einschätzung von deutschen QCom-Expert:innen zu Aspekten

von technologischer Souveränität analysiert. Hierbei wurde häufig auch ein über die technologische Souveränität hinausgehendes Ziel betont, die wirtschaftlichen Zukunftspotenziale von QCom-Technologien zu heben.

Bedarfe bestehen in Deutschland und Europa QCom-Technologien zumindest auf Systemebene zu verstehen, zu entwickeln und herstellen zu können. Dabei wird der Import benötigter Komponenten ohne einseitige Abhängigkeiten als unproblematisch angesehen, unter der Voraussetzung, dass importierte Komponenten und Systeme auf ihre Sicherheit geprüft werden können.

Herausforderungen für die Erreichung einer technologischen Souveränität bestehen in den hohen Investitionskosten für Infrastruktur und QCom-Technologien sowie der notwendigen Weiterentwicklung der Systeme und Technologien. Auch die breitere Marktimplementierung steht vor Herausforderungen, insbesondere in Hinblick auf das mangelnde Bewusstsein für Sicherheitsrisiken in der Kommunikation, der Wahrnehmung von QCom bei potenziellen Nutzern, der Entwicklung von Märkten und Geschäftsmodellen im privaten Sektor, der starken Regulierung einiger Märkte (insb. im öffentlichen Sektor) sowie bei Sicherheitsbeweisen.

Maßnahmen zur Erreichung von technologischer Souveränität könnten entsprechend die Fortführung der öffentlichen Finanzierung, Kaufanreize für Endnutzer in der Industrie, Investitionen in europäische Infrastruktur sowie Öffentlichkeitsarbeit und Bildungsprogramme für Interessenvertreter aus den relevanten Fachbereichen sein. Weitere Maßnahmen stellen die Förderung des Technologietransfers in die Industrie, Zusammenarbeit entlang der Wertschöpfungskette, Beseitigung von Hürden für Zulassungen, Unterstützung von Normungs- und Zertifizierungsaktivitäten, eine gute Zusammenarbeit der Behörden der europäischen Mitgliedsstaaten und eine Verschlankung und Abbau der Bürokratie dar.

1 Einleitung

Die Informationstechnik und Telekommunikation wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als einer von zehn kritischen Infrastrukturbereichen definiert. Seit Jahrhunderten werden kryptografische Verfahren entwickelt und eingesetzt, um eine sichere Kommunikation zu gewährleisten, denn diese schützt nicht nur die Privatsphäre des kommunizierenden Individuums, sondern ist auch erforderlich, um die Handlungsfähigkeit eines Staates zu schützen. Mit dem Aufkommen von Quantencomputern wächst die Bedrohung für herkömmliche Verschlüsselungsmethoden. Noch bevor die Quantenüberlegenheit erreicht ist, ist die Geheimhaltung durch die Strategie "jetzt sammeln – später entschlüsseln" gefährdet. Dies macht es notwendig, jetzt zu handeln. Quantenkommunikationstechnologien (QCom) sind ein möglicher Ansatz, um dieser Bedrohung zu begegnen und eine potenziell perfekte Sicherheit entlang des Übertragungsweges zu erreichen. Die Erlangung und Sicherung der Technologiehoheit in der Quantenkommunikation ist daher als ein Ziel der Bundesregierung formuliert worden.

Dieser Monitoring-Bericht soll einen Überblick über den aktuellen Stand der Quantenkommunikationsforschung, -technologie und -wirtschaft in Europa geben und Aspekte der Technologiesouveränität diskutieren. Ein Update dieses Berichts ist geplant. Um ein detailliertes Bild zu erhalten, wurde eine Kombination von Methoden (Abschnitt 2) angewandt.

Die Hintergründe für den Bedarf nach Quantenkommunikation (Abschnitt 3) und der Stand der Forschung im Bereich der Quantenkommunikation wird im Rahmen einer qualitativen Analyse erörtert (Abschnitt 4). Es werden verschiedene Software- und Hardwareansätze für die Quantenkommunikation vorgestellt und die mögliche Entwicklung von Technologiegenerationen aufgezeigt.

Die quantitative Analyse (Abschnitt 5) umfasst eine Patent- und Publikationsanalyse, die die Akteure aus Wissenschaft und Industrie identifiziert und die globale Dynamik skizziert. Die Akteurs-Analyse wird durch eine Metamarktanalyse ergänzt. Neben der Analyse der am häufigsten genannten Akteure wurden auch potenzielle Marktgrößen für QCom-Technologien eruiert. Die Förderschwerpunkte von Forschungsprojekten in Deutschland und Europa wurden identifiziert und geben Einblicke in die Strategien der jeweiligen politischen Entscheidungsträger:innen. Im Anschluss wurden die Quantenkommunikationsstrategien und -förderungen verschiedener Länder analysiert und verglichen. Das Konzept der technologischen Souveränität wird eingeführt und auf die Quantenkommunikation angewendet (Abschnitt 6). Auf der Grundlage von Experteninterviews werden die Kompetenzen im Bereich der europäischen Quantenkommunikation dargestellt und mögliche Herausforderungen und Maßnahmen erörtert.

Schließlich werden Schlussfolgerungen aus den vorgestellten Ergebnissen gezogen (Abschnitt 7).

2 Methoden

Publikationsanalyse

Für die Publikationsanalyse wurden begutachtete Veröffentlichungen aus dem "Web of Science" mittels einer stichwortbasierten Suche extrahiert. Die Suche wurde auf begutachtete Publikationen beschränkt, um "Schlüsselpublikationen" zu ermitteln, die einen Vergleich der F&E-Aktivitäten zwischen Ländern und wichtigen Organisationen ermöglichen. Die folgende Suchstrategie wurde verwendet:

{"quantum communication" OR "quantum key distribution" OR "quantum cryptography" OR "quantum repeater" OR ("quantum memory" AND communication) OR ("entangled photon" AND communication) OR (entanglement AND communication) OR ("entangled state" AND communication) OR (entanglement AND distribution) OR ("Bell state" AND communication)}

Für die Zitationsanalyse wurden die QCom-bezogenen Veröffentlichungen aus dem Jahr 2019 herangezogen. Wir haben dieses Jahr gewählt, da es ausreichend Zeit für die Zitierung bietet, aber dennoch nicht zu weit in der Vergangenheit liegt.

Patentanalyse

Die Gesamtzahl der Patentanmeldungen wurde mithilfe einer Suchstrategie ermittelt, die sowohl auf Patentklassifikationscodes als auch auf einer stichwortbasierten Textsuche in Titeln, Zusammenfassungen und Ansprüchen basierte. Um einen fairen Vergleich zwischen den Patentaktivitäten verschiedener Länder zu ermöglichen, wurde die Suche auf transnationale Patentanmeldungen beschränkt, d. h. auf Patentanmeldungen beim Europäischen Patentamt (EPA) oder bei der Weltorganisation für geistiges Eigentum (WIPO). Unterschiede in den nationalen Patentsystemen führen dazu, dass die Patentierung in bestimmten Ländern überschätzt wird, wenn nur die nationalen Patentämter berücksichtigt werden. Außerdem sind länderübergreifende Patente in der Regel mit Erfindungen verbunden, die einen höheren erwarteten wirtschaftlichen Wert haben. Die folgende Suchstrategie wurde verwendet:

"quantum communication" OR "quantum key distribution" OR "quantum cryptography" OR (qkd NOT A61#/IPC) OR "quantum repeater" OR ("quantum memory" AND communication) OR ("entangled photon" AND communication) OR (entanglement AND communication) OR ("entangled state AND communication) OR (entanglement AND distribution) OR ("bell state" AND communication) OR H04B0010-70/IPC,CPC OR (H04L0009-0852 OR H04L0009-0855 OR H04L0009-0858)/CPC AND (WO OR EP)/PC

Meta-Marktanalyse

Für diese Analyse wurde die Suchmaschine Google verwendet, um nach relevanten Marktstudien über Quantenkommunikation, Quantenkryptografie und Quantenschlüsselverteilung zu suchen. Diese Methode garantiert keine Vollständigkeit, aber wir identifizierten 68 relevante Marktstudien mit Erscheinungsdaten von 2019 bis Juli 2023. Da der Zugang zu Marktstudien in der Regel sehr kostenintensiv ist, haben wir uns ausschließlich auf die frei verfügbaren Informationen gestützt, die auf den Homepages der Marktstudienanbieter abrufbar sind. Dazu gehören globale Umsatzschätzungen und -prognosen, erwartete Wachstumsraten und relevante Akteure im Bereich der Technologie. Wir haben diese Informationen systematisch gesammelt, fehlende Prognosewerte unter der Annahme eines gleichmäßigen Wachstums interpoliert und die Umsatzprognosen und Unternehmensnennungen analysiert.

Projekt-Monitoring

Die Suche nach BMBF-Projekten erfolgte über die offizielle Website des Ministeriums, auf der Ausschreibungen und geförderte Projekte in den Bereichen IT-Sicherheit und Kommunikationssysteme aufgeführt sind. [1] Die Projekte, die sich auf die Quantenkommunikation beziehen, wurden auf der Grundlage der in der Projektbeschreibung enthaltenen Informationen, wie Ziele und Ansatz, ermittelt. Für EU-Projekte wurde die CORDIS-Projektdatenbank verwendet. [2] Die Suchmethodik für die EU-Datenbank umfasste eine erste Filterung anhand der Schlüsselwörter "communication" und "quantum" im Titel oder in der Zusammenfassung der Projekte. In der zweiten Runde wurden verwandte Projekte auf der Grundlage des Inhalts ihrer Zusammenfassungen ausgewählt. In einigen Fällen wurden weitere Nachforschungen anhand der Websites oder Veröffentlichungen der Projekte angestellt.

Internationale Situation und Initiativen

Regierungen legen in der Regel nicht die gesamte öffentliche Finanzierung von QCom-Technologien offen. Daher haben wir uns bei der Datenerhebung auf die wichtigsten Quantenstrategien in den USA, dem Vereinigten Königreich und Japan konzentriert, nämlich:

- US: Nationale Quanteninitiative (National Quantum Initiative - NQI) im Haushaltsjahr 2019-2023 [3]
- UK: Nationales Programm für Quantentechnologie (National Quantum Technology Programme – NQTP) im Zeitraum 2014-2023 [4]
- JP: Strategie für Quantentechnologie und Innovation (Quantum Technology and Innovation Strategy), veröffentlicht im Jahr 2020 [5]

Für die EU und Deutschland wurden die Daten aus dem Projekt-Monitoring aus Abschnitt 5.4 genutzt. Darüber hinaus wurde für die EU die EuroQCI-Initiative einbezogen, da sie eine wichtige Rolle bei der Unterstützung der Implementierung spielt. Die untersuchten Programme sind:

- EU: Horizont 2020/Horizon Europe und die europäische Quantenkommunikationsinfrastruktur (EuroQCI)
- DE: Rahmenprogramme "Quantentechnologien (2018)" und "Vernetzung und Sicherheit digitaler Systeme (2017)"

Trotz ihrer Bedeutung in diesem Bereich, sind offizielle Informationen über Chinas Investitionen in die QCom-Forschung nur schwer zu erhalten. Frühere Untersuchungen haben drastisch voneinander abweichende Zahlen aus verschiedenen Quellen ergeben. [6] Daher liefert unsere Analyse nur eine grobe Schätzung der chinesischen Investitionen.[1]

Die Gesamtfinanzierung für Quantentechnologien wurde auf der Grundlage der jeweiligen Hauptinitiativen berechnet (der NQI-Bericht für die USA, das NQTP für das Vereinigte Königreich und die Strategie für Quantentechnologie und Innovation für Japan). Im Falle der EU umfassen die Daten unseres Projekt-Monitorings zwar auch Projekte, die im Rahmen thematisch offener Initiativen (z. B. Europäischer Forschungsrat) finanziert werden, doch wurden hier nur Projekte im Rahmen des Quantum Flagships berücksichtigt, um die Intensität von QCom in der quantenspezifischen Strategie zu vergleichen. Darüber hinaus wurden zwei Specific Grant Agreement (SGA)-Projekte (Qu-Test und Qu-Pilot) aus der QCom-Förderung ausgeschlossen, da sie sich auf Quantentechnologien im

[1] Die Schätzung der Investitionen Chinas in die Quantenkommunikation erfolgt durch Multiplikation der angekündigten staatlichen Investitionen Chinas in alle Quantentechnologien (Mckinsey&Co. 2023) [7] mit dem durchschnittlichen Verhältnis der QCom-Förderung zur QT-Förderung in anderen analysierten Ländern.

Allgemeinen konzentrieren und es nicht möglich war, ihren Beitrag zu QCom-Themen zu differenzieren.[2] Für die Gesamtinvestitionen in Deutschland wurde neben den beiden oben genannten BMBF-Rahmenprogrammen auch das COVID-Konjunkturprogramm für Quantentechnologien (2 Milliarden Euro) berücksichtigt.

Um die Entwicklung der Fördermittel im Zeitverlauf zu untersuchen, wurden aus unserem Projekt-Monitoring Daten zur jährlichen Verteilung der geschätzten Fördermittel für Deutschland und die EU abgeleitet. Das bedeutet, dass die jährliche Verteilung durch Multiplikation der Anzahl der im Jahr begonnenen Projekte mit dem durchschnittlichen Projektbudget ermittelt wurde. EuroQCI wurde für die EU aufgrund fehlender Daten zur zeitlichen Aufteilung der Budgets von dieser Berechnung ausgeschlossen.

Die Daten für die USA wurden dem NQI Annual Budget Report 2023 entnommen, der das tatsächliche Budget für die Haushaltsjahre 2019-2021, das geschätzte Budget für das Haushaltjahr 2022 und das vorgeschlagene Budget für das Haushaltjahr 2023 enthält. In Japan basiert die Haushaltsplanung in der Regel auf einem einzigen Jahr, und unsere Daten spiegeln größtenteils die tatsächlichen jährlichen Zuweisungen für Projekte und Programme wider. Wenn keine jährlichen Haushaltsdaten verfügbar waren (z. B. beim SIP-Programm), wurde der Jahresdurchschnitt des gesamten Projektbudgets verwendet.

Das Vereinigte Königreich wurde in diesem Unterabschnitt nicht analysiert, da keine Informationen über die zeitliche Verteilung der Finanzierung vorlagen.

Überlegungen zu Technologiesouveränität

Die Diskussion über Aspekte der Technologiesouveränität in der Quantenkommunikation basiert auf fünf Interviews mit Expert:innen aus Wissenschaft, Wirtschaft und Politik. Den Interviewpartnern wurde das vom Fraunhofer ISI entwickelte Konzept der Technologiesouveränität vorgestellt. [8] Ziel der Interviews war es, die Einschätzung der Expert:innen zum Status quo der europäischen Quantenkommunikation in Bezug auf Bedürfnisse und Anforderungen (Welches Maß an Souveränität sollte Europa in der Quantenkommunikation anstreben?), Legitimation und Motivation (Warum brauchen wir technologische Souveränität in der Quantenkommunikation?), Herausforderungen (Welche Herausforderungen müssen bewältigt werden, um technologische Souveränität in der Quantenkommunikation zu erreichen?) und Maßnahmen (Wie können diese Herausforderungen von Wissenschaft, Industrie und Politik angegangen werden?) zu erhalten. Die Diskussion über den Status quo, die Herausforderungen und Maßnahmen wurde durch den Verweis auf die innovationshemmenden Faktoren strukturiert, wie sie im Oslo-Handbuch der OECD diskutiert werden. [9]

[2] Im Nachgang unserer Analyse haben wir erfahren, dass Qu-Test auch für QCom strategische Wichtigkeit besitzt. Im Update dieses Berichts wird dieses Projekt entsprechend berücksichtigt werden.

3 Hintergrund

In einer digitalisierten Welt, in der Informationen im Netz in Sekundenschnelle von A nach B übertragen werden, spielt Kryptografie eine entscheidende Rolle beim Schutz von Privatsphäre und IT-Sicherheit. Darunter versteht man im Wesentlichen die Verschlüsselung von digitalen Informationen, die sicherstellen soll, dass sensible Daten gegen Manipulation und unbefugten Zugriff geschützt sind. Kryptografie ist heutzutage mehr als nur ein Instrument zur Geheimhaltung, bildet sie doch das Fundament für die Sicherheit von kritischen Infrastrukturen wie Behördenkommunikation, Gesundheitswesen, Energie- und Wasserversorgung und vielem mehr. Sie ermöglicht es nicht nur, Informationen verschlüsselt vom Sender zum Empfänger zu übermitteln, sondern gewährleistet zudem die sichere Funktionsfähigkeit von Anwendungen, und ist demnach ein wesentlicher Bestandteil der heutigen hypervernetzten Welt, der auch für Banken, Behörden, Rechenzentren und Unternehmen von zentraler Bedeutung ist. So ist Kryptografie im Finanzsektor beispielsweise unerlässlich beim Schutz von Online-Transaktionen. Banken setzen komplexe Verschlüsselungstechnologien ein, um sicherzustellen, dass Geldtransfers und andere finanzielle Operationen vor betrügerischen Aktivitäten geschützt sind. Ein herausragendes Beispiel hierfür ist die Blockchain-Technologie, die auf fortschrittlicher Kryptografie basiert und bei Kryptowährungen wie Bitcoin (BTC) zum Einsatz kommt. Diese dezentrale, sichere Transaktionsverarbeitungsmethode hat die Finanzbranche nachhaltig beeinflusst und zeigt weiterhin auf, wie Kryptografie Innovationen vorantreibt. Ohne sie wären unsere Kommunikation, unsere Finanzen und unsere Privatsphäre massiv gefährdet. Klar ist, dass ihr Einsatz in allen denkbaren Bereichen des täglichen Lebens inzwischen allgegenwärtig und weiterhin auf dem Vormarsch ist.

In den zurückliegenden Jahren haben sich die Bereiche Quantencomputing, Quantensensorik, Quantensimulation und Quantenkommunikation als neuartige, wichtige Entwicklungs- und Investitionsfelder herausgestellt und werden als Schlüsselbereiche in der Forschung und Industrie angesehen. Die Gemeinsamkeit der vier thematischen Technologiesäulen liegt darin, dass sie sich den Gesetzen der Quantenmechanik bedienen, also dem Zweig der Physik, der das Verhalten von Teilchen auf atomarer und subatomarer Ebene beschreibt. Die Anwendungen der Quantentechnologien sind vielfältig und reichen von Quantensensoren und Quantencomputern bis hin zu kryptografischen Systemen. So bietet die Quantenkryptografie eine Möglichkeit, digitale Kommunikation sicher zu gestalten und Verschlüsselung auf höchstem Sicherheitsniveau zu garantieren. Anders als moderne Verschlüsselungsprotokolle wie RSA (Rivest–Shamir–Adleman) oder ECC (Elliptic Curve Cryptography) beruht diese nicht auf der erwarteten Komplexität eines mathematischen Algorithmus, sondern auf fundamentalen physikalischen Naturgesetzen, mit deren Hilfe eine informationstheoretisch herausgehobene Sicherheitsebene erreicht werden kann. Quantentechnologien befinden sich derzeit in verschiedenen Entwicklungsstadien, bergen jedoch vielversprechende Potenziale für den Wirtschafts- und Wissenschaftsstandort Deutschland und könnten zukünftig in unterschiedlichen Bereichen und Branchen der modernen Gesellschaft weitreichend zum Einsatz kommen. Im Bereich der Quantenkommunikation steht der Entwicklung von praktikablen Technologien, die den Anforderungen an Sicherheit in der Kommunikation gerecht werden und zugleich den strengen Kriterien wie hohen Kommunikationsraten und Resilienz gegenüber Seitenkanalangriffen, sogenannten Hackern, genügen, eine erhebliche Herausforderung in Forschung und Entwicklung gegenüber. Das übergeordnete Ziel liegt darin, Systeme zu schaffen, die nicht nur sicher und skalierbar, sondern auch kostengünstig sind, um eine breite Verfügbarkeit für die Gesellschaft zu gewährleisten.

In der Quantenkommunikation werden Informationen auf Basis von grundlegenden quantenmechanischen Prinzipien jenseits von klassischer Physik übertragen. Dabei kommt vor allem der Quantenkryptografie eine besondere Bedeutung zu. Darunter versteht man die Unterstützung der

Datenverschlüsselung mittels Quantenphysik. Dies ermöglicht nicht nur einen prinzipiell abhörsicheren Austausch von Schlüsseln über größere Entfernungen hinweg, sondern weist auch auf eine aussichtsreiche Zukunft hin, in der Quantentechnologie eine zentrale Rolle in der digitalen Kommunikation spielen könnte. Denn auch wenn die heute gängigen mathematischen kryptografischen Verfahren nach aktuellem Stand von modernen Computern nicht ökonomisch und in einer überschaubaren Zeit zu brechen und damit als sicher angesehen werden, darf nicht vergessen werden, dass die Sicherheit digitaler Informationen neben der Wachsamkeit vor allem von ständiger Forschung und Entwicklung abhängt. Ihre größte Bedrohung stellen hierbei Quantencomputer mit immenser Leistungsfähigkeit dar. So präsentierte der US-amerikanische Mathematiker und Informatiker Peter Shor bereits 1994 einen bahnbrechenden Quantenalgorithmus namens „Shor's Algorithm". Dieser Algorithmus ist insbesondere dafür bekannt, große natürliche Zahlen effizienter in ihre Primfaktoren zu zerlegen als dies herkömmliche Computer tun, und demonstriert somit die Fähigkeit von Quantencomputern zur schnelleren Lösung bei der klassischen asymmetrischen Public-Key-Kryptografie eingesetzten und bislang als nur schwer lösbar erachteten mathematischen Probleme. Indem Quantencomputer dank effizientem Algorithmus die kryptografischen Schlüssel in polynominaler statt exponentieller Zeit brechen können, ist davon auszugehen, dass sie grundsätzlich in der Lage sind, die Sicherheit zahlreicher aktueller Verschlüsselungsverfahren zu untergraben. Außerdem ist es auch heute schon möglich, konventionell verschlüsselte Daten abzufangen und zu einem späteren Zeitpunkt zu entschlüsseln ("jetzt sammeln – später entschlüsseln", engl. „harvest now, decrypt later"). Dadurch könnte ein Angreifer mithilfe eines Quantencomputers Zugang zu Informationen erhalten, die in der Vergangenheit verschlüsselt waren. Bei der Langzeitspeicherung von Daten und dem späteren Zugriff darauf entstehen massive Sicherheitsbedenken, die schon heute sorgfältig berücksichtigt werden müssen, um die Integrität und Vertraulichkeit von digitalen Informationen im Zeitalter von Quantencomputern zu gewährleisten. Kurz gefasst haben Quantencomputer das Potenzial, einige der derzeit verwendeten Verschlüsselungsalgorithmen zu zerschlagen und die Kommunikation unsicher zu machen. Um IT-Sicherheit auch in einer quantencomputergestützten Welt zu gewährleisten, müssen Verschlüsselungstechniken entwickelt werden, die gegenüber Quantenangriffen robust sind, und damit zusammenhängend abhörsichere Kommunikationsnetze aufgebaut werden.

Obwohl es derzeit noch keinen Quantencomputer gibt, der die heute angewandten Public-Key-Kryptografieverfahren umgehen könnte, hat die US-amerikanische National Security Agency (NSA) schon 2015 vor dieser bevorstehenden Gefahr gewarnt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nimmt in der Arbeitshypothese seiner 2017 bis 2020 durchgeführten Studie „Entwicklungsstand Quantencomputer" [10] an, dass Anfang der 2030er-Jahre erste kryptografisch relevante Quantencomputer zur Verfügung stehen, und hat darauf basierend auf dem Arbeitsgebiet der Post-Quanten-Kryptografie (PQK) gemeinsam mit dem im September 2018 vom Bundesministerium für Bildung und Forschung (BMBF) auf den Weg gebrachten Rahmenprogramm „Quantentechnologien – von den Grundlagen zum Markt" [11] den Wechsel zu quantenresistenter Kryptografie eingeleitet.

Um den Wechsel zu quantensicherer Verschlüsselung zu vollziehen, werden gegenwärtig zwei Lösungsstrategien verfolgt: zum einen die quantenbasierte Schlüsselverteilung (Quantum Key Distribution, QKD), zum anderen die soeben erwähnte Post-Quanten-Kryptografie (PQK). Bei letzterer handelt es sich um eine Weiterentwicklung der klassischen Public-Key-Kryptografie. In diesem Rahmen werden neue Verschlüsselungsverfahren auf der Grundlage klassischer Informationstheorie entwickelt, die auch mittels zukünftiger leistungsstarker Quantencomputer nicht zu brechen sind, d. h. eine höhere Komplexität aufweisen als die bisher verwendete Primfaktorzerlegung, beispielsweise Algorithmen basierend auf elliptischen Kurven oder gitterbasierte Protokolle. [12] Dadurch, dass sie keine spezielle Hardware erfordert, bietet sie eine kurzfristig verfügbare Möglichkeit, um die Schlüsselübertragung vor Quantenangriffen zu schützen. In diesem Zusammenhang hat das

US-amerikanische Standardisierungsinstitut (National Institute of Standards and Technology, NIST) seit 2017 in einem mehrstufigen Prozess zahlreiche eingerichtete Verfahren auf ihre Verwundbarkeit hin untersucht. Nur ein Algorithmus zur Public-Key-Kryptografie und drei Algorithmen für digitale Signaturen haben es im Jahr 2022 in die vierte Runde geschafft: das Schlüsseleinigungsverfahren CRYSTALS-Kyber sowie die Signaturverfahren CRYSTALS-Dilithium, Falcon und SPHINCS+. Zudem werden derzeit die drei codebasierten Schlüsseleinigungsverfahren Classic McEliece, BIKE und HQC sowie weitere Signaturverfahren einer Prüfung unterzogen, mit dem Ziel eine Auswahl von Methoden zu standardisieren, deren Sicherheit durch möglichst verschiedene mathematische Probleme gewährleistet wird. [13] Die Verfahren der Post-Quanten-Kryptografie werden im weiteren Verlauf dieses Berichts nicht weiter behandelt, sodass der Fokus auf der Quantenschlüsselverteilung als kryptografischem Verfahren liegt.

Die Quantenkryptografie gilt heutzutage als Schlüsseltechnologie für die Sicherheit digitaler Infrastrukturen in unserer Gesellschaft und lässt sich von den oben genannten Technologiesäulen als technologisch am weitesten fortgeschritten bezeichnen. Sie verspricht durch Nutzbarmachung quantenphysikalischer Effekte auch im Zeitalter von Quantencomputern einen sicheren Schlüsselaustausch zwischen zwei Parteien. Auf diesem Gebiet werden Protokolle zum sicheren Austausch kryptografischer Schlüssel entwickelt, mit denen Abhörversuche infolge von Veränderungen durch die dazu erforderliche Messung zuverlässig entdeckt werden können. Dabei werden nicht die Nachrichten selbst übertragen, sondern es werden symmetrische Schlüssel erzeugt, mit deren Hilfe die zu übermittelnde Nachricht kodiert werden kann. Durch die Verschlüsselung kann die Übertragung über einen klassischen, möglicherweise unsicheren Kanal erfolgen, sodass keine neue Kommunikationsinfrastruktur vonnöten ist. Aus diesem Grund gilt die Quantenkryptografie als wegweisend für die abhörsichere Schlüsselverteilung innerhalb von Kommunikations- und Informationsnetzen und ist gegenwärtig Gegenstand vielfältiger Forschungs- und Entwicklungsbemühungen. Ein Beispiel für ein solches Kryptografieverfahren ist die quantenbasierte Schlüsselverteilung, die im folgenden Kapitel näher beschrieben wird.

4 Qualitative Analysen: Theoretische Grundlagen und Forschung zu Quantenkommunikation

Um den aktuellen Stand der Forschung und die neuesten Entwicklungen im Bereich der Quantenkommunikation aufzuzeigen, wird nachfolgend ein Überblick über die theoretischen Grundlagen sowie die laufenden nationalen und internationalen Aktivitäten gegeben. Dabei wird auf eine systematisch aufeinander aufbauende Struktur zurückgegriffen, wobei die verschiedenen Generationen den Entwicklungsstand der jeweils besprochenen Technologie von fortgeschritten (2.1.) bis elementar (2.3.) widerspiegeln. Jede Generation steht dabei für eine Stufe in der Realisierung, Implementierung und Integration in die bestehende Infrastruktur. Die Generationen sind gegliedert in: 1. Quantenschlüsselverteilung nach dem Prepare & Measure-Prinzip, 2. Quantenschlüsselverteilung mit photonischen Verschränkungsquellen und 3. Quantenrepeater mit Verschränkungsverteilung.

4.1 Erste Generation: Quantenschlüsselverteilung (Prepare & Measure)

4.1.1 Theoretische Grundlagen

Die Quantenkryptografie bietet eine Möglichkeit, digitale Kommunikation mithilfe einzelner Photonen abhörsicher zu machen und Verschlüsselung auf höchstem Sicherheitsniveau zu gewährleisten. Wie oben erwähnt, bietet diese nicht algorithmische, sondern physikalische Sicherheit. Der Hauptzweck der Quantenschlüsselverteilung besteht darin, die Sicherheit der von Sender und Empfänger gemeinsam erzeugten Schlüssel zu garantieren. Die physikalischen Grundlagen der ersten Generation, die Quantenüberlagerung und das No-Cloning-Theorem, werden nachfolgend skizziert.

a) *Quantenüberlagerung*: Quantenüberlagerung ist ein grundlegendes Prinzip in der Quantenmechanik, das besagt, dass ein Quantenteilchen nicht nur in einem Zustand, sondern zur gleichen Zeit in einer Überlagerung von beliebig vielen Zuständen existieren kann. In der Quantenkryptografie wird dies genutzt, um mithilfe quantenmechanischer Prinzipien sichere Schlüssel zu erzeugen, mit denen Nachrichten kodiert und dekodiert werden können. In diesem Sinne können Quantenbits (Qubits), die kleinsten logischen Einheiten in der Quanteninformation, verschiedene Schlüsselwerte gleichzeitig annehmen. Ein Angreifer, der versucht, den Schlüssel abzufangen, würde aufgrund der Überlagerung nicht wissen, in welchem Zustand sich das Qubit befindet, bis er es misst – denn erst die Messung erzwingt die Entscheidung für einen endgültigen Zustand. Nach der Messung befindet sich das Quantensystem nicht mehr im Überlagerungszustand, sondern in einem bestimmten Eigenzustand, der durch das Messergebnis determiniert wird – die Überlagerung wird durch die Messung zerstört. In einem Übertragungsprotokoll der legitimen Kommunikationspartner (siehe unten) erzeugt die durch den Angreifer durchgeführte Messung Fehler, die die Kommunikationspartner detektieren und so den Angriff nachweisen können. Eine Herausforderung ist die Dekohärenz, bei der die Überlagerung aufgrund der inhärent fragilen Natur von Qubits durch externe Einflüsse – vor allem bei langen Übertragungsdistanzen – gestört werden kann. Werden Qubits jedoch auf den Zuständen von Photonen kodiert, kann man von der vergleichsweise geringen Dekohärenz der Lichtteilchen profitieren.

b) *No-Cloning-Theorem*: Gemäß dem quantenmechanischen No-Cloning-Theorem nach William Wootters und Wojciech Zurek (1982) ist es nicht möglich, eine exakte Kopie eines unbekannten Quantenzustands herzustellen, ohne den Zustand des Originalsystems zu verändern. Immer dann, wenn der Zustand eines Quantenobjekts (z. B. eines Photons) kopiert wird, wird unweigerlich auch der Zustand des Originalobjekts verändert. Dieses Prinzip hat erhebliche Auswirkungen auf die IT-Sicherheit, da es sicherstellt, dass ein Angreifer einen Schlüssel nicht unbemerkt kopieren kann, ohne dabei dessen Zustand notwendig zu verändern.

In Rahmen der Quantenschlüsselverteilung werden identische Schlüssel in Form zufälliger Bitabfolgen bei Sender und Empfänger gleichzeitig erzeugt. Durch die nachfolgende Verschlüsselung und Entschlüsselung unter Nutzung der identischen Schlüssel kann die Kommunikation auch über einen unsicheren Kanal stattfinden, ohne dass sich die beiden Parteien um die Integrität der Daten sorgen müssen.

Die Funktionsweise von QKD lässt sich wie folgt beschreiben: Die QKD verwendet Qubits, die auf verschiedene Arten dargestellt werden können. Eine Möglichkeit sind abgeschwächte kohärente Lichtpulse oder Einzelphotonen, die in komplementären Quantenzuständen mit nicht-orthogonalen Basen präpariert werden, wie beispielsweise horizontale/vertikale und diagonale/antidiagonale Polarisation. Im ersten Schritt erzeugt der Sender Qubits (z. B. als Einzelphotonen), die er in einer zufälligen Abfolge aus 0 und 1 und in zufälligen Basen kodiert und dann mittels Kommunikationskanal wie Glasfaserkabel an den Empfänger übermittelt (*Prepare*). Dies geschieht für jedes Photon einzeln und ohne vorherige Absprache zwischen den beiden Parteien. Der legale Empfänger misst die einzelnen Qubits wiederum in zufällig ausgewählten Messbasen (*Measure*). Sender und Empfänger tauschen sich über einen öffentlichen Kanal über die gewählten Präparations- und Messbasen aus und nutzen nur diejenigen Messergebnisse, bei denen die Basen übereinstimmen (denn nur dann liefert eine Messung ein deterministisches Ergebnis). Versucht ein Angreifer die Qubits während der Übertragung abzuhören oder zu kopieren, muss er eine zufällige Messbasis wählen und eine Messung durchführen. Dadurch verändert sich im Sinne des No-Cloning-Theorems unweigerlich ihr Zustand. Diese Zustandsänderung bleibt nicht unbemerkt, denn Sender und Empfänger vergleichen die Zustände eines Teils der gesendeten und empfangenen Teilchen. Eine – im Verhältnis zu den Kanalverlusten – hohe Fehlerrate bei diesem Vergleich deutet auf einen Angriff hin. Demzufolge kann ein Angreifer zwar Informationen über den Schlüssel abfangen, aber er kann es nicht tun, ohne von Sender und Empfänger wahrgenommen zu werden. In diesem Fall bricht das Protokoll ab, bevor sensible Daten verschlüsselt und übertragen werden, was die Sicherheit der QKD als prinzipiell abhörsicherem Verfahren herausstellt. Zur Erhöhung der Sicherheit können mehrere Schlüsselbits durch logische Operationen kombiniert werden („Privacy Amplification"), um den sogenannten Sifted Key zu erhalten, mit dem die zu übertragende Information verschlüsselt und entschlüsselt werden kann. Ist ein Schlüssel mindestens genauso lang wie die Nachricht, wird er zufällig erzeugt, geheim gehalten und niemals recycelt, d. h. als Einmalschlüssel bzw. im One-Time-Pad- bzw. OTP-Verfahren verwendet, so ist es nachweislich ausgeschlossen, dass die verschlüsselte Nachricht auf dem Übertragungsweg von einer unbefugten Partei gebrochen werden kann. [13] Der praktische Nutzen der QKD besteht somit darin sicherzustellen, dass die von Sender und Empfänger vereinbarten Schlüssel geheim und unverändert bleiben, um Nachrichten informationstheoretisch abhörsicher zu übertragen.

In seinem in 2024 veröffentlichten Positionspapier weist das Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen mit seinen internationalen Partnern auf die Grenzen der QKD hin. Eine liege beispielsweise darin, dass sie im Gegensatz zur schon heute verfügbaren PQK nicht auf aktueller Hardware implementiert werden könne, sondern spezielle Hardware benötige, die wiederum kostspielig sei. Daneben schränke die durch Signalverluste in Glasfasern bedingte geringe

Reichweite den Einsatzbereich ein. Das wichtigste Argument des BSI besteht jedoch darin, dass die Sicherheit konkreter Implementierungen von QKD bislang nicht bewiesen ist. Der Einsatz von QKD für die kommerzielle Nutzung wird derzeit in vielen Feldversuchen getestet, ist zum jetzigen Zeitpunkt aber noch auf wenige Nischen-Anwendungen beschränkt. [14]

4.1.2 Varianten der Kodierung

Der Ausdruck *Variable* bezieht sich auf die Quanteneigenschaften oder Freiheitsgrade (Degrees of Freedom, DOF), mit denen Informationen kodiert werden. Die QKD kann grundsätzlich auf unterschiedliche Arten bzw. in verschiedenen Quantenzuständen implementiert werden, nämlich in diskreten oder kontinuierlichen Zuständen. Diese beiden repräsentieren die zwei Klassen von Verfahren zum Quantenschlüsselaustausch. Die im vorhergehenden Abschnitt beschriebene Variante von QKD basiert auf diskreten Variablen, weswegen man in diesem Zusammenhang von DV-QKD-Protokollen spricht. Das bedeutet, dass die Zustände der Qubits eine diskrete Natur aufweisen. Diese Protokolle beruhen auf der Unbestimmtheitsrelation (Überlagerungsprinzip und Kopierverbot). Eine Kodierung, bei der Qubit-Zustände kontinuierlich verteilt sind, bezeichnet man entsprechend als CV-QKD-Protokolle. [14] Im Gegensatz zu DV-QKD-Protokollen arbeiten CV-QKD-Protokolle mit unendlich dimensionalen Quantenzuständen.

Die Kodierung von Qubits kann in verschiedenen Freiheitsgraden eines physikalischen Systems erfolgen. Ein bereits genanntes Beispiel ist die Polarisation eines Photons oder eines Lichtpulses in nicht-orthogonalen Basen (horizontal/vertikal, diagonal/antidiagonal, links-/rechtszirkular). Lichtzustände können zudem in ihrer Ankunftszeit (Time-Bin) oder räumlichen Moden kodiert werden. In CV-QKD-Protokollen werden Zustände über ihre Amplitude und ihren Phasenwinkel relativ zu einer Referenzwelle definiert. Die beiden Klassen (DV und CV) von Verfahren zum Quantenschlüsselaustausch werden im Folgenden erläutert.

DV-Kodierung

Die DV-Kodierung benutzt diskret verteilte Freiheitsgrade eines physikalischen Systems zur Kodierung, beispielsweise die binäre Verteilung „horizontale Polarisation" oder „vertikale Polarisation" eines Lichtteilchens für die Zustände 0 und 1 oder zwei definierte Energiezustände eines Elektrons.

Das älteste und bekannteste Verfahren zur quantenbasierten Schlüsselverteilung ist das 1984 von Gilles Brassard und Charles Bennett eingeführte BB84-Protokoll, das seit den ersten Implementierungen zu Beginn der 1990er Jahre noch heute standardmäßig eingesetzt wird. Bei ihm handelt es sich um ein DV-QKD-Protokoll, bei dem das oben beschriebene Prepare & Measure-Verfahren zum Einsatz kommt. Zur Übertragung nutzt es in der Originalversion die Polarisationsfreiheitsgrade von Einzelphotonen. Der Vorteil eines DV-QKD-Protokolls wie des BB84-Protokolls liegt neben der Robustheit und großen Reichweite von ca. 100 Kilometern insbesondere in der Einfachheit seiner Modulation, da die dabei verwendeten Techniken einfach zu implementieren und kontrollieren sind. Sein Nachteil liegt jedoch darin, dass die dabei erforderlichen Verfahren zur Photonendetektion teuer und aufwendig sind. [15]

Das BB84-Protokoll wurde ursprünglich für einzelne Photonen formuliert, was einen hohen Aufwand für die Erzeugung und den Nachweis der Einzelphotonen nach sich zieht. Technisch wesentlich einfacher ist das Senden sehr schwacher Laserpulse, allerdings gibt es hier mit einer bestimmten Wahrscheinlichkeit immer auch Pulse, in denen mehr als ein Photon detektiert werden könnte. Eine Abhörstrategie wäre nun, sich einen Teil des Lichtpulses abzuzweigen, zu warten, bis die richtige Basis aus der Kommunikation zwischen Sender und Empfänger bekannt wird, und erst dann zu messen. So könnte eine vollständige Information über diese Signale erlangt werden. Durch geschickte Verwendung von schwachen Lichtpulsen unterschiedlicher Intensität (sogenannte „Köder-

zustände“, engl. Decoy State Protocol) können dennoch die schwachen Lichtpulse für den Quantenschlüsselaustausch genutzt werden, was die praktische Anwendbarkeit erheblich vereinfacht. Bei diesem Verfahren testen die Kommunikationspartner, ob ein Angreifer von intensiveren Lichtpulsen größere Anteile abzweigt als von schwächeren, was eine Angriffsstrategie darstellt, die die Chance auf Entdeckung minimiert. Die Decoy State-Variante des BB84-Protokolls wird heute in nahezu allen Anwendungen der DV-QKD eingesetzt.

CV-Kodierung

Die Quantenkryptografie umfasst nicht nur diskrete Verfahren zum Quantenschlüsselaustausch, sondern auch solche, die auf kontinuierlichen Variablen basieren. Während DV-QKD-Protokolle, wie soeben beschrieben, Informationen in diskreten Zuständen von Einzelphotonen kodieren, verwenden CV-QKD-Protokolle kontinuierliche Parameter wie die Amplitude und Phase von Licht für die Kodierung und Messung.

CV-QKD wurde zuerst 1999 von Timothy C. Ralph vorgeschlagen [16] und von Frédéric Grosshans und Philippe Grangier in ein praktikables Protokoll überführt [17]. Typisch für CV-QKD ist eine Phasenkodierung, d. h. der Sender wählt eine feste Amplitude eines Lichtfelds (Laser) und zufällige Phasen, die dem Lichtfeld durch Phasenmodulatoren aufgeprägt werden. Im Idealfall folgen diese Phasen einer Gauß-Verteilung im Phasenraum; sie können prinzipiell unendlich viele Werte annehmen, wobei die Wahrscheinlichkeiten für diese Werte gaußverteilt sind. In der Praxis ist dies schwierig zu realisieren, sodass die Gauß-Verteilung durch diskrete Verteilungen mit endlich vielen Phaseneinstellungen approximiert wird. Diese diskreten Modulationsschemata benutzen M verschiedene Phasenwerte und entsprechend M äquidistant verteilte kohärente Zustände im Phasenraum („M Symbol Quadrature Modulation“).

Ein typisches Protokoll zur Schlüsselerzeugung läuft wie folgt ab: Der Sender präpariert einen von M verschiedenen kohärenten Zuständen und sendet ihn über einen Kanal zum Empfänger; dieser führt eine Messung des Zustands über eine Homodyn-Methode (Bestimmung von Amplitude und Phase relativ zu einer Referenzwelle) durch. Dabei wird das optische Signal mit einem Referenzlichtfeld, dem sogenannten lokalen Oszillator (LO), interferiert, der bei der Phasenausrichtung von Sender und Empfänger hilft und dessen Intensität viel höher ist als die des Quantensignals. So enthält das Quantensignalfeld in CV-QKD-Protokollen grundsätzlich nur wenige Photonen, um die Nicht-Orthogonalität der Quantenzustände zu gewährleisten. Der Empfänger muss die gemessenen Phasenwerte noch einer diskreten Verteilung der M möglichen Phasen zuordnen („Reverse Reconciliation“). Der Schlüssel wird schließlich durch Methoden der Fehlerkorrektur und „Privacy Amplification“ erstellt. Analog zu DV-QKD-Protokollen werden Angriffe auf den Kanal wiederum detektiert, da Messungen den Quantenzustand verändern.

Ein Vorteil von CV-QKD-Protokollen besteht darin, dass sie keine speziellen Lichtquellen wie Einzelphotonen oder zugehörige Einzelphotonendetektoren benötigen, sondern ein ähnliches Verfahren wie die phasenkodierte klassische Kommunikation, die sogenannte Phasenumtastung (Phase Shift Keying) nutzen, die für sehr hohe Datenraten eingesetzt wird. Da sich beide Methoden stark ähneln, ist die CV-QKD leichter mit bestehenden klassischen Kommunikationssystemen zu integrieren und daher gegenüber DV-QKD insbesondere in kohärenten optischen Kommunikationsverfahren die bevorzugte Variante. [18] Neben der Kompatibilität mit bestehender Infrastruktur und damit einhergehender Kosteneffizienz profitieren CV-QKD-Protokolle auch von Praktikabilität im Nachweisverfahren. Von Nachteil sind jedoch die beschränktere Reichweite von durchschnittlich weniger als 100 Kilometern [19] sowie die kompliziertere theoretische Sicherheitsanalyse. [15] Ein weiterer Nachteil besteht in der oft komplexen Implementierung, der erforderlichen präzisen Kontrolle über die kontinuierlichen Variablen des Lichts und den aufwendigen Entfaltungs- und Abgleichverfahren.

4.1.3 Netzwerkarchitekturen

QKD kann in verschiedenen strukturellen Anordnungen eingesetzt werden, um Schlüssel zwischen zwei oder mehr Parteien über verschiedene Entfernungen sicher auszutauschen. Die gängigsten Netzwerkarchitekturen werden nachfolgend skizziert:

c) *Punkt-zu-Punkt-Verbindung*: Die Punkt-zu-Punkt-Verbindung repräsentiert die einfachste Architektur zur abhörsicheren Kommunikation zwischen zwei Parteien. Theoretische Grundlage dafür ist das einfache Sender-Empfänger-Modell zur Kommunikation, das in den 1940er Jahren von Claude E. Shannon und Warren Weaver entwickelt wurde. Gemäß diesem Modell erfolgt der Schlüsselaustausch zwischen einem Sender und einem Empfänger über einen direkten Kommunikationskanal. Punkt-zu-Punkt-Verbindungen sind also bereits realisiert und weithin in Betrieb. Ein Beispiel hierfür sind Direktverbindungen, die eine Distanz von 1000 Kilometern über Glasfaser überbrücken.

d) *Quantenkommunikationsnetzwerk*: Ein Quantenkommunikationsnetzwerk erweitert die Grundidee der Punkt-zu-Punkt-Verbindung zu größeren, verzweigten Quantennetzen mit einer Vielzahl von Knoten. Hier können nicht nur zwei, sondern mehr Kommunikationspartner über Kommunikationskanäle miteinander agieren, die in verschiedenen Topologien (z. B. Stern-, Ring-, Baum- oder Netzstrukturen) angeordnet sein können. Diese Netzwerke bieten somit den Vorteil, eine größere Anzahl von Teilnehmern in die Kommunikation einzubinden, was besonders in komplexen Szenarien von Vorteil ist. Dabei kann sich jeder Teilnehmer verschlüsselt mit jedem anderen Netzwerkteilnehmer austauschen, ohne dass Unbefugte die Nachricht unbemerkt abfangen, verändern oder kopieren können. Ebensolche Netze können an den Zwischenknoten je nach Anwendungsszenario vertrauenswürdige Knoten, sogenannte „Trusted Nodes“, beinhalten. An diesen Knoten werden „Messe und leite weiter“-Verfahren angewandt, die für Punkt-zu-Punkt-Sicherheit sorgen. Da der Schlüssel an diesen Stellen als klassischer Bitstring verfügbar und leicht angreifbar ist, müssen die Verbindungsknoten in hohem Maße abhörsicher sein. Durch diese Architektur können beispielsweise in Ballungsräumen Mehrparteiennetze eingerichtet werden. Ihren echten Vorteil spielen Mehrparteiennetzwerke jedoch erst durch die Verwendung verteilter verschränkter Zustände aus, durch die spezielle Protokolle wie sichere Abstimmungen und Gruppenentscheidungen ermöglicht werden.

Die Wahl der Netzwerkarchitektur hängt von den spezifischen Anforderungen der jeweiligen Anwendung, den verfügbaren Ressourcen und der gewünschten Sicherheitsstufe ab. Während Punkt-zu-Punkt-Verbindungen in einigen Szenarien (z. B. wenn eine direkte physische Verbindung zwischen zwei Kommunikationspartnern besteht und der Schlüsselaustausch auf diese beiden beschränkt ist) ausreichend sein mögen, sind für umfangreichere Netzwerke oder Übertragungen über große Distanzen hinweg komplexere Architekturen erforderlich. Diese müssen entsprechend höhere Anforderungen an Zuverlässigkeit, Skalierbarkeit und Sicherheit erfüllen. Zudem müssen ebensolche Netzwerkarchitekturen Herausforderungen wie Störungen, optischer Dämpfung und anderen Umwelteinflüssen entgegenwirken, die die Quanteninformation unerwünscht beeinflussen könnten.

Netzwerkintegration

Punkt-zu-Punkt-Verbindungen können auf verschiedene Arten implementiert werden. Neben klassischen Glasfasern gibt es auch die Möglichkeit der Implementierung über Freistrahl oder Satelliten. Aus Gründen der Praktikabilität existieren zudem hybride Ansätze, bei denen QKD in bereits bestehende klassische Kommunikationsnetzwerke integriert wird. In diesem Fall wird die Quantenkryptografie genutzt, um einen sicheren Schlüsselaustausch in einem übergeordneten Netzwerk zu ermöglichen, das auch herkömmliche Kommunikationskanäle umfasst. Dabei werden per QKD mit

einer relativ niedrigen Rate Schlüssel erzeugt, die anschließend in einem klassischen Verschlüsselungsverfahren (oftmals die beiden symmetrischen Verschlüsselungsalgorithmen bzw. Blockchiffren Data Encryption Standard, DES, oder Advanced Encryption Standard, AES) verwendet und regelmäßig aufgefrischt werden. Die Integration von QKD verspricht nicht nur eine erhöhte Sicherheit und Flexibilität in verschiedenen Kommunikationsszenarien, sondern ermöglicht es auch, bestehende Kommunikationsnetzwerke in hybrider Funktion einzusetzen, ohne eine neue Infrastruktur aufbauen zu müssen.

4.1.4 Stand der Forschung und Industrie

QKD-Demonstrationen und Teststrecken

Die QKD nach dem Prepare & Measure-Prinzip, obwohl vergleichsweise neu, hat sich Stand 2024 als marktreife Technologie zur Ermöglichung sicherer Kommunikation etabliert. Weltweit wird sie auf vielen Teststrecken erprobt und in bestehende Infrastrukturen wie Glasfasernetzwerke integriert. Dies zeigt, dass der Übergang von der Forschung zur kommerziellen Anwendung in einigen Nischenmärkten bereits gelungen ist.

Das weltweit erste Netzwerk zur Verteilung von Quantenschlüsseln, das 2004 in Massachusetts in Betrieb genommen wurde, war das DARPA-QKD-Netz (Defense Advanced Research Projects Agency). Dieses betrieb zehn optische Knotenpunkte und demonstrierte erstmals die Realisierbarkeit der QKD in einer realistischen Testumgebung. [20] Im Jahr 2004 folgte in Wien mit SECOQC (SEcure COmmunication based on Quantum Cryptograph) das erste funktionale EU-geförderte QKD-Netz, das sechs Knotenpunkte und acht Verbindungen umfasste und über 200 Kilometer Glasfaser sechs Standorte in Wien und die ca. 70 Kilometer westlich gelegene Stadt St. Pölten verband. [21] Im Rahmen der „Swiss Quantum Initiative (SQI)" wurde 2009 ein weiteres QKD-Netz installiert, das fast zwei Jahre in Betrieb war. Dessen Ziel bestand darin, die Zuverlässigkeit und Robustheit von QKD im Dauerbetrieb in einer Feldumgebung zu demonstrieren. [22] Ähnliche Entwicklungen finden sich auch in Asien. So präsentierte China in Wuhu 2009 ein hierarchisches Quantennetzwerk, das aus einem Backbone-Netzwerk mit vier Knoten und einer Reihe an Subnetzen bestand. [23] In Tokio wurde 2010 ein weiteres Netz errichtet, mit dem zum ersten Mal eine quantengesicherte Videokonferenz durchgeführt werden konnte, die als Meilenstein auf dem Weg zu abhörsicherer Kommunikation gilt. [24] Auf US-amerikanischer Seite ist an dieser Stelle das seit 2011 vom Los Alamos National Laboratory installierte Hub-and-Spoke-Netzwerk zu nennen, mit dem die Möglichkeit auf quantengesichertes Internet getestet wurde. [25] Zudem gelang es 2017 auf europäischer Ebene erstmals, mittels chinesischem Satelliten ein durch Quantenkryptografie gesichertes Videotelefonat von Wien nach Peking zu führen. [15] Ähnliches fand 2021 im Rahmen des Projekts „QuNET" statt, bei dem in Bonn die erste quantengesicherten Videokonferenz zwischen zwei Bundesbehörden stattfand. [26]

Das derzeit sicher weitreichendste und fortschrittlichste QKD-Netz ist das Beijing-Shanghai Backbone Network (BSBN), dessen Betrieb im August 2017 aufgenommen wurde. Dabei handelt es sich um die weltweit erste quantensichere Langstrecken-Kommunikationsverbindung, die unter der Leitung der University of Science and Technology of China (USTC) entwickelt wurde und bereits von Banken und anderen Finanzunternehmen für die Datenübertragung genutzt wird. Das Netz vom Typus Trusted Node-Netzwerk befindet sich in China und verbindet die Städte Peking, Jinan, Hefei und Shanghai miteinander. Es besteht aus mehr als 700 Faserverbindungen und zwei Hochgeschwindigkeits-Freiraumverbindungen zwischen dem Quantenkommunikationssatelliten Micius, der seit 2016 die Erde in ca. 500 Kilometern Entfernung umkreist, und den Bodenstationen, die die QKD-Übertragung unterstützen. Das Netzwerk umfasst eine insgesamt etwa 2000 Kilometer lange Glasfaserverbindung zwischen den vier Städten sowie eine 2600 Kilometer lange Satellitenverbindung zwischen zwei Observatorien östlich von Peking und in der Nähe der chinesischen Grenze zu

Kasachstan. Die Glasfaserverbindungen werden von 32 vertrauenswürdigen Knoten unterstützt, die die Quanteninformation weiterleiten. Die Knotenpunkte des Netzes verzweigen sich jeweils in verschiedene Richtungen bis zum Nutzer, wodurch eine umfassende und abgesicherte Quantenkommunikationsinfrastruktur geschaffen wird. [27] In den USA plant das Start-up Quantum Xchange ein weitreichendes QKD-Netzwerk entlang der Ostküste. Die erste Etappe soll die Metropole Manhattan mit seiner Nachbarstadt New Jersey verbinden, wo sich die Rechenzentren vieler Banken befinden. [28] Weitere wichtige Beispiele für bereits existierende Forschungsnetzwerke auf diesem Gebiet sind unter anderem die Chicago Quantum Exchange (CQE) sowie die Brookhaven National Laboratory Quantum Network Facility (BNL): Während sich die sechs (vorwiegend universitären) Mitglieder des CQE auf die Entwicklung neuer Wege zum Verständnis und zur Nutzung der Gesetze der Quantenmechanik konzentrieren, [29] ist die BNL eine staatliche experimentelle Einrichtung, die eine Infrastruktur und Fähigkeiten zur Verfügung stellt, die der Entwicklung des Quanten-Ökosystems dienen sollen. [30] Auf akademischer Seite findet sich seit September 2020 das an der University of Arizona angesiedelte „NSF Engineering Research Center for Quantum Networks (CQN)", das bestrebt ist, technische und soziale Grundlagen für Quantennetze zu schaffen. [31] Daneben kündigte Amazon im Juni 2022 auf industrieller Ebene das „AWS Center for Quantum Networking" an, dessen Aufgabe darin besteht, neue Hardware, Software und Anwendungen für Quantennetzwerke zu entwickeln. [32] Innerhalb der EU wird die Quantenkommunikation vor allem im Rahmen der niederländischen Initiative „QuTech" gefördert. Hier finden insbesondere auf theoretischer Ebene umfangreiche Aktivitäten wie Protokollentwicklung, Layer-Strukturen und Einbettung in existierende Infrastruktur statt. [33] Zudem fungiert QuTech auch als technischer Koordinator der „Quantum Internet Alliance (QIA)". Dabei handelt es sich um einen Zusammenschluss aus vierzig führenden europäischen akademischen, industriellen und forschungsorientierten Technologieorganisationen, dessen Ziel der Aufbau eines weltweit ersten vollständigen Prototyps eines Quantennetzwerks ist. Exemplarisch für die hybride Integration von QKD in existierende klassische Netze ist das „Londoner Quantum-Secured Metro Network" zu nennen. Dieses verfügt über drei mittels Glasfaser verbundene Knoten und ist inzwischen auch kommerziell nutzbar. [34, 35] Außerdem wurde 2021 von Toshiba UK und BT das erste quantensichere Netzwerk Großbritanniens in Bristol realisiert. Über ein sieben Kilometer langes Glasfaserkabel überträgt dieses Daten und Quantenschlüssel zwischen drei Instituten in Bristol. [36] Weitere Bemühungen finden sich mit der länderübergreifenden Initiative „Europäische Quantenkommunikationsinfrastruktur (EuroQCI)" und dem von der Deutschen Telekom geleiteten Koordinationsprojekt „PETRUS". Diese beiden zielen darauf ab, ein hochsicheres EU-weites Glasfaser-Backbone für QKD-Anwendungen aufzubauen. Im Rahmen von EuroQCI wird ein auf Glasfasern beruhendes terrestrisches Segment sowie ein auf Satelliten basierendes Weltraumsegment eingesetzt, das zugleich Bestandteil von IRIS, dem neuen raumgestützten sicheren Kommunikationssystem der EU, sein wird. [37]

QKD-Leistungsparameter

Ein zentrales Problem, dem QKD noch immer gegenübersteht, ist die beschränkte Reichweite, denn die verwendeten Photonen werden grundsätzlich entweder über Glasfasern oder im freien Raum (Free-Space Optical Communication, FSO) übertragen. In beiden Fällen sind große Distanzen problematisch: Während große Entfernungen zu starker Absorption im Material der Glasfasern führen, weitet sich der Strahl bei der optischen Freiraumübertragung auf. Dadurch ist die Übertragung auf einige Hundert Kilometer begrenzt und somit nicht ausreichend für umfassende sichere Kommunikationsnetzwerke. Mit dem Ziel die Absorption möglichst gering zu halten, findet die Übertragung meist in Wellenlängenbereichen mit besonders geringer Absorption, den sogenannten Telekom-Fenstern, im Infraroten bei 1310 bzw. 1550 nm statt. Dagegen sind die Verluste im freien Raum deutlich geringer, sodass mittels FSO im nahen Infrarot (ca. 800 bis 850 nm) eine satellitenbasierte Kommunikation über mehrere Tausend Kilometer ermöglicht werden kann. [13]

Direkte QKD-Verbindungen können typischerweise Distanzen von 100 bis maximal 400 oder 500 Kilometer überbrücken. Diese Distanzen sind limitiert durch die Verluste in optischen Glasfasern (in der Regel 1 % Transmission nach 100 km) und das Dunkelrauschen der eingesetzten Detektoren. Als maximale Distanz einer Direktverbindung mittels Glasfaser wurde bislang eine Strecke von 1000 Kilometern erreicht. Hierbei kam die sogenannte Twin-Field-QKD zum Einsatz, bei der die Interferenz zweier verschiedener phasenstabiler optischer Felder verwendet wird, um die Quanteninformation zwischen den Kommunikationspartnern auszutauschen. [38] Neben der Distanz spielt ebenfalls die Taktrate der Übertragung eine bedeutende Rolle bei der Implementierung. Die größte bisher erzielte Schlüsselrate für DV-QKD betrug 110 Mbit/s bei einer Reichweite von zehn Kilometern Glasfaser. [38–40] Ein CV-QKD-System mit 16 Symbolen erzielte Schlüsselraten von 49 Mbit/s über 25 Kilometer bis 2 Mbit/s über 80 Kilometer Glasfaserstrecke. [41] Eine Übersicht über aktuelle Leistungsparameter (mit einem Fokus auf CV-QKD) geben Zhang et al. (2023). [42]

Hybride Integration

Die Integration von QKD erfolgt oftmals in hybrider Form, bei der sie mit klassischen Verschlüsselungsverfahren kombiniert wird. Grund dafür sind die – im Vergleich zu Datenkommunikationsraten – recht niedrigen Schlüsselerzeugungsraten der QKD, sodass die Quantenschlüssel mit einer geringen Auffrischungsrate als Eingangsgröße für klassische Verschlüsselungsverfahren eingesetzt werden. Die Implementierung von QKD und ihre Integration in bestehende Kommunikationsinfrastrukturen erfordert generell spezielle Hardwarekomponenten wie Photonenquellen mit Polarisationsfiltern, Quantenkanäle und -detektoren. So werden im Falle der kontrollierten Erzeugung einzelner Photonen beispielsweise aufwendige Quellen und empfindliche Detektoren benötigt, mit denen diese nachgewiesen werden können. Aus diesem Grund gibt es zahlreiche Forschungsbemühungen, die darauf abzielen, diese Hardware effizienter und kostengünstiger zu gestalten, um die Verbreitung der Technologie weiter voranzutreiben. Als Beispiele für die hybride Integration von QKD lassen sich das weiter oben erwähnte Metronetz in London, aber auch das Cambridge Quantum Network anführen. [34, 35] Letzteres beinhaltet drei Knotenpunkte, die durch eine fünf bis zehn Kilometer lange Glasfaserstrecke miteinander verbunden sind.

QKD-Forschungsprojekte

Von der Erprobung auf Teststrecken und Einbindung in existierende Infrastruktur ausgehend haben sich zahlreiche nationale und internationale Forschungsprojekte herausgebildet, die auf die Entwicklung von Systemen und Komponenten abzielen. Einer der zentralen Akteure auf diesem Gebiet in Deutschland ist die BMBF-geförderte „QuNET"-Initiative. Diese untersucht Implementierungen von QKD für den Aufbau einer quantensicheren IT-Infrastruktur und entwickelt innovative Technologien für die Quantenkommunikation, wie beispielsweise im Bereich der Faser- und Freistrahl-Links sowie der Entwicklung von Einzelphotonenquellen und -detektoren. Das Ziel des Projekts besteht darin, auf Quantentechnologie beruhende hochsichere Kommunikationssysteme zu implementieren, die vor Cyberangriffen sicher sind. Dies soll eine sichere Kommunikation zwischen Behörden und (Hoch-)Sicherheitsbereichen sowie innerhalb von Bankennetzen und kritischer Infrastruktur gewährleisten. Daneben bereichern die „QuNET+"-Projekte unter der Leitung von Industriepartnern das Spektrum um technologische Aspekte der QKD. [43] Eine Kooperation mit „QuNET" und vielen weiteren akademischen, institutionellen und industriegeführten Projekten findet zudem im Rahmen des ebenfalls BMBF-geförderten „Schirmprojekts Quantenkommunikation Deutschland (SQuaD)" statt. Im Fokus des Projekts stehen der nachhaltige Technologietransfer von der Wissenschaft in die Industrie, die Vernetzung mit der deutschen Quantenkommunikationsgemeinschaft, die Implementierung von Teststrecken für QKD sowie die Einbindung in klassische Kommunikationsinfrastrukturen. [44] Ferner existieren einzelne BMBF-geförderte Projekte, die Forschung und Entwicklung im Umfeld der QKD betreiben. Hierzu gehören beispielsweise die Projekte „Integration von QKD in IKT-Netze (Q-net-Q)" und „Quantum Physical Layer Service Integration (QuaPhySI)" zur Integration

von QKD in bestehende Systeme der Informations- und Kommunikationstechnologie. [45, 46] Ähnliches stand innerhalb des kürzlich durchgeführten Projekts „OpenQKD" im Fokus, das von der Europäischen Kommission gefördert wurde und dessen Ziel die Demonstration einer transparenten Integration von quantensicheren Lösungen für potenzielle Endnutzer und relevante Stakeholder auf breiter Ebene war. Durch dieses Vorhaben sollte der Grundstein für die Einführung einer europaweiten quantensicheren digitalen Infrastruktur gelegt und die globale Position Europas an der Spitze der Quantenkommunikationsfähigkeiten gestärkt werden. [47] Erwähnt sei an dieser Stelle auch das Projekt „Anwendungsorientierte Demonstration von Quantenkommunikation in Deutschland (DemoQuanDT)", dessen Fokus auf der Erforschung, Entwicklung und Demonstration eines sicheren, netzwerkübergreifenden und herstellerunabhängigen QKD-Netzwerkmanagementsystems in Deutschland liegt. Im Rahmen dieses Projekts wird eine durch QKD gesicherte Demonstrationsstrecke in einer realen Umgebung zwischen Bonn und Berlin aufgebaut, die dem Forschungsbetrieb dient und das längste Quantennetzwerk Deutschlands werden soll. Hierfür werden die bereits bestehenden Glasfasern und regulären Betriebsstellen genutzt. [48] Daneben zielt das ebenso BMBF-geförderte Projekt „6G-Quantum Security (6G-QuaS)" auf die Entwicklung eines hybriden drahtgebundenen Industrienetzes ab. Dabei soll die Quanteninformation kontinuierlich in der Phase und Amplitude des Lichts kodiert werden. Dies soll zu deutlich geringeren Latenzzeiten und größerer Widerstandsfähigkeit gegen Angriffe bei gleichbleibender Sicherheit führen. [49] Ziel des BMBF-geförderten Projekts „Entwicklung hochperformanter Übertragungskomponenten für quantensichere Kommunikation über Glasfaserleitungen in Metro- und Weitverkehrsnetzen (DE-QOR)" ist die Weiterentwicklung bestehender CV-QKD-Ansätze basierend auf kohärenter optischer Übertragungstechnik. In diesem Kontext sollen zentrale Komponenten auf Sender- und Empfängerseite entwickelt und zu kompakten Systemen integriert und Übertragungsstrecken im urbanen Raum mit einer Länge von mehr als 80 Kilometern angestrebt werden. [50] Ebenfalls zu erwähnen ist das Verbundprojekt „Quantum Internet of Things (QUIET)", das auf die Entwicklung eines Kommunikationsnetzwerks und eine Vernetzung von Quantensensoren mit verteilten Quantenzuständen und konventioneller Übertragung abzielt. Auf diese Weise soll die Leistungsfähigkeit und Sicherheit des Netzwerks deutlich gesteigert werden. [51]

Da sie auf quantenmechanischen Prinzipien basiert, gilt die QKD als äußerst robust gegenüber Seitenkanalangriffen. Infolgedessen wird sie als Grundlage für die Sicherheit in der Kommunikation im Zeitalter von Quantencomputern betrachtet. Diese Widerstandsfähigkeit hat dazu geführt, dass QKD nicht nur als Mittel zur Absicherung herkömmlicher Kommunikation angesehen wird, sondern auch als Schlüsseltechnologie für zukünftige Anwendungen gilt. Laufende Forschungsprojekte und Entwicklungen zeigen, dass sie kontinuierlich verbessert wird, um den Herausforderungen der sich stetig weiterentwickelnden Technologielandschaft gerecht zu werden. Ihr Potenzial erstreckt sich über die abhörsichere Kommunikation hinaus und findet ebenso Anwendung in aufstrebenden Technologiefeldern wie dem Internet der Dinge (Internet of Things, IoT) und sicheren Cloud-Kommunikationsplattformen. In diesem Zusammenhang hat die QKD in den letzten Jahren erheblich an Bedeutung gewonnen und wird in Forschung und Industrie intensiv vorangetrieben, um die Kommunikation auch im Zeitalter einer von Quantencomputern geprägten Welt aufrechtzuerhalten.

4.2 Zweite Generation: Quantenschlüsselverteilung (Photonische Verschränkungsquellen)

4.2.1 Theoretische Grundlagen

Verschränkungsbasierte QKD, die auf verschränkten Photonen basiert, erweitert das Spektrum von Punkt-zu-Punkt-Verbindungen, bei denen der Informationsaustausch unmittelbar zwischen einem Sender und einem Empfänger stattfindet. Anders als das in 4.1.1. beschriebene Prepare & Measure-Verfahren, das auf dem Präparieren, Senden und Messen einzelner Teilchen beruht und eine vertrauenswürdige Quelle bzw. Detektoren voraussetzt, geht dieser Ansatz von einer hochgradigen Korrelation verschränkter Teilchen aus. Dadurch werden keine vertrauenswürdigen Quellen oder Detektoren benötigt. Ihm liegt das Prinzip der Quantenverschränkung zugrunde. Darunter versteht man eine spezielle Form der Verknüpfung zwischen zwei oder mehr quantenmechanischen Teilchen, unabhängig von der räumlichen Entfernung zwischen ihnen. Dabei sind die gemeinsamen Eigenschaften aller Teilchen zusammen festgelegt, die Zustände der individuellen Qubits jedoch unbestimmt. Diese werden erst bei der Messung eindeutig festgelegt. Durch das Messen des Zustands des einen Qubits ist ebenso der Zustand der anderen bekannt, ohne dass er direkt gemessen werden muss. Jede Störung oder Abhörung der übertragenen Informationen führt zu einer unvermeidlichen Zustandsänderung in einem der Qubits. Da die Teilchen verschränkt sind, wird diese Änderung sofort im korrelierten Qubit registriert, wodurch die Störung oder der Seitenkanalangriff detektiert werden kann.

Die Funktionsweise des Protokolls (nach den Grundlagen der von Artur Ekert 1991, E91, [52] sowie Charles H. Bennett, Gilles Brassard und N. David Mermin 1992, BBM92, [53] beschriebenen Protokolle) lässt sich wie folgt umreißen: Ausgangspunkt der Betrachtungen ist eine Quelle verschränkter Photonen. Im ersten Schritt wird ein Paar verschränkter Photonen zwischen den beiden Kommunikationspartnern aufgeteilt. Ähnlich wie im BB84-Protokoll messen die beiden Partner ihr Photon jeweils in einer zufällig gewählten Basis. Der Unterschied zum BB84-Protokoll liegt nun darin, dass hier nicht nur zwei nicht-orthogonale Basen gewählt werden, sondern drei. Je nach Kombination der ausgewählten Messbasen können die Kommunikationspartner ein gemeinsames Schlüsselbit erzeugen oder einen Nachweis führen, dass die gemessenen Photonen tatsächlich verschränkt sind. Die erhöhte Sicherheit dieser Technologie wird somit durch den Verschränkungsnachweis gewährleistet, mit dessen Hilfe belegt werden kann, dass die Teilchen tatsächlich aus der Verschränkungsquelle stammen und nicht modifiziert wurden. In der Praxis werden für den Verschränkungstest verschiedene Verfahren angewandt. Neben dem 1964 von John Steward Bell vorgeschlagenen Bell-Test wird beispielsweise auch die 1969 von John Clauser, Michael Horne, Abner Shimony und Richard Holt entwickelte CHSH-Ungleichung eingesetzt. Verschränkungsbasierte QKD kann in speziellen Anwendungsszenarien von Vorteil sein, insbesondere in solchen, die eine Kommunikation zwischen mehreren Teilnehmern erfordern (Mehrparteien-QKD). Sie sorgt für sichere Übertragungen über große Distanzen hinweg und könnte daher auch in komplexen Netzwerken oder Anwendungen wie dem IoT eine Rolle spielen. Gleichwohl diese Technologie auf Teststrecken weithin erprobt wird, ist sie zum gegenwärtigen Zeitpunkt noch nicht so ausgereift wie ihre Vorgängergeneration.

4.2.2 Varianten der Kodierung

DV-Kodierung

Die Implementierung von verschränkungsbasierten DV-QKD-Protokollen erfordert Quellen für verschränkte Photonenpaare, für die oftmals die parametrische Fluoreszenz (Spontaneous Parametric

Down-Conversion, SPDC) eingesetzt wird. Bei diesem physikalischen Vorgang wird ein hochenergetisches (z. B. ultraviolettes) Photon in einem nichtlinearen Kristall in zwei verschränkte niederenergetische (z. B. infrarote) Photonen, die sogenannten Signal- und Idler-Photonen, umgewandelt. Die Verschränkung existiert dabei in der Regel im Freiheitsgrad der Polarisation (z. B. ein Photon ist horizontal polarisiert, das andere vertikal, wobei bis zu einer Messung unbestimmt ist, welches Photon welche Polarisation aufweist). Diese beiden verlassen den Kristall in unterschiedlichen Winkeln, wodurch eine räumliche Trennung möglich wird. Somit können mithilfe der parametrischen Fluoreszenz verschränkte Photonenpaare erzeugt und räumlich aufgetrennt an die Kommunikationspartner verteilt werden, sodass sie für die Umsetzung von DV-QKD-Protokollen zur Verfügung stehen. Eine aufwendigere Methode zur Erzeugung verschränkter Photonen besteht in der Verwendung von Halbleiter-Quantenpunkten, d. h. künstlichen Atomen bestehend aus Halbleitermaterialien. Hier wird eine strahlende Kaskade (nahezu gleichzeitige Emission von zwei Photonen in aufeinanderfolgenden optischen Übergängen) genutzt, um für gewöhnlich polarisationsverschränkte Photonen zu erzeugen. Der hohe technische Aufwand (Betrieb bei kryogenen Temperaturen) wird aufgewogen durch eine deterministische Emission mit hoher Rate bei hoher Reinheit des erzeugten verschränkten Zustands. [54]

CV-Kodierung

Zurzeit basieren die meisten CV-QKD-Implementierungen auf einem Ein-Weg-Verfahren, wobei wie in Abschnitt 4.1.2. beschrieben, die Quantenschlüssel mithilfe kontinuierlicher Parameter wie Amplitude und Phase von Lichtpulsen erzeugt werden, die von Sender zu Empfänger gesendet werden. Die Platzierung einer Verschränkungsquelle in der Mitte zwischen zwei Nutzern bietet wie beim E91-Protokoll mit diskreten Variablen eine alternative Option für eine sichere Kommunikation mit effizienter Nutzung von Quantenressourcen. Die Verschränkungsquelle produziert hier Zustände, deren Verschränkung in kontinuierlich verteilten Variablen kodiert ist (Einstein-Podolsky-Rosen- bzw. EPR-Zustände), beispielsweise „Squeezed States“, bei denen die quantenmechanische Unschärfe einer Variable (z. B. Phase) unter die Grenze der Heisenbergschen Unschärferelation reduziert wird (auf Kosten der Fluktuationen der komplementären Variable, beispielsweise der Amplitude). Die beiden Kommunikationspartner benutzen dann wie bei der CV-QKD der ersten Generation Homodyn-Messungen, um zufällig Amplitude oder Phase der Zustände zu messen. Der Vergleich der Messbasen und die Nachbearbeitungsprozeduren der CV-QKD führen auch hier zu einer Schlüsselerstellung und einer Verifikation der Verschränkungseigenschaften. Verschränkungsbasierte CV-QKD Verfahren sind seit etwa zehn Jahren theoretisch vorgeschlagen, [55] bisher jedoch experimentell nur in wenigen Demonstrationsexperimenten implementiert. [56]

4.2.3 Netzwerkarchitekturen

Wie die Vorgängergeneration bietet auch die verschränkungsbasierte QKD Punkt-zu-Punkt-Quantensicherheit. Der Unterschied zwischen beiden Technologien besteht in erster Linie darin, dass die QKD der zweiten Generation durch die Möglichkeit des Verschränkungsnachweises keine vertrauenswürdige Quelle oder Detektoren voraussetzt. Da die Sicherheit des Quantenschlüsselaustauschs durch die intrinsische Natur der Quantenverschränkung gewährleistet wird und eine hochgradige Korrelation zwischen Zuständen der Einzelteilchen existiert, bedarf es keiner vorherigen Zustandsvorbereitung, um die effiziente Schlüsselerstellung zu gewährleisten.

Im Bereich der verschränkungsbasierten QKD ist die Mehrparteien-Quantenverschlüsselung von großem Interesse, bei der vom Dienstanbieter verschränkte Photonenpaare generiert und an mehrere Nutzer an verschiedenen Standorten verteilt werden. [57, 58] Eine technische Umsetzung dessen ist mittels einer breitbandigen Paarquelle möglich, die per Wellenlängendemultiplexing auf verschiedene Frequenzkanäle aufgeteilt wird. [59] In solchen Mehrparteien-Netzwerken mit multi-

partiter Verschränkungsverteilung werden weitreichendere Protokolle als bei Punkt-zu-Punkt-Verbindungen möglich: Bei der Kommunikation mit mehreren Benutzern ist es oft wünschenswert, dass alle Teilnehmer einen einzigen geheimen Schlüssel teilen, sodass jedes Mitglied Nachrichten entschlüsseln kann, die von einem anderen Mitglied der Gruppe gesendet wurden. Das Verfahren, bei dem die Nutzer eines solchen Netzes einen Schlüssel gemeinsam nutzen, wird als Konferenzschlüsselvereinbarung (Conference Key Agreement) bezeichnet. Diese Art der Schlüsselverteilung kann für mehrere Benutzer eine starke Verschlüsselung beispielsweise für Aufgaben wie Videokonferenzen bieten. Die Aufteilung einer Information auf mehrere Nutzer in diesen Netzwerken ermöglicht die gemeinsame Nutzung von „Quantengeheimnissen" (Quantum Secret Sharing, QSS). QSS kann geheime Nachrichten vor Abhörern und unehrlichen Spielern schützen und besitzt wichtige Anwendungen wie in der Schlüsselverwaltung, Identitätsauthentifizierung, Abstimmungen bei entfernteren Partnern und sogenannten „Quantenauktionen".

4.2.4 Stand der Forschung und Industrie

QKD-Demonstrationen und Teststrecken

Wie zuvor beschrieben, gilt die QKD inzwischen als marktreife Technologie, die auf zahlreichen Teststrecken erprobt und in bestehende Kommunikationsinfrastrukturen integriert wird. Obwohl die verschränkungsbasierte QKD noch nicht so ausgereift ist wie ihre Vorgängergeneration, wurden bereits experimentelle Untersuchungen dazu durchgeführt. Dabei wurde verschränkungsbasierte Kommunikation über Faserstrecken bis hin zu Satelliten-Verbindungen mit mehr als 1100 Kilometer demonstriert. [60] Während in vielen Demonstrationsexperimenten bisher SPDC-basierte probabilistische Verschränkungsquellen eingesetzt wurden, bleibt die Verwendung von Halbleiter-Quantenpunkt-Verschränkungsquellen zunächst noch auf erste Experimente über kurze Distanzen beschränkt. [61, 62]

Für die Einbindung in existierende Netzwerke für sichere Kommunikation ist in dieser Generation vor allem das „Quantum Communications Hub" in Großbritannien von zentraler Bedeutung, das sich seit 2019 in der zweiten Förderperiode befindet und dessen Ziel die Entwicklung sicherer Quantenkommunikation auf allen Entfernungsskalen ist. Die Faserstrecke des Hubs reicht von Bristol über London bis nach Cambridge/Ipswich und verfügt an den Endpunkten über Metro-Netzwerke. In diesem Rahmen werden unter anderem Verschränkungsverteilung an eine Vielzahl an Nutzern, Architekturen für den physikalischen und höheren Layer sowie die Integration von Quantenkommunikation mit klassischem Datenverkehr untersucht. [63]

QKD-Leistungsparameter

Aktuell ermöglicht die verschränkungsbasierte QKD über Glasfaser eine Reichweite von etwa 100 bis 250 Kilometern. So wurde mittels verlegter Glasfaser bisher eine Reichweite von ca. 50 Kilometern erreicht, mittels Untersee-Glasfaserkabel bzw. Unterwasser-Kommunikationskabel eine Reichweite von ca. 96 Kilometern sowie mittels transnationaler Punkt-zu-Punkt-Verbindung eine Reichweite von ca. 248 Kilometern. [64–66]

Trotz der beschränkten Reichweite können durch die Aneinanderreihung mehrerer kurzer Segmente allerdings Kommunikationsnetzwerke aus vertrauenswürdigen Knoten geschaffen werden. Wie oben erwähnt, spielt neben der Reichweite auch die Taktrate eine große Rolle bei der Implementierung. Die bislang größte Schlüsselrate der verschränkungsbasierten QKD der zweiten Generation betrug 110 bit/s bei einer Distanz von zehn Kilometern Glasfaser. [67]

QKD-Forschungsprojekte

Auf den oben beschriebenen Fortschritten aufbauend haben sich einige nationale und internationale Forschungsprojekte herausgebildet. So zielt das Projekt „IT-Sicherheit durch verschränkungsbasierten Quantenschlüsselaustausch" („Quantum based Security Promise", Q-Sec-Pro) unter anderem darauf ab, ein neues Sicherheitslevel, insbesondere für kritische Infrastrukturen, durch Entwicklungen im Bereich der Quantenkryptografie auf Basis einer Quelle für verschränkte Photonenpaare im Telekom-Wellenlängenbereich zu gewährleisten. Um dies zu realisieren, sollen ein QKD-Protokoll sowie geeignete Hard- und Software erforscht und implementiert werden. Dies leistet nicht nur einen wichtigen Beitrag zum Aufbau einer deutschen Quantenkommunikationsindustrie, sondern sichert gleichermaßen die technologische Souveränität Deutschlands. [68] Ähnliche Bemühungen finden im Rahmen des BMBF-geförderten Projekts „Q-Fiber" statt, dessen Ziel darin besteht, verschränkungsbasierte QKD mit vier Kommunikationsteilnehmern zu demonstrieren, was zukünftig unter anderem im Medizinsektor relevant sein könnte. In diesem Kontext könnten beispielsweise sensible Gesundheitsdaten mittels verschränkter Lichtquanten verschlüsselt und ausgetauscht werden. Für die Übertragung und kostengünstige Detektion der Lichtquanten innerhalb der bestehenden IT-Infrastruktur sollen neuartige Lichtleitkabel eingesetzt und erforscht werden. [69]

Ein aktueller Schwerpunkt der Forschung liegt auf der Device-Independent Quantum Key Distribution (DI-QKD). Diese basiert ebenso auf quantenmechanischen Prinzipien, wurde jedoch mit dem Ziel entwickelt, die Sicherheit des Schlüsselaustauschs unabhängig von der genauen Implementierung der Quantengeräte zu gewährleisten. So verlässt man sich bei herkömmlichen Quantenschlüsselaustauschprotokollen wie dem BB84-Protokoll darauf, dass die verwendeten Quantengeräte bestimmte Eigenschaften erfüllen und dass die Messergebnisse verlässlich auf Quantenverschränkung und -messungen zurückzuführen sind. DI-QKD versucht dagegen, auf diese Annahmen zu verzichten und die Sicherheit des Protokolls selbst dann zu gewährleisten, wenn die Geräte von einem Angreifer manipuliert werden könnten. Die Grundidee besteht darin, den Schlüsselaustausch so zu gestalten, dass er gegenüber allgemeinen Quantenangriffen robust ist, selbst wenn der Angreifer die genaue Natur der verwendeten Quantengeräte kennt oder beeinflusst. Gegenwärtig gibt es verschiedene Ansätze und Protokolle im Bereich der DI-QKD. Einige dieser Ansätze beruhen auf der nicht-lokalen Korrelation quantenverschränkter Zustände und der lückenlosen Verletzung von Bell-Ungleichungen, um mögliche Störungen und Manipulationen auszuschließen. Obwohl DI-QKD in der Praxis eine große Herausforderung darstellt, haben die jüngsten theoretischen und experimentellen Bemühungen zu grundlegenden DI-QKD-Implementierungen geführt. [70] Technologische Basis für diese Protokolle sind die Verteilung von Verschränkung (in Form von Photonenpaaren oder verschränkten Quantenspeichern) mit hoher Güte und nahezu perfekte Quantenmessungen – dies ist in der Praxis sehr schwer zu erreichen. Erste Demonstrationsanwendungen in Laborumgebungen zeigen DI-QKD mit verschränkten Photonenpaaren im Telekom-Wellenlängenbereich über eine Faserstrecke von 220 Metern. [71] Eine andere Option ist die Erzeugung verschränkter Zustände von stationären Quantenspeichern, die räumlich getrennt sind (siehe auch Abschnitt zur 3. Generation und Verschränkungsverteilung). Hier wurden in ersten Experimenten gefangene Strontium-Ionen [72] und Rubidium-Atome [73] verwendet, die zwei Meter und 440 Meter räumlich getrennt waren. Die Schlüsselerzeugungsraten in allen diesen Experimenten sind derzeit noch deutlich zu niedrig für technologisch relevante Anwendungen und im Wesentlichen durch die Detektionseffizienzen von Einzelphotonendetektoren und zu geringe Wiederholraten limitiert. Auf der anderen Seite garantiert der DI-QKD Ansatz die höchstmögliche Sicherheit von QKD-Methoden.

4.3 Dritte Generation: Quantenrepeater (Verschränkungsverteilung)

4.3.1 Theoretische Grundlagen

Wie bereits erwähnt, stellt die Realisierung größtmöglicher Übertragungsdistanzen derzeit eine große Herausforderung für die QKD dar. Bereitet die Informationsübertragung auf kürzeren Strecken in der Regel keine Schwierigkeiten, gestaltet sich dies bei größeren Entfernungen über viele Hundert Kilometer allerdings deutlich schwieriger. Über solche Distanzen werden optische Signale wie die einzelnen oder verschränkten Photonen wie auch die abgeschwächten Laserpulse der QKD der ersten und zweiten Generation aufgrund von Verlusten und optischer Dämpfung von Glasfasern enorm abgeschwächt. Werden die Verluste zu hoch, kann nicht mehr zwischen einem Lauschangriff und der technischen Abschwächung des Kanals unterschieden werden und die Sicherheit des Schlüsselaustauschs wird kompromittiert. Ebenso sinkt die erzielbare Schlüsselrate massiv. Eine Option, die bereits genannt wurde, ist die serielle Aneinanderreihung einzelner kurzer Segmente in sogenannten Trusted Node-Netzwerken. Diese Netzwerke besitzen den Nachteil, dass die Information an jedem Zwischenknoten wieder klassisch vorliegt, leichter angreifbar ist und somit keine Ende-zu-Ende quantenmechanische Sicherheit garantiert werden kann. Um das Problem des Informationsverlusts auszuräumen und die Übertragung auch über längere Strecken hinweg zu ermöglichen, konzentriert sich die Forschung auf die Entwicklung von Quantenrepeatern.

Quantenrepeater wurden erstmals 1998 von Hans Briegel et al. vorgestellt [74] und gelten seitdem als wegweisender Technologiebaustein. Der Ausdruck *Quantenrepeater* ist dabei leicht irreführend und kann schnell zu Missverständnissen führen. Im Unterschied zu den weithin bekannten Repeatern (Wiederholverstärkern) in Kommunikationsstrecken werden die ankommenden Signale nämlich nicht gemessen und weitergesendet oder verstärkt. Dies würde, wie aus dem Messproblem der Quantenmechanik bekannt, zu unerwünschten Fehlern führen. Stattdessen teilen Quantenrepeater eine ausgedehnte Übertragungsstrecke entlang eines Kommunikationskanals in kürzere Abschnitte auf, innerhalb derer Verschränkung mit nur geringen Verlusten verteilt wird, ohne dass Quantenzustände gemessen oder kopiert werden. Die Verteilungsverschränkung geschieht über das Versenden von verschränkten Photonenpaaren oder Verschränkungsaustausch (siehe weiter unten). An den Enden dieser Segmente werden die empfangenen oder erzeugten verschränkten Zustände mithilfe von Quantenspeichern gespeichert. Durch die Speicherung der Quanteninformation muss die Verschränkungsverteilung nicht für alle Segmente synchron erfolgen, was bei endlicher Erfolgswahrscheinlichkeit des Protokolls einen entscheidenden Vorteil bietet. Die zweite entscheidende Komponente von Quantenrepeatern ist das Prinzip des Verschränkungsaustauschs („Entanglement Swapping“). Dadurch können jeweils zwei Abschnitte der Übertragungsstrecke miteinander verknüpft werden, wodurch sich die Reichweite von Quantenverschränkung in Kommunikationsnetzwerken sukzessive vergrößert. Zur Erläuterung dieses Prinzips lässt sich eine einfache Kette von Knoten A – B – C – D betrachten. In einem ersten Schritt erzeugen die Knoten A und B jeweils eine lokale Verschränkung zwischen einem Quantenspeicher und einem Photon (z. B. durch spezielle Protokolle, die Auswahlregeln bei der Emission von Photonen ausnutzen). Die beiden Photonen von A und B werden zu einer Messstation zwischen A und B gesendet, wo eine Messung ihrer gemeinsamen Eigenschaften, eine sogenannte Bell-Messung durchgeführt wird. Dabei bleibt der Zustand der einzelnen Teilchen unbekannt. Diese Messung sorgt bei Vorliegen des richtigen Ergebnisses dafür, dass die Quantenspeicher bei A und B in einen verschränkten Zustand projiziert werden (aus den Möglichkeiten des gemeinsamen Zustands der Quantenspeicher wird durch die Messung der verschränkte Zustand ausgewählt). Mit dieser Operation wird Verschränkung über das Segment A – B verteilt; die Knoten C – D können analog verfahren. In einer weiteren Verschrän-

kungstausch-Operation kann nun eine Bell- Messung an den Quantenspeichern B und C durchgeführt werden. Wiederum bei Vorliegen eines ausgewählten Messergebnisses werden nun die Quantenspeicher A und D verschränkt. Auf diese Art und Weise kann nun Verschränkung zwischen den Enden der Kette erzeugt werden. Bei größeren Distanzen und mehreren Segmenten wird dieser Vorgang entsprechend so lange wiederholt, bis die Enden der gesamten Kette verschränkt sind.

Die verteilten verschränkten Zustände können schließlich als Ressource genutzt werden: zum einen für die verschränkungsbasierte QKD der zweiten Generation, bei der das Prinzip der Schlüsselerzeugung identisch ist. Der Unterschied zwischen beiden QKD-Generationen besteht darin, dass der Quantenrepeater größere Entfernungen überbrücken kann, ohne auf vertrauenswürdige Knoten zurückgreifen zu müssen. Der eigentliche Vorteil des Quantenrepeaters besteht jedoch in der Option, dass die verteilte Verschränkungsressource zur Verteilung von Quantenzuständen genutzt werden kann, ohne dass diese zerstört werden. Dazu bedient man sich der Quantenteleportation, bei der der zu transportierende Quantenzustand zusammen mit einem Teil des verschränkten Zustands gemessen wird (Bell-Messung) und anhand des Ergebnisses eine spezifische Operation auf dem zweiten Teil des verschränkten Zustands den originalen Ausgangszustand wieder herstellt. Durch die Verteilung verschränkter Zustände über große Distanzen mithilfe des Quantenrepeaters kann die Teleportation ebenso über große Distanzen durchgeführt werden. Durch die Verteilung von Quantenzuständen ist zudem auch verteiltes Quantenrechnen (Distributed Quantum Computing) möglich. Dabei handelt es sich um die Verknüpfung mehrerer Quantencomputer via Quantenlinks an verschiedenen physischen Standorten mit dem Ziel, die Rechenleistung zu steigern und gemeinsam komplexe Aufgaben zu lösen. Auf diese Weise können Quantencomputer auch mit klassischen Systemen vernetzt werden, was ebenfalls mehr Anwendungsmöglichkeiten und höhere Flexibilität bietet. Denn ein verteiltes Quantenrechnen würde bei gleicher Größe der Quantencomputer eine exponentielle Zunahme des verfügbaren Rechenraums und der Leistungsfähigkeit bewirken und es ermöglichen, komplexe Probleme in bisher unerreichter Geschwindigkeit zu lösen. Die Möglichkeit, mehrere Quantencomputer miteinander zu vernetzen, ist ein Schritt von enormer Bedeutung für zukünftige Netze von Quantencomputern.

Die durch den Quantenrepeater erzeugten Verschränkungsressourcen gewährleisten im Kontext der Quantenkommunikation in einer hypervernetzten Welt nicht nur eine erhöhte IT-Sicherheit durch eine durch quantenmechanische Prinzipien geschützte Ende-zu-Ende-Verschlüsselung, sondern sie können zudem auch in der verschränkungsassistierten klassischen Kommunikation Anwendung finden und die Sicherheit und Resilienz von Kommunikationsnetzen erhöhen. Die Vorteile der verschränkungsassistierten Kodierung liegen in niedrigeren Latenzzeiten, höherer Übertragungskapazität und Resilienz sowie der Verhinderung von DoS-Attacken (Denial of Service). Dies zeigt, dass Quantenrepeater einen wichtigen Beitrag zur Forschung an 6G-Netzen liefern können, wie im Rahmen des in 2021 vom BMBF herausgegebenen Forschungsrahmenprogramm „Kommunikationssysteme: Souverän. Digital. Vernetzt." festgehalten ist. [75] Die verschiedenen Anwendungsperspektiven, die Quantenrepeater eröffnen, haben hohe gesellschaftliche Bedeutung im Kontext der IT-Sicherheit und des Schutzes kritischer Infrastrukturen. Dennoch sind ihre Entwicklung und großflächige Implementierung äußerst komplex. Obwohl bis heute noch kein ernstzunehmender kommerzieller Markt und keine direkte wirtschaftliche Konkurrenz besteht, ist anzunehmen, dass beides innerhalb der nächsten Jahre stark vorangetrieben wird. Denn Quantenrepeater sind eine notwendige Voraussetzung für den Aufbau von weitreichenden Quantenkommunikationsnetzen, die Strecken von mehreren Hundert Kilometern abdecken, und bieten deswegen einen enormen Nutzen für die Kommunikation der Zukunft.

4.3.2 Varianten der Kodierung

Ähnlich wie die DV-Protokolle der ersten und zweiten QKD-Generation beruhen auch Quantenrepeater auf diskreten Variablen, d. h. auf DV-QKD-Protokollen, bei denen Informationen in diskreten Zuständen einzelner oder verschränkter Quantensysteme kodiert und projektive Messungen vorgenommen werden. CV-QKD-Protokolle, die wegen ihrer technologischen Verwandtschaft mit aktuellen klassischen Kommunikationssystemen attraktiv sind, finden bei der Realisierung von Quantenrepeatern bisher keine Anwendung. Selbst bei theoretischen Studien, die derzeit das Wissenschaftsgebiet der Quantenrepeater gegenüber experimentellen Untersuchungen bei Weitem dominieren, werden CV-Konzepte kaum betrachtet. [76–78] Gründe dafür sind die Komplexität der benötigten Operationen, die Fehlerkorrektur für CV-Zustände und das Fehlen von Quantenspeichern. CV-Systeme erfordern fortgeschrittene Fehlerkorrekturtechniken, um die transmittierten Quantenzustände vor Rauschen und Verlusten in den Übertragungskanälen zu schützen und die Verschränkung aufrechtzuerhalten. Während die Quantenfehlerkorrektur für DV-Systeme etabliert ist, ist die Ausweitung dieser Techniken auf kontinuierliche Variablen immer noch ein aktives Forschungsgebiet. Die Implementierung von Quantenspeichern für CV-Systeme, die Zustände mit kontinuierlichen Variablen effizient speichern und wiederherstellen können, bleibt somit eine technische Herausforderung.

4.3.3 Netzwerkarchitekturen

Quantenrepeater-Netzwerke bilden die Grundlage dieser Technologie. Ihr Ziel liegt darin, die Reichweite der Übertragung von Quanteninformation mittels Repeaterstationen zu erhöhen. Die Stationen werden in regelmäßigen Abständen entlang des Übertragungswegs platziert. Sie erzeugen lokal Verschränkung, speichern sie mittels Quantenspeicher und geben sie über Verschränkungsaustausch an die nächste Station weiter. Mittels dieser Verschränkungsaustausch-Operationen werden die Enden der einzelnen Abschnitte so miteinander verknüpft, dass schließlich verschränkte Quantenzustände zwischen den Endpunkten der Übertragungsstrecke zur Verfügung stehen. Quantenrepeater bieten durch Ende-zu-Ende-Verschränkung Sicherheit in Kommunikationsverbindungen über mehrere Knoten und weite Entfernungen hinweg. Außerdem ermöglichen sie eine sichere Vernetzung von Quantencomputern in Quantennetzwerken. Wie bei der QKD liegt der Fokus auch bei der Implementierung von Quantenrepeatern vor allem auf den Merkmalen Distanz und Schlüsselrate. Da diese Technologie noch in der Entwicklung ist, gibt es derzeit keine realisierten Strecken oder Schlüsselraten.

4.3.4 Stand der Forschung und Industrie

QKD-Demonstrationen und Teststrecken

Quantenrepeater gelten perspektivisch als tragende Säule für die sichere Kommunikation und die Verteilung von Quantenzuständen in Quantennetzwerken. Ihre Anwendungsfelder in der sicheren Kommunikation sind prinzipiell identisch zu denjenigen der Quantenschlüsselverteilung, mit dem Unterschied, dass der Quantenrepeater prinzipiell größere Distanzen ohne Rückgriff auf Ketten vertrauenswürdiger Knoten überbrücken kann. Aus diesen Gründen können sie einen wichtigen Beitrag zur Umsetzung der strategischen Ziele der IT-Sicherheitsforschung im Forschungsrahmenprogramm „Digital. Sicher. Souverän." leisten und die technologische Souveränität bei der abhörsicheren Kommunikation über große Distanzen gewährleisten. Vor diesem Hintergrund hat sich beispielsweise das derzeit durchgeführte Projekt „QR.X" zum Ziel gesetzt, die Verteilung und Speicherung von Verschränkung als Ressource für Quantenkommunikation und Quantennetzwerke zu untersuchen. Zu diesem Zweck werden optimierte Komponenten und modularisierte Geräte

entwickelt, Glasfaser-Teststrecken außerhalb der Laborumgebung eingerichtet und eine elementare Quantenrepeater-Verbindung unter realistischen Feldbedingungen demonstriert. [79]

Obwohl der Übergang von der Forschung zur kommerziellen Anwendung von QKD in einigen Nischenmärkten bereits gelungen ist, ist eine breite Verfügbarkeit für die Gesellschaft noch weit entfernt. So besteht weiterhin hoher Forschungsbedarf bei der Implementierung der physikalischen Prinzipien in feldtaugliche Anwendungen. Trotz innovativer Ansätze (wie z. B. Twin-Field-QKD) können fasergebundene Strecken von mehr als 1000 Kilometern nur über Ketten aus vertrauenswürdigen Knoten überwunden werden, deren Ende-zu-Ende-Sicherheit infolge der notwendigen Umwandlung von Quanteninformation in klassische Information an jedem Knotenpunkt begrenzt ist. Um quantensichere Kommunikation in Netzwerken jenseits von Punkt-zu-Punkt-Verbindungen zu realisieren, sind Quantenrepeater eine notwendige Voraussetzung.

QKD-Leistungsparameter

Auf dem Gebiet der Forschung wurden in den letzten Jahren bedeutende Fortschritte bei Demonstrationen grundlegender Quantenrepeater-Elemente erreicht. Diese beschränken sich jedoch aufgrund der großen technologischen Herausforderungen auf kurze Strecken bis zu zwei Knoten. So konnte beispielsweise die Verteilung von Verschränkung zwischen Quantenspeichern über Glasfaser über eine Distanz von ca. 500 Metern bis ca. 35 Kilometer gezeigt werden. [80–84] Außerdem wurde die Verteilung von Qubit-Telekom-Photon-Verschränkung über größere Faserdistanzen demonstriert, darunter eine Strecke von 101 Kilometern via Faserspule (Rubidium-Atom-Quantenspeicher) und 50 Kilometern über verlegte Fasern in einem Ballungsgebiet (Selten-Erd-Speicher). [85, 86] Ebenso wurde die Teleportation von quantenmechanischen Zuständen über größere Faserstrecken zwischen Photonen (ca. 64 km) sowie zwischen Quantenspeichern und Photonen (ca. fünf Kilometer) und Ionen (ca. 14 km) erfolgreich durchgeführt. [87–89] Im Rahmen von „QR.X" wurde erfolgreich eine Quantenrepeater-Zelle als zentrales Element eines Quantenrepeaters für die photonische Verschränkungsverteilung und Gatteroperationen an zwei Quantenspeichern demonstriert. [90, 91] Die am weitesten fortgeschrittene Demonstration eines komplexeren Quantennetzwerks aus drei Knoten wurde mit NV-Zentren in Diamant erreicht. Dabei wurden Verschränkungsverteilung zwischen den äußeren Knoten und Verschränkungsaustausch über den mittleren Knoten gezeigt. Auf dieser Grundlage konnte die Teleportation eines Quantenzustands zwischen den äußeren Knoten durchgeführt werden. [92] Zusätzlich wurden im „QR.X"-Konsortium analytische Modelle und Simulationen von Quantenrepeater-Strecken entwickelt, die realistische Parameter existierender Hardware-Komponenten aufgreifen. [93–96] Ähnliche Entwicklungen sind auch auf internationaler Ebene zu beobachten, wie zum Beispiel in einer Studie der TU Delft auf Basis modularer Simulationsumgebungen, die einen perspektivischen Quantenrepeater entlang der DemoQuanDT-Strecke Berlin-Bonn simuliert. [95, 97] Durch den Einsatz neuer verschränkungsassistierter Protokolle für klassische Kommunikation kann die Kommunikationsperformance verbessert und Angriffe auf IT-Infrastrukturen verhindert werden. [98] Für eine umfassende Übersicht über aktuelle theoretische Konzepte und experimentelle Fortschritte sei auf Azuma et al. verwiesen. [99]

QKD-Forschungsprojekte

Trotz stetiger Fortschritte stellt die Entwicklung von Quantenrepeatern und perspektivisch von Ende-zu-Ende-Quantennetzwerken eine enorme technische Herausforderung dar. Beispielsweise müssen Quantenzustände mit hoher Qualität erzeugt, zwischengespeichert und übertragen werden, zusätzlich sind zur Fehlerkorrektur und Güteverbesserung Gatteroperationen zwischen den Zuständen notwendig. Zudem bedarf es nicht nur der Forschung an Systemkomponenten, sondern auch der Entwicklung angepasster Protokolle. Und mit zunehmendem Entwicklungsstand von Quantenrepeatern müssen letztlich in Kooperation mit der Industrie Anwendungsperspektiven und -beispiele in den Blick genommen werden.

Im Rahmen des Forschungsverbunds „Quantenrepeater.Link (QR.X)“ konnten bereits wichtige Elemente eines Quantenrepeaters an Faserstrecken demonstriert werden. Dazu gehörten unter anderem die Qubit-Photon-Verschränkung über große Distanzen [86] sowie die Erzeugung von Verschränkung zwischen räumlich getrennten Qubits [82]. Auch im internationalen Kontext werden Forschungsaktivitäten zu Quantenkommunikation derzeit stark gefördert. Ein Beispiel hierfür ist die US-amerikanische „National Quantum Initiative“, die sich zum Ziel gesetzt hat, die Quantenforschung und -entwicklung für die wirtschaftliche und nationale Sicherheit der USA zu beschleunigen. [100] Daneben gibt es bereits eine Reihe an existierenden Forschungsnetzwerken. Auf akademischer Seite sind hier vor allem „Chicago Quantum Exchange“, [29] das „Brookhaven National Laboratory Quantum Network Facility (BNL)“ [30] und das Center for Quantum Networks [31] zu nennen. Auf industrieller Seite findet sich unter anderem das „AWS Center for Quantum Networking“. [32] In Asien wurde das Potenzial der Quantentechnologien ebenfalls längst erkannt und wird beispielsweise durch das japanische „Moonshot Research and Development Program“ gefördert, [101] das ein Forschungsnetzwerk zum Thema Quantenrepeater unterstützt. Mit der Inbetriebnahme des Beijing-Shanghai Backbone Network (BSBN) baut auch China seine Förderung der Quantenkommunikation weiter aus, mit dem Ziel der Erforschung eines globalen Quantennetzwerks. In Europa wird die Forschung zu Quantennetzwerken stark durch die „Quantum Internet Alliance (QIA)“ vorangetrieben, deren Ziel die Demonstration eines prototypischen Quanteninternets mit Integration aller Netzwerkebenen ist. [102]

Alle diese nationalen und internationalen Bemühungen zeigen, dass Quantenrepeater derzeit weltweit intensiv erforscht werden. Da sie im Prinzip „kleine Quantencomputer mit optischer Schnittstelle“ darstellen, ist der technische Aufwand jedoch außerordentlich. Weil jedoch nur mit dieser Methode Quantenzustände in einem Netzwerk verteilt werden können, ist ihr Nutzen zukünftig allerdings enorm.

5 Quantitative Analysen

5.1 Publikationsanalyse

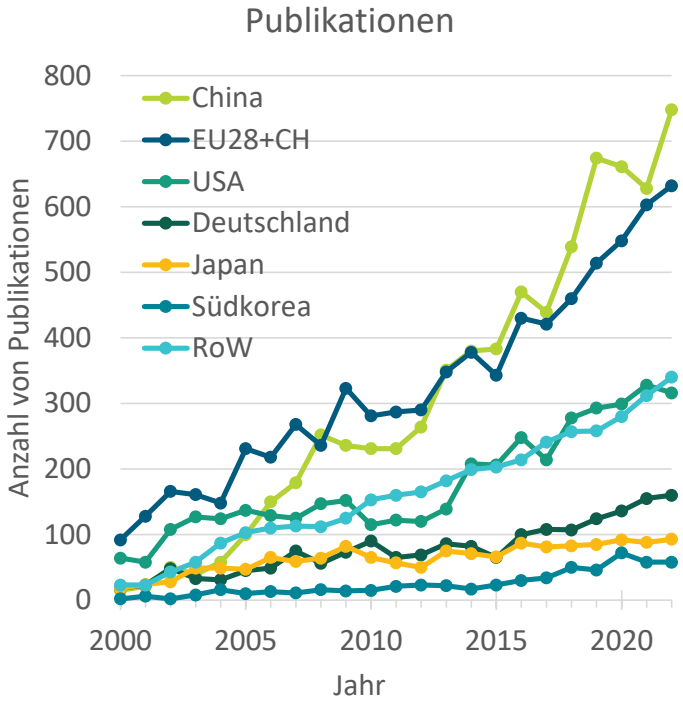
Wissenschaftliche Veröffentlichungen dokumentieren den wissenschaftlichen Fortschritt auf einem bestimmten Gebiet der Technik. Durch die Analyse ihrer Entwicklung können Trends in der wissenschaftlichen Tätigkeit sowie die wichtigsten Akteure in einem Bereich erfasst werden.

Wir berücksichtigten alle im Web of Science (WoS) gelisteten, von Expert:innen begutachteten Veröffentlichungen im Zeitraum von 2000 bis 2022 und verwendeten eine stichwortbasierte Suchstrategie (Details in Abschnitt 2).

Dynamik der Veröffentlichungen

Die Zahl der Veröffentlichungen zum Thema Quantenkommunikation ist in den letzten 20 Jahren deutlich und kontinuierlich gestiegen (Abbildung 1). Während im Jahr 2000 weltweit ca. 200 Publikationen zur Quantenkommunikation veröffentlicht wurden, waren es im Jahr 2022 bereits fast 2000. Die meisten Publikationen stammen von Autoren, die mit Instituten aus China verbunden sind, dicht gefolgt von der EU (EU28 + CH) und, mit etwa halb so vielen Publikationen, den USA. Weitere Länder mit einer relevanten Anzahl von Publikationen sind Japan, Südkorea (beide in Abbildung 1), Kanada, Indien, Russland, Australien und Singapur (alle unter "übrige Welt – RoW" in Abbildung 1).

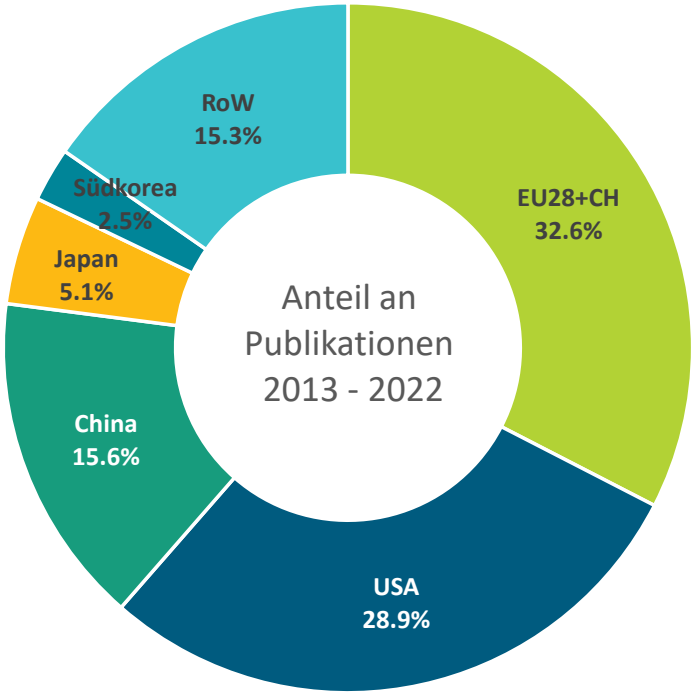
Abbildung 1: Begutachtete Veröffentlichungen zum Thema Quantenkommunikation in den Ländern mit der höchsten Anzahl von Veröffentlichungen von 2000 bis 2022.



Ländervergleich

Um die Publikationsaktivitäten in verschiedenen Ländern/Regionen zu vergleichen, wurden die Anzahl der Veröffentlichungen der letzten zehn Jahren des untersuchten Zeitraums addiert (2013-2022, Abbildung 2). China weist in diesem Zeitraum mit einem Patentanteil von 33 Prozent die höchste Publikationsaktivität auf, gefolgt von der EU mit 29 Prozent und den USA mit 16 Prozent. Deutschland trägt 7 Prozent zu den gesamten Publikations-Aktivitäten bei.

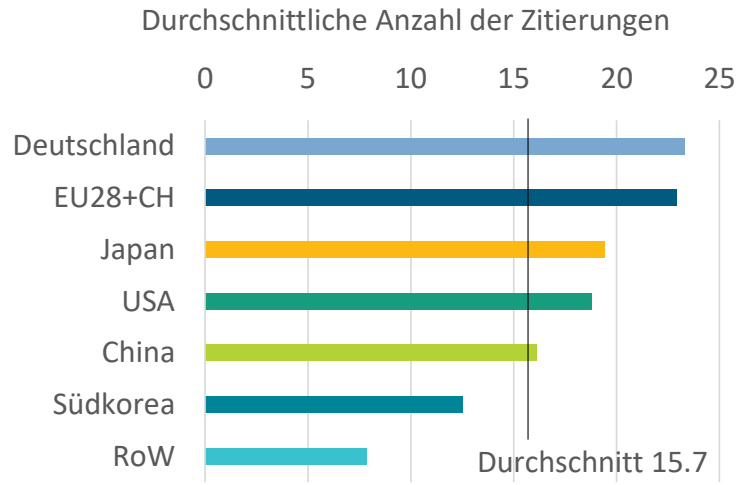
Abbildung 2: Anteil der QCom-bezogenen Veröffentlichungen der Länder mit der höchsten Anzahl von Veröffentlichungen (und der EU) in den letzten 10 Jahren des analysierten Zeitraums (2013-2022).



Die bloße Anzahl der Veröffentlichungen sagt jedoch wenig über die Relevanz und Qualität der Forschungsergebnisse und Erkenntnisse in diesen Publikationen aus. Um einen Eindruck der Relevanz der Publikationen zu erhalten, wurde die durchschnittliche Anzahl der Zitationen der QCom-bezogenen Publikationen aus dem Jahr 2019 in den verschiedenen Ländern analysiert (Abbildung 3). Publikationen aus der EU wurden im Durchschnitt 23-mal zitiert (gleiches gilt für Deutschland), jene aus Japan und den USA 19-mal, aus China 16-mal, aus Südkorea 13-mal und alle anderen Länder 8-mal. Der weltweite Durchschnitt lag bei 16 Zitationen pro Veröffentlichung.

Diese durchschnittlichen Zitationszahlen können nicht direkt mit der Qualität der Veröffentlichungen korreliert werden, da sie anfällig für Verzerrungen sind, z. B. in Bezug auf englischsprachige Fachzeitschriften mit hohem Impact-Faktor. Nichtsdestotrotz zeigen sie die Relevanz der veröffentlichten Ergebnisse für die jeweilige akademische Gemeinschaft und die hohe Qualität der QCom-Publikationen in Europa.

Abbildung 3: Durchschnittliche Anzahl der Zitierungen von QCom-bezogenen Veröffentlichungen aus verschiedenen Ländern (und der EU) aus Veröffentlichungen des Jahres 2019 (um die Zeitverzögerung der Zitate zu berücksichtigen).



Relevante Akteure

Eine Publikationsanalyse ermöglicht es, die relevanten Institutionen in einem bestimmten Bereich zu identifizieren. Tabelle 1 listet die Institutionen und Organisationen mit den meisten QCom-Publikationen in den letzten beiden Jahren des untersuchten Zeitraums auf. Es sei darauf hingewiesen, dass in dieser Tabelle sowohl Fördereinrichtungen (z. B. das Energieministerium der USA), Forschungsorganisationen (z. B. die Chinesische Akademie der Wissenschaften) als auch einzelne Institutionen (z. B. die University of Science and Technology of China) aufgeführt sind. Daher ist beim Vergleich verschiedener Organisationen und Einrichtungen darauf zu achten, dass die verschiedenen Ebenen nicht miteinander verwechselt werden. Die meisten Organisationen und Einrichtungen in der Liste stammen aus China (10), gefolgt von Europa (4, aus Frankreich, Deutschland und Spanien) und den USA (3).

Tabelle 1 Einrichtungen mit der höchsten Anzahl von QCom-bezogenen Veröffentlichungen in den Jahren 2021-2022 (Top-20):

Einrichtung (Land)	Anzahl der Publikationen (2021-22)
Chinese Academy of Sciences (CN)	248
University of Science Technology of China (CN)	174
Beijing University of Posts Telecommunications (CN)	105
Centre National de la Recherche Scientifique (FR)	98
Center for Excellence in Quantum Information Quantum Physics (CN)	94
Udice French Research Universities (FR)	80
Nanjing University of Posts Telecommunications (CN)	71
Central South University (CN)	70

Einrichtung (Land)	Anzahl der Publikationen (2021-22)
United States Department of Energy (US)	70
Russian Academy of Sciences (RU)	69
Shanxi University (CN)	63
Nanjing University (CN)	59
Tsinghua University (CN)	55
University of California System (US)	53
Indian Institute of Technology System (IN)	52
Max-Planck-Gesellschaft (DE)	52
University of Arizona (US)	47
University of the Chinese Academy of Sciences (CN)	47
National University of Singapore (SG)	44
Universitat Politecnica de Catalunya (ES)	44

Um die europäischen Aktivitäten im Bereich der QCom-Publikationen zu analysieren, haben wir die europäischen Institutionen mit mindestens 20 QCom-bezogenen Publikationen in den letzten zwei Jahren des untersuchten Zeitraums aufgelistet (Tabelle 2). Insgesamt haben 34 Einrichtungen aus der EU (EU28 + CH) mindestens 20 Beiträge in wissenschaftlichen Zeitschriften veröffentlicht. Die meisten Einrichtungen mit mindestens 20 Veröffentlichungen kommen aus Frankreich und dem Vereinigten Königreich, gefolgt von Deutschland, Spanien, Italien, Österreich und der Schweiz. Dies deutet auf eine breite F&E- und Wissensbasis an den Forschungseinrichtungen in Europa hin. Natürlich gibt es viele andere Einrichtungen, die sich mit QCom-F&E befassen und unter der hier gewählten Schwelle von 20 Veröffentlichungen liegen. Alle Einrichtungen aus Deutschland mit mindestens 10 QCom-bezogenen Publikationen in den Jahren 2021-2022 sind in Tabelle 3 aufgeführt.

Tabelle 2: Einrichtungen aus der EU28(+CH) mit mindestens 20 QCom-bezogenen Veröffentlichungen in den Jahren 2021-2022:

Einrichtung (Land)	Anzahl der Publikationen (2021-22)
Centre National de la Recherche Scientifique (FR)	98
Udice French Research Universities (FR)	80
Max-Planck-Gesellschaft (DE)	52
Universitat Politecnica de Catalunya (ES)	44
Österreichische Akademie der Wissenschaften (AT)	41
University of Cambridge (UK)	40

Einrichtung (Land)	Anzahl der Publikationen (2021-22)
Barcelona Institute of Science Technology (ES)	37
Consiglio Nazionale delle Ricerche (IT)	36
Delft University of Technology (NL)	36
Institut De Ciencies Fotoniques (ES)	36
Technische Universität München (DE)	35
Swiss Federal Institutes of Technology Domain (CH)	33
Sorbonne Universite (FR)	30
University of Bristol (UK)	29
Fahrenheit Union of Universities (PL)	28
Helmholtz-Gemeinschaft (DE)	28
Istituto Nazionale di Fisica Nucleare (IT)	28
Palacky-Universität Olomouc (CZ)	28
Technical University of Denmark (DK)	28
University of York (UK)	28
Universität Wien (AT)	27
University of Gdansk (PL)	26
University of Geneva (CH)	26
Fraunhofer Gesellschaft (DE)	24
Heriot Watt University (UK)	24
Polytechnic University of Milan (IT)	24
Universite Paris Saclay (FR)	24
Communaute Universite Grenoble Alpes (FR)	23
Universite Grenoble Alpes (FR)	23
Universität Innsbruck (AT)	22
ETH Zürich (CH)	21
Catalan Institution for Research and Advanced Studies (ES)	20
Imperial College London (UK)	20
University of Oxford (UK)	20

Tabelle 3: Einrichtungen aus Deutschland mit mindestens 10 QCom-bezogenen Veröffentlichungen in den Jahren 2021-2022:

Einrichtung (Land)	Anzahl der Publikationen (2021-22)
Max-Planck-Gesellschaft (DE)	52
Technische Universität München (DE)	35
Helmholtz-Gemeinschaft (DE)	28
Fraunhofer Gesellschaft (DE)	24
Münchner Zentrum für Quantenwissenschaften und -technologie (DE)	19
Technische Universität Berlin (DE)	15
Ruhr-Universität Bochum (DE)	14
Universität München (DE)	14
Heinrich-Heine-Universität Düsseldorf (DE)	12
Deutsches Zentrum für Luft- und Raumfahrt – DLR (DE)	11
Universität Ulm (DE)	11
Universität Siegen (DE)	11
Universität Stuttgart (DE)	11
Freie Universität Berlin (DE)	10
Friedrich-Schiller-Universität Jena (DE)	10
Ruprecht Karl Universität Heidelberg (DE)	10
Technische Universität Darmstadt (DE)	10
Technische Universität Dresden (DE)	10

5.2 Patentanalyse

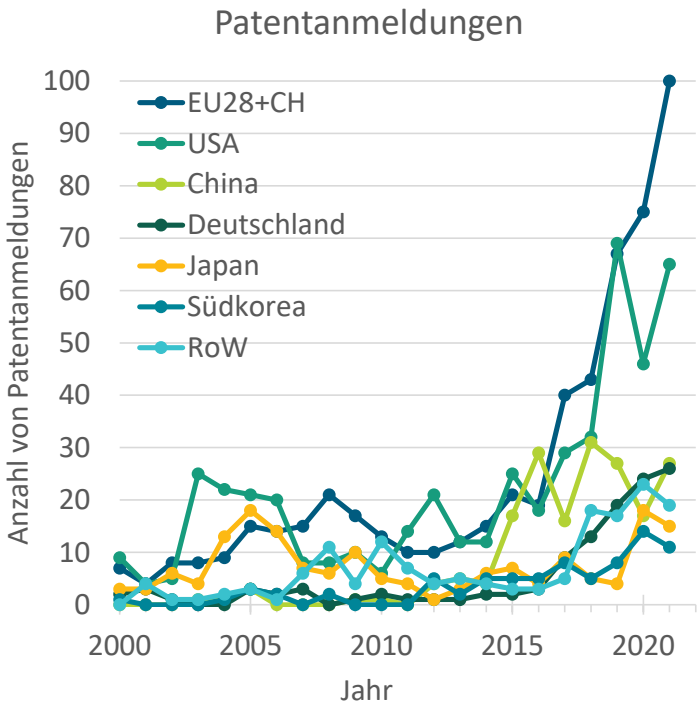
Patente deuten häufig auf ein kommerzielles Interesse an einem Technologiebereich hin. Die Analyse der Entwicklung der Patentierungsaktivitäten ist eine Möglichkeit, Trends des kommerziellen Interesses sowie die aktiven Akteure in diesem Bereich zu bewerten.

Für die Patentrecherche wurde eine Suchstrategie verwendet, die sowohl auf Patentklassifizierungscodes als auch auf einer Textsuche in Titel, Zusammenfassung und Ansprüchen basierte (Details siehe Abschnitt 2). Um einen fairen Vergleich zwischen den Ländern zu ermöglichen, wurde die Suche auf transnationale Patentanmeldungen beschränkt, d. h. Patentanmeldungen beim Europäischen Patentamt (EPA) oder bei der Weltorganisation für geistiges Eigentum (WIPO). Diese Patente konzentrieren sich auf Erfindungen mit einem hohen erwarteten kommerziellen Wert.

Dynamik der Patentanmeldungen

Abbildung 4 zeigt die Anzahl der QCom-bezogenen Patentanmeldungen zwischen 2000 und 2021 aus verschiedenen Ländern (und der EU). Insgesamt ist ein starker Anstieg der Patentierungsaktivitäten (von weniger als 20 im Jahr 2000 auf mehr als 200 im Jahr 2021) zu beobachten, insbesondere seit 2014. Die meisten Patentanmeldungen kommen aus der EU (EU28 und CH), gefolgt von den USA und China. Andere Länder mit einer relevanten Patentaktivität sind Japan und Südkorea (beide in Abbildung 4), Kanada, Russland, Singapur, Australien und Indien (alle unter "übrige Welt – RoW" in Abbildung 4).

Abbildung 4: QCom-bezogene transnationale Patentanmeldungen der Länder mit den meisten Patentanmeldungen (und der EU) von 2000 bis 2021.

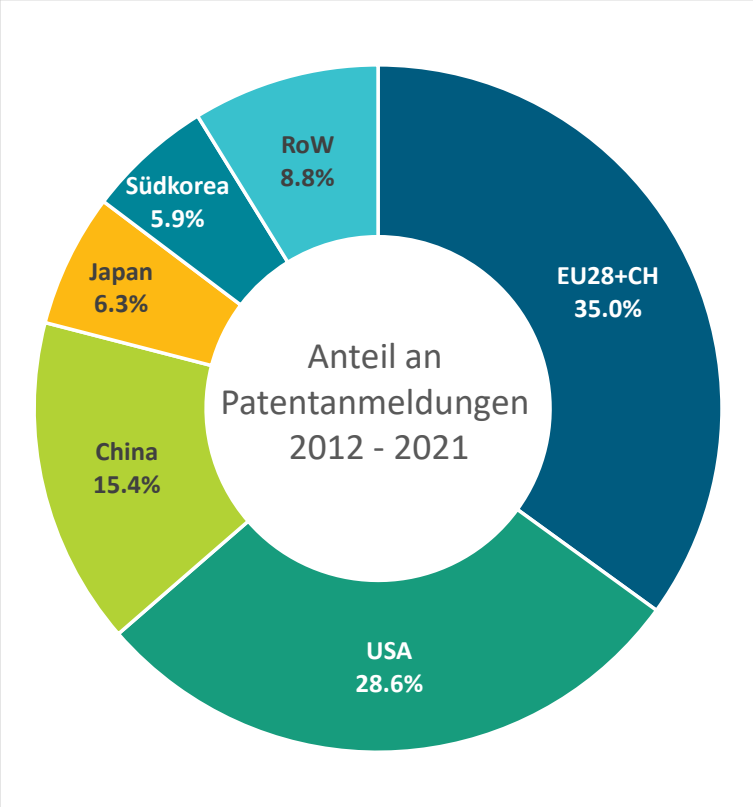


Ländervergleich

Um die Patentierungsaktivitäten in verschiedenen Ländern/Regionen zu vergleichen, haben wir die Anzahl der Patentanmeldungen von Einrichtungen in den verschiedenen Ländern in den letzten zehn Jahren des untersuchten Zeitraums (2012-2021) aufaddiert (Abbildung 5). Die EU weist mit

einem Patentanteil von 35 Prozent die höchste Patentaktivität auf, gefolgt von den USA mit 29 Prozent und China mit 15 Prozent. Deutschland trägt 9 Prozent zu den gesamten Patentanmeldungen bei.

Abbildung 5: Anteil der QCom-bezogenen transnationalen Patentanmeldungen der Länder mit den meisten Patentanmeldungen (und der EU) in den letzten 10 Jahren des analysierten Zeitraums (2012-2021).



Es sei darauf hingewiesen, dass diese Zahlen nicht unbedingt das tatsächliche kommerzielle Interesse an QCom-Technologien widerspiegeln, da sich Unternehmen möglicherweise bewusst gegen eine Patentierung entscheiden, da sie potenziellen Konkurrenten keine Informationen über ihre Systeme preisgeben wollen. Außerdem ist die Entwicklungsdynamik derzeit sehr hoch, sodass neue Generationen von QCom-Systemen innerhalb der Zeit entwickelt werden, die für die Veröffentlichung eines Patents benötigt wird, was dessen Schutzwert verringert. Hinzu kommt, dass sichere Kommunikationstechnologien und ihre Verwendung durch offizielle Institutionen stark reguliert sind und die Einfuhr solcher Technologien von den nationalen Behörden verboten werden könnte. Dies könnte sich in einem größeren Interesse an nationalen Patenten als an transnationalen Patenten niederschlagen.

Relevante Akteure

Der Bereich der QCom wird nach wie vor weitgehend von der Forschung und Entwicklung sowohl in der Industrie als auch in Forschungsorganisationen/Universitäten vorangetrieben. Die Analyse der Institutionen mit den meisten Patentanmeldungen in den Jahren 2018-21 zeigt, welche Unternehmen im Bereich QCom besonders aktiv sind und welche Universitäten und Forschungseinrichtungen in der angewandten Forschung zu diesen Themen tätig sind. Tabelle 4 listet die 20 Institutionen mit der höchsten Anzahl an QCom-bezogenen Patentanmeldungen in den letzten vier Jahren des analysierten Zeitraums auf. Die höchste Patentaktivität ist bei Technologieunternehmen

(einschließlich Intel, Arquit, Huawei, LG Electronics, Toshiba und QuantumCTek), großen Telekommunikationsanbietern (einschließlich Deutsche Telekom und British Telecom) und Forschungseinrichtungen/Organisationen (einschließlich MIT, Fraunhofer, Delft University of Technology und South China Normal University) zu verzeichnen. Vor allem große, internationale Technologieunternehmen neigen dazu, ihre Forschung und Entwicklung durch Patente zu schützen, weshalb sie in dieser Liste gut vertreten sind. Start-ups hingegen legen ihren (finanziellen und personellen) Schwerpunkt oft auf die Technologieentwicklung und tauchen daher in solchen Analysen nicht oder nicht so prominent auf.

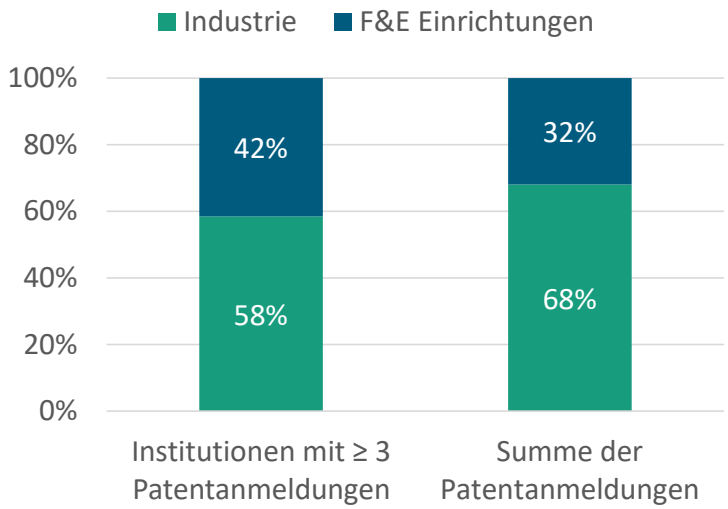
Tabelle 4 Institutionen mit der höchsten Anzahl von QCom-bezogenen, transnationalen Patentanmeldungen in den Jahren 2018-2021 (Top-20):

Einrichtung (Land)	Anzahl der Patentanmeldungen (2018-21)
Intel (US)	24
Deutsche Telekom (DE)	23
Arqit (GB)	20
Huawei Technologies Düsseldorf (DE)[3]	20
LG Electronics (KR)	20
Toshiba (JP)	18
British Telecom (GB)	14
QuantumCTek (CN)	14
Huawei Technologies (CN)	12
MIT (US)	12
Ericsson (SE)	12
Fraunhofer (DE)	11
IBM (US)	11
PsiQuantum (US)	11
Eagle Technology (US)	10
Delft University of Technology (NL)	10
Corning (US)	9
ID Quantique (CH)	9
Microsoft (US)	9
South China Normal University (CN)	9

[3] Patente werden auf Unternehmensebene und nicht auf der Ebene der Muttergesellschaft vergeben werden.

Mehr als 40 Prozent der Einrichtungen mit mindestens drei QCom-bezogenen Patentanmeldungen zwischen 2018 und 2021 sind Forschungseinrichtungen (Abbildung 6). Diese sind auch für mehr als 30 Prozent der Patentanmeldungen von Einrichtungen mit drei oder mehr QCom-Patenten in diesem Zeitraum verantwortlich. Dies unterstreicht das frühe Entwicklungsstadium der QCom-Technologien, in dem F&E-Einrichtungen eine wichtige Rolle bei der Technologieentwicklung spielen.

Abbildung 6: Anteile der Industrie und Forschungseinrichtungen mit ≥ 3 QCom-bezogenen Patentanmeldungen zwischen 2018 und 21 und ihre Anteile an der Summe der Patentanmeldungen in diesem Zeitraum.



Um die europäischen Aktivitäten im Bereich der QCom-Patentierung zu analysieren, wurden alle europäischen Institutionen mit mindestens drei QCom-bezogenen Patentanmeldungen in den letzten vier Jahren des untersuchten Zeitraums aufgelistet (Tabelle 5). Auch hier sind Technologieunternehmen (einschließlich Arqit, Ericsson, ID Quantique, Terra Quantum, Thales und Nokia) und große Telekommunikationsanbieter (einschließlich Deutsche Telekom und British Telecom) gut vertreten. In Europa werden die QCom-bezogenen Patentaktivitäten jedoch mehr als weltweit von Forschungseinrichtungen/Organisationen vorangetrieben (u. a. Fraunhofer, Delft University of Technology, Netherlands Organization for Applied Scientific Research – TNO, Österreichische Akademie der Wissenschaften, Centre National de la Recherche Scientifique – CNRS, CEA, Fundació Institut de Ciències Fotòniques – ICFO, und Max-Planck-Gesellschaft). Mehr als die Hälfte der Institutionen mit mindestens drei QCom-bezogenen Patentanmeldungen sind Forschungseinrichtungen/Organisationen. Diese sind jedoch nur für ein Drittel der Patentanmeldungen der Institutionen mit drei oder mehr QCom-Patenten verantwortlich. Dies bedeutet, dass in Europa viele F&E-Einrichtungen aktiv an QCom arbeiten, aber in Bezug auf die Patentzahlen nicht mit den Telekommunikations- und Technologieunternehmen mithalten können.

Tabelle 5: Institutionen aus EU28(+CH) mit mindestens drei QCom-bezogenen, transnationalen Patentanmeldungen zwischen 2018 und 2021:

Einrichtung (Land)	Anzahl der Patentanmeldungen (2018-21)
Arqit (UK)	20
Huawei Technologies Düsseldorf (DE)	20
British Telecom (UK)	14
Ericsson (SE)	12
Fraunhofer (DE)	11
Delft University of Technology (NL)	10
ID Quantique (CH)	9
Terra Quantum (CH)	6
Thales (FR)	6
Netherlands Organization for Applied Scientific Research (NL)	5
Österreichische Akademie der Wissenschaften (AT)	5
Centre National de la Recherche Scientifique (FR)	4
CEA (FR)	4
Element Six (UK)	4
Fundació Institut de Ciències Fotòniques (ES)	4
Max-Planck-Gesellschaft (DE)	4
Österreichisches Institut für Technologie GmbH (AT)	3
Nokia Technologies Oy (FI)	3
University of Geneva (CH)	3
University of Warsaw (PL)	3
University of York (UK)	3
VTT Technical Research Centre of Finland Ltd (FI)	3

5.3 Meta-Marktanalyse

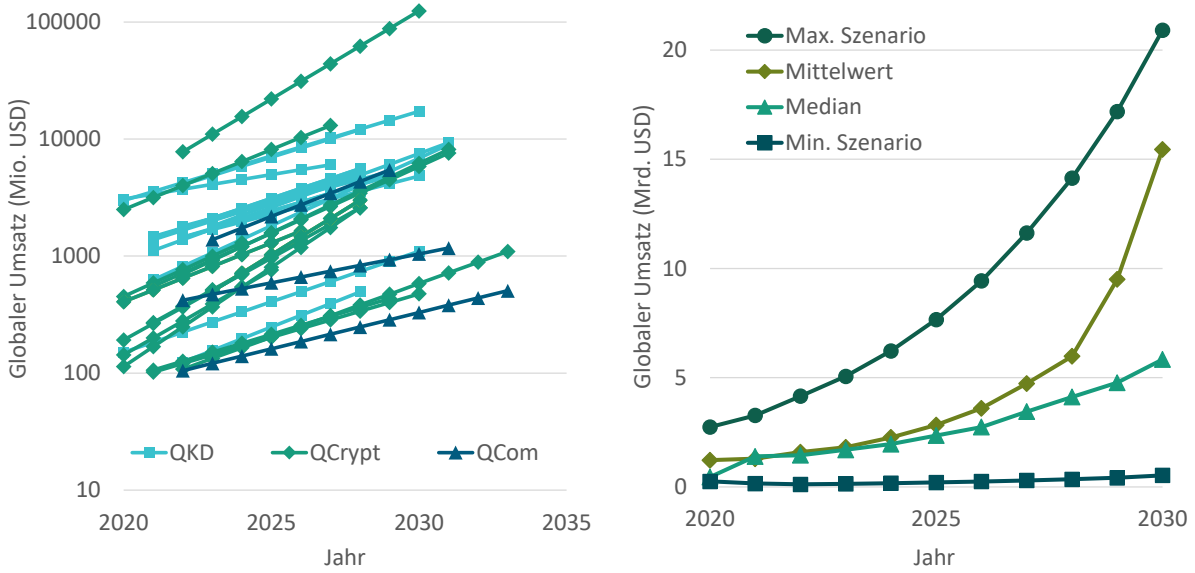
Die Bewertung der globalen Marktgröße eines aufstrebenden Technologiefeldes ist sehr schwierig. Im Gegensatz zu etablierten Märkten, die oft von großen Akteuren dominiert und von Fachverbänden eng begleitet werden, werden die Aktivitäten in aufstrebenden Märkten in der Regel von kleinen Unternehmen, Start-ups und F&E-Einrichtungen vorangetrieben. Dies macht eine realistische Einschätzung des Weltmarktes schwierig.

Um dieses Thema zu behandeln, wurden die (teils stark voneinander abweichenden) Ergebnisse von Marktberichten und Prognoseszenarien verglichen (Meta-Marktanalyse). Der Zugang zu kommerziellen Marktstudien ist in der Regel kostenintensiv, was die Möglichkeiten für vergleichende Analysen einschränkt. Viele Anbieter von Marktstudien geben jedoch begrenzte Informationen zu Werbezwecken frei, die kostenlos erhältlich sind. Diese öffentlich zugänglichen Informationen umfassen in der Regel aggregierte Umsatzdaten, Prognosen zu den Wachstumsraten und die Namen der relevanten Unternehmen in diesem Bereich. Für diesen Bericht wurden relevante Daten aus 68 Marktstudien gesammelt und analysiert, die zwischen 2019 und Juli 2023 zu Quantenkommunikation, Quantenkryptografie und Quantenschlüsselverteilung veröffentlicht wurden. [103–170]

Marktgröße und prognostizierte Trends

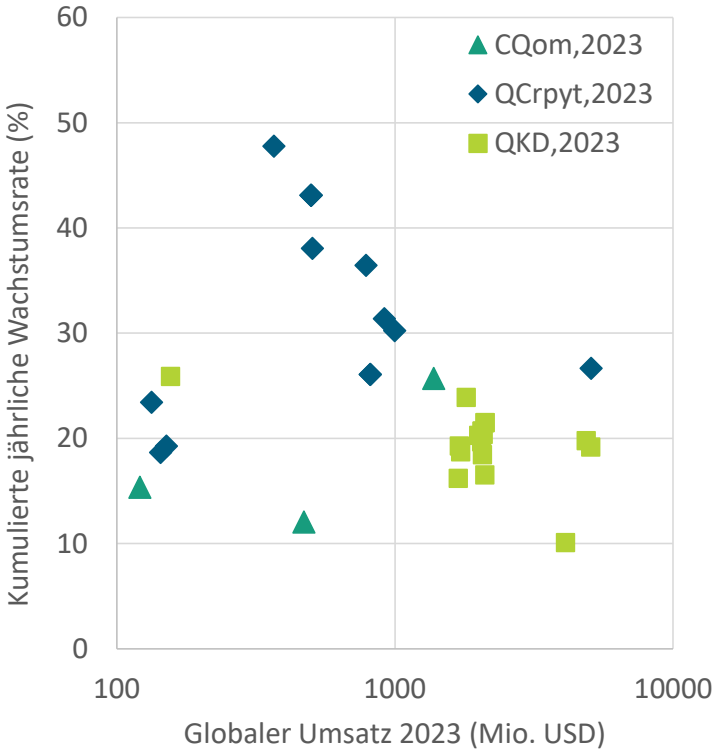
Den analysierten Marktberichten zufolge werden die weltweiten Umsätze auf den Märkten für Quantenkommunikation (QCom), Quantenkryptografie (QCrypt) und Quantenschlüsselverteilung (QKD) in den kommenden Jahren voraussichtlich deutlich wachsen (Abbildung 7). Es werden kumulierte jährliche Wachstumsraten (CAGR) zwischen 12 und 41 Prozent prognostiziert, wobei die Mehrzahl der Studien CAGRs zwischen 15 und 25 Prozent erwartet. Die prognostizierten und aktuellen Umsatzzahlen unterscheiden sich erheblich zwischen den Marktberichten und liegen zwischen 120 Millionen und 11 Milliarden USD im Jahr 2023 und zwischen 330 Millionen und 124 Milliarden im Jahr 2030 (linke Grafik in Abbildung 7). Diese Extremwerte können als eher unrealistisch angesehen werden, und insbesondere die höchsten Schätzungen erscheinen für eine so neuartige Technologie unrealistisch hoch. Um einen guten Überblick über all diese Umsatzprognosen zu erhalten, wurden der Median, der Durchschnitt sowie ein Maximal- und ein Minimalszenario berechnet (Median der oberen 4 bzw. der unteren 4, rechte Graphik von Abbildung 7). Die Berechnung des Medians ergibt globale Umsätze in Höhe von 1,7 Milliarden im Jahr 2023, die bis 2030 auf 5,8 Milliarden ansteigen. Die künftige Entwicklung wird wahrscheinlich zwischen der höchsten und der niedrigsten Vorhersage liegen, möglicherweise in der Nähe der Mittelwert- oder Mediankurve.

Abbildung 7: Umsatzdaten aus den 68 analysierten Marktstudien über den globalen Quantenkommunikationsmarkt zwischen 2020 und 2035 (links) und Ergebnisse eigener Berechnungen (rechts).



Die analysierten Marktberichte beziehen sich auf die Quantenkommunikation, die Quantenkryptografie bzw. die Quantenschlüsselverteilung. Diese Technologieklassen sind sicherlich nicht identisch und QKD kann als eine Unterklasse der beiden anderen betrachtet werden. In den meisten Marktberichten wird jedoch keine klare Definition der Technologieklasse gegeben – zumindest nicht in den kostenlosen Vorschauen. In jedem Fall scheinen die globalen Marktprognosen der drei Klassen sehr ähnlich zu sein, und weder die Umsatzzahlen noch die CAGR-Werte lassen eine klare Unterscheidung zwischen ihnen zu (Abbildung 8).

Abbildung 8: Vergleich der weltweiten Umsatzschätzungen und kumulierter jährlicher Wachstumsraten aus den analysierten Marktberichten über Quantenkommunikation (QCom), Quantenkryptografie (QCrypt) und Quantenschlüsselverteilung (QKD). Anhand der Prognosezahlen kann keine klare Unterscheidung zwischen den drei Technologieklassen getroffen werden.



Relevante Akteure und Länder

Die meisten Anbieter von Marktstudien erwähnen in der Vorschau ihres Berichts Unternehmen, die im Bereich der Quantenkommunikation, Quantenkryptografie oder Quantenschlüsselverteilung tätig sind. Die Analyse der in den 68 Studien erwähnten Unternehmen führt zu einem Ranking der genannten Firmennamen (Tabelle 6). Diese Analyse gibt keinen Aufschluss darüber, welches Unternehmen führend oder am aktivsten in diesem Bereich ist, sondern vielmehr darüber, welche Unternehmen von den Marktanalysten als relevant angesehen und dementsprechend in ihren Marktberichten erwähnt werden. Sie hat auch die Einschränkung, dass sie nur englischsprachige Marktstudien berücksichtigt. Daher werden nur Unternehmen mit öffentlich zugänglichen Informationen in englischer Sprache eine signifikante Anzahl von Erwähnungen aufweisen, da die meisten Marktberichtsanbieter ihre Suche nicht über die englische Sprache hinaus ausdehnen.

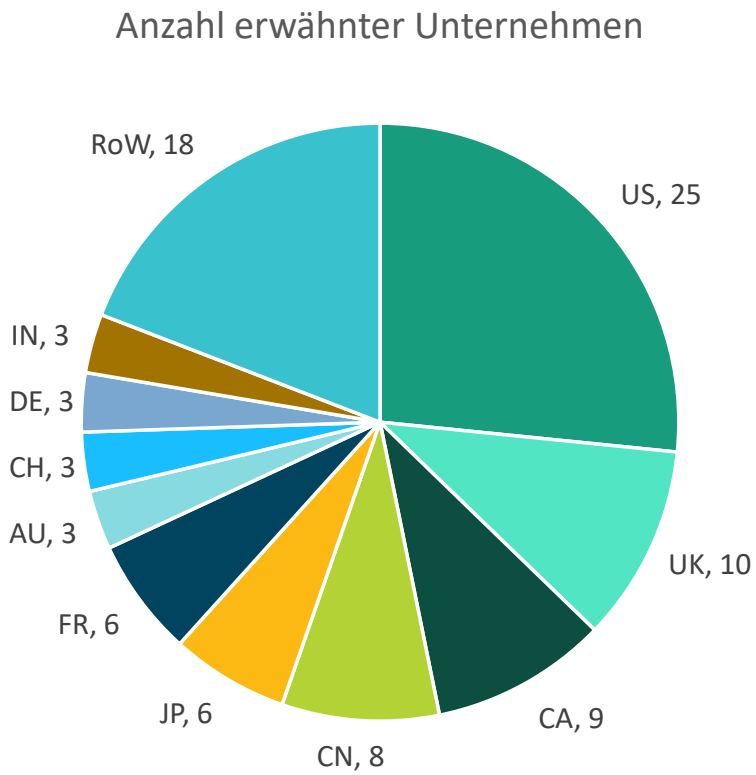
Tabelle 6: Unternehmen mit der höchsten Anzahl von Erwähnungen in Marktstudien über QKD, QCom und QCrypt (Top-20):

Unternehmen/Institution (Land)	Anzahl der Erwähnungen
MagiQ Technologies (US)	65
Quintessence Labs (AU)	60

Unternehmen/Institution (Land)	**Anzahl der Erwähnungen**
ID Quantique (CH)	60
Toshiba (JP)	58
Qasky (CN)	51
QuantumCTek (CN)	48
SeQureNet (FR)	29
Qubitekk (US)	28
Crypta Labs (UK)	25
NuCrypt (US)	24
IBM (US)	21
PQ Solutions (UK)	21
NEC (JP)	21
Qudoor (CN)	19
Infineon (DE)	18
Quantum Xchange (US)	15
HP (US)	14
Qutools (DE)	14
ISARA (CA)	14
Mitsubishi (JP)	13

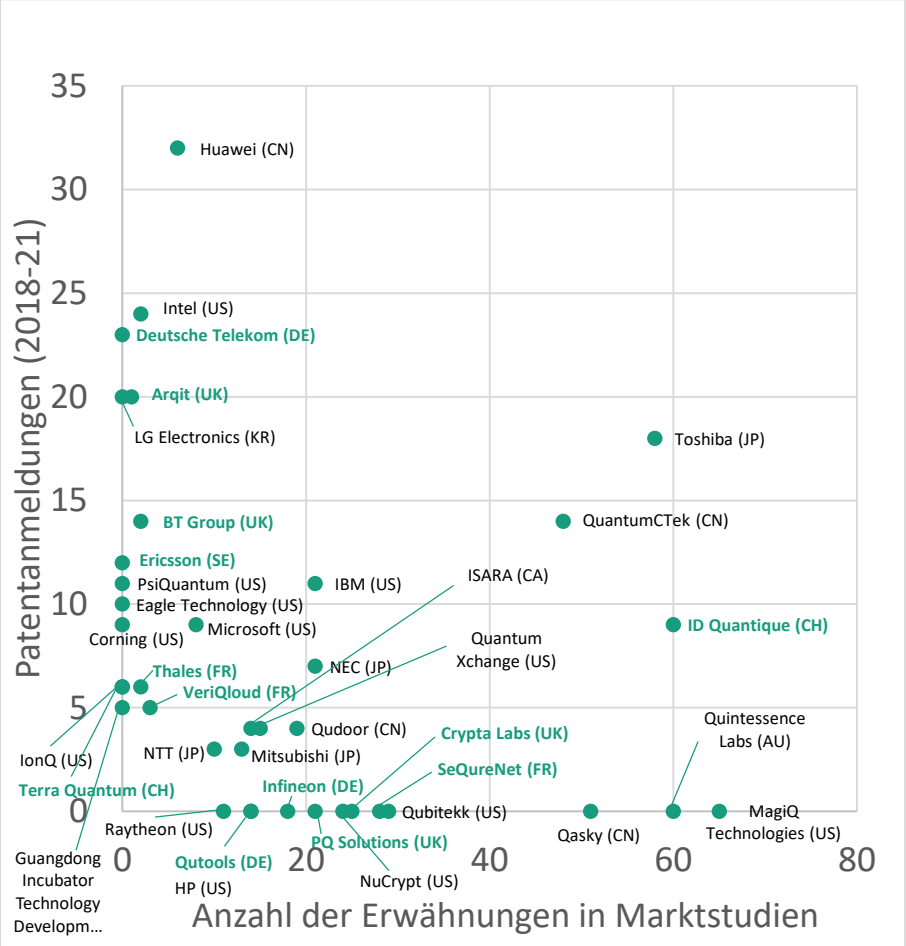
Betrachtet man das Herkunftsland der genannten Unternehmen, so kommen die meisten aus den USA (25), dem Vereinigten Königreich (10) und Kanada (9), gefolgt von China (8), Japan (6) und Frankreich (6) (Abbildung 9). Die Dominanz der Unternehmen aus englischsprachigen Ländern weist erneut auf eine Bevorzugung englischsprachiger Unternehmen hin.

Abbildung 9: Anzahl der in den analysierten Marktberichten erwähnten Unternehmen nach Herkunftsland.



Im Gegensatz zur Patentaktivität der Unternehmen spiegeln ihre Erwähnungen in Marktstudien wider, wie ihre Aktivitäten auf dem Gebiet der Technologie von anderen wahrgenommen werden. Abbildung 10 vergleicht die Anzahl der Erwähnungen mit der Patentaktivität der betreffenden Unternehmen. Es ist überraschend, dass die fünf größten Patentanmelder Huawei, Intel, Deutsche Telekom, LG Electronics und Arqit in den analysierten Marktstudien nicht häufig (und einige überhaupt nicht) erwähnt werden. Im Gegensatz dazu tauchen einige der häufig genannten Unternehmen wie MagiQ Technologies, Quintessence und Qasky in unserer Patentanalyse nicht auf. Toshiba, QuantumCTek und ID Quantique sind die Unternehmen, die sowohl eine signifikante Patentaktivität als auch häufige Erwähnungen in den Marktstudien aufweisen.

Abbildung 10: Vergleich der Anzahl der Patentanmeldungen und der Anzahl der Erwähnungen in Marktstudien von Unternehmen mit mindestens 10 Erwähnungen oder mindestens 5 Patentanmeldungen (europäische Unternehmen sind grün hervorgehoben).



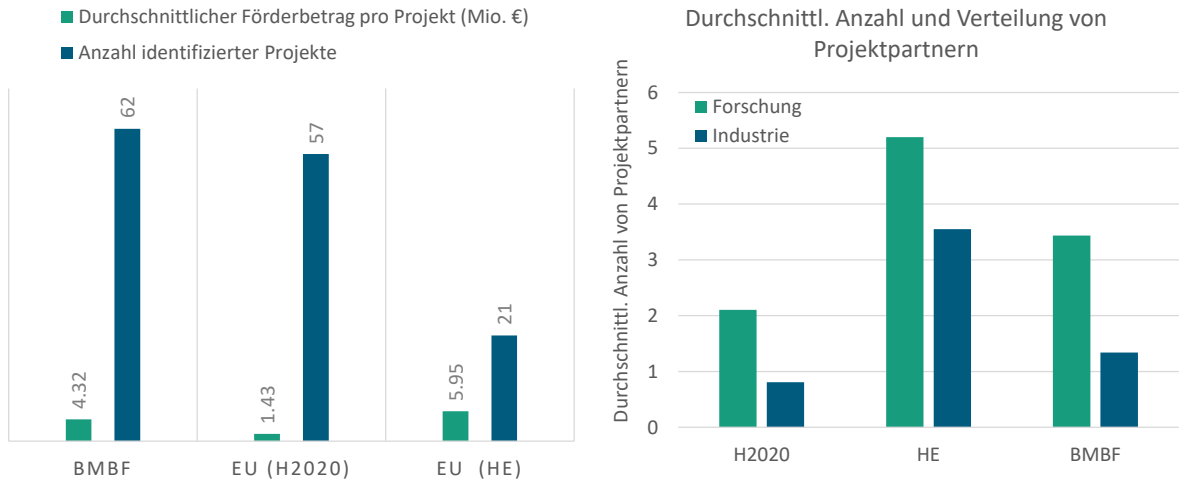
5.4 Projekt-Monitoring

Projekte, die in einem Wissenschafts- oder Technologiebereich durchgeführt werden, gelten als guter Indikator für laufende Forschungs- und Innovationaktivitäten, Forschungs- und Industrietrends sowie für die Innovationspolitik in einem Land oder einer Region. Dementsprechend wurden die jüngsten geförderten Projekte im Bereich der Quantenkommunikation als quantitatives Maß für die Technologielandschaft untersucht. Für diesen Bericht wurden Analysen für Deutschland und die EU durchgeführt.

Das Verständnis der deutschen F&I-Landschaft im Bereich der Quantenkommunikation ist für die Ziele dieses Monitoring-Berichts von großer Bedeutung. Darüber hinaus ist Deutschland ein führendes Land in der Forschung und Innovation in Europa und auf der ganzen Welt. Dementsprechend geben die F&E-Programme im Bereich der Quantenkommunikation in Deutschland einen guten Hinweis auf den Umfang und das Ausmaß der entsprechenden Aktivitäten in technologisch fortgeschrittenen Ländern auf globaler Ebene. Die Gesamtausgaben für F&E in Deutschland beliefen sich im Jahr 2021 auf rund 113 Milliarden Euro, was mehr als 3 Prozent des Bruttoinlandsprodukts (BIP) des Landes entspricht. [171] Die Bundesregierung stellte davon 22 Milliarden Euro zur Verfügung, von denen 12 Milliarden Euro vom Bundesministerium für Bildung und Forschung (BMBF) bereitgestellt wurden. Das BMBF ist eine der wichtigsten F&I-Förderorganisationen in Deutschland und vergibt oft den größten Anteil der F&E-Ausgaben des Bundes. Aus diesem Grund wurden in dieser Studie BMBF-geförderte Projekte im Bereich der Quantenkommunikation für die Analyse ausgewählt.

Die EU wurde als führender Forschungsförderer auf globaler Ebene ausgewählt, der mit seinen verschiedenen Forschungsrahmenprogrammen und Förderprogrammen umfangreiche F&I-Aktivitäten und -Initiativen unterstützt. Für das Jahr 2021 wurden die Gesamtausgaben der EU für Forschung und Entwicklung mit rund 328 Milliarden Euro angegeben, was 2,27 Prozent des BIP der Union entspricht. [172] Wir haben die wichtigsten EU-Förderprogramme für Forschung und Innovation, d. h. Horizont 2020 und Horizont Europa, auf ihre Projekte im Bereich der Quantenkommunikation hin untersucht.

Abbildung 11: Anzahl und durchschnittliche Finanzierung pro Projekt der identifizierten BMBF- und EU-Projekte (links). Durchschnittliche Anzahl der Projektpartner aus Industrie und Forschungseinrichtungen (rechts).



Wir haben 62 vom BMBF geförderte Projekte im Bereich der Quantenkommunikation identifiziert sowie 57 Projekte und 21 Projekte, die durch die EU-Rahmenprogramme Horizont 2020 (H2020)

bzw. Horizont Europa (HE) gefördert werden (Abbildung 11, links). Die identifizierten BMBF-Projekte haben Startzeiten von 2017 bis Mitte 2023 und Endzeiten von 2019 bis 2026. Der durchschnittliche BMBF-Beitrag pro Projekt beträgt rund 4,32 Millionen. Die im Rahmen von H2020 (2014-2020) geförderten EU-Projekte begannen im Zeitraum 2015-2021 und enden 2026, wobei die durchschnittlichen EU-Ausgaben pro Projekt bei 1,43 Millionen Euro liegen. Das HE-Programm (2021-2027) umfasst nur die Projekte, die im Rahmen der in den Jahren 2021 und 2022 durchgeführten Aufforderungen zur Einreichung von Vorschlägen finanziert wurden. Diese Projekte begannen 2022 oder 2023 und enden 2027 mit einem durchschnittlichen EU-Beitrag pro Projekt von 5,95 Millionen Euro. Sowohl für das BMBF als auch Horizont Europa können im Jahr 2023 nach dem Stichtag unserer Analyse (Juli 2023) weitere Projekte gefördert werden.

Sowohl in den BMBF- als auch in den EU-Programmen kommen die Projektteilnehmer häufiger aus Hochschulen und Forschungs- und Technologieorganisationen (Abbildung 11, rechts). Im Durchschnitt war an den von BMBF und von H2020 geförderten Projekten jeweils ein Teilnehmer aus der Industrie beteiligt. Für die kurze Laufzeit seit Beginn des HE-Programms wird für jedes Projekt eine höhere Anzahl von Teilnehmern gemeldet, darunter im Durchschnitt mehr als drei Partner aus der Industrie.

Abbildung 12: Verteilung der Projekte und geschätzte Finanzierung pro Jahr.

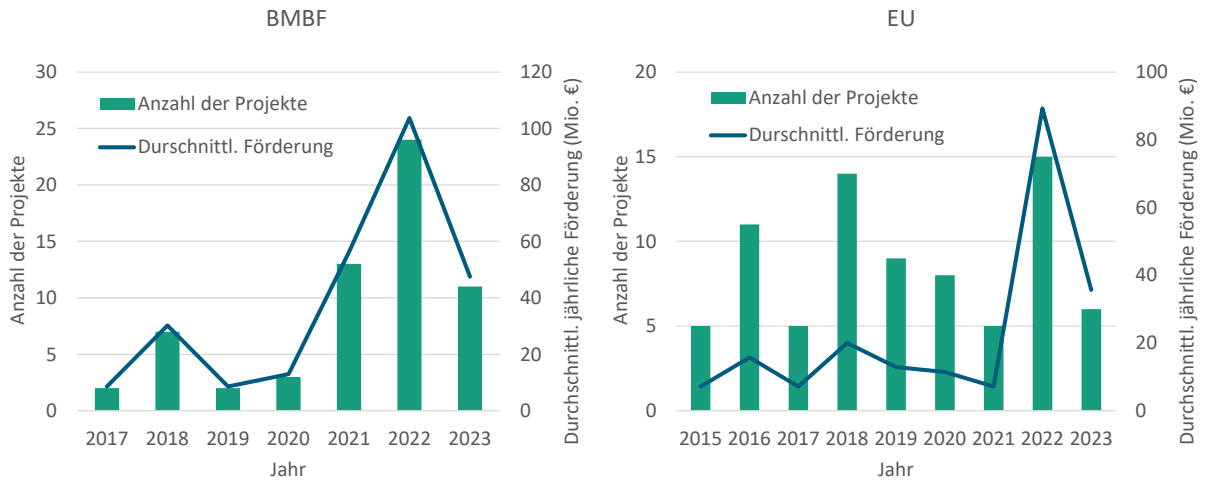
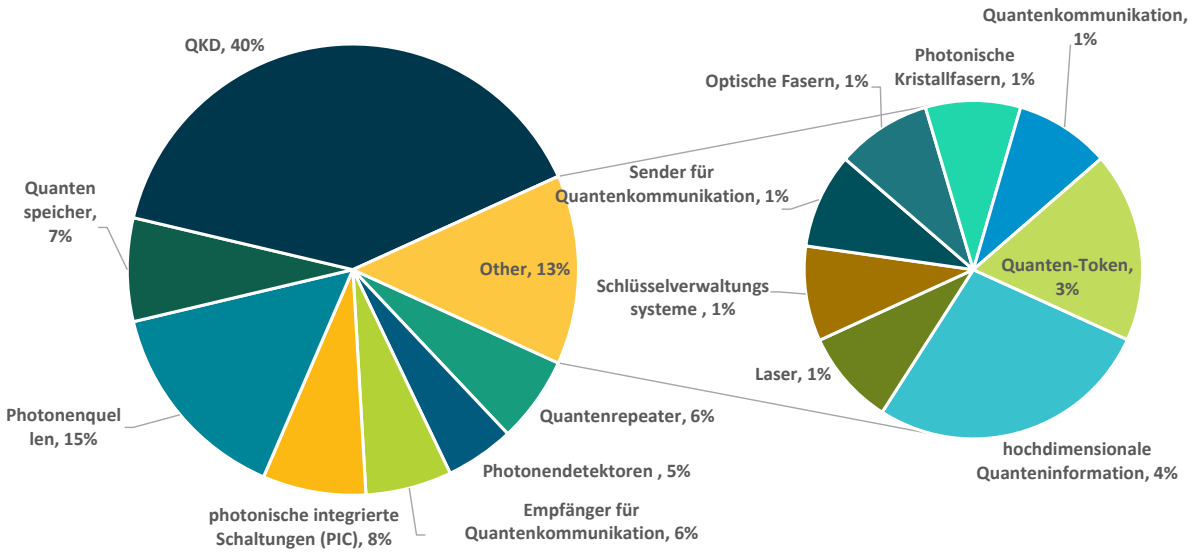


Abbildung 12 zeigt die Anzahl der geförderten Projekte und eine Schätzung des zugewiesenen Budgets basierend auf der durchschnittlichen Förderung pro Projekt seit 2015 und 2017. Es ist zu erkennen, dass die Anzahl der vom BMBF geförderten Projekte und dementsprechend die jährlichen Investitionen seit 2021 gestiegen sind. Ein ähnliches Muster lässt sich für den Start des HE-Programms mit einem Anstieg der Anzahl der Projekte im Jahr 2022 und einem stark wachsenden durchschnittlichen Projektbudget im Vergleich zu H2020 beobachten. Der Rückgang der Anzahl der Projekte und der durchschnittlichen Finanzierung im Jahr 2023 ist hauptsächlich darauf zurückzuführen, dass die gemeldeten Werte nur die erste Jahreshälfte umfassen. Es wird erwartet, dass sich der Trend der erhöhten Investitionen in F&I-Aktivitäten im Bereich der Quantenkommunikation im Jahr 2023 fortsetzt.

Es wurde auch eine Analyse der Themen der in Deutschland und der EU geförderten Quantenkommunikationsprojekte durchgeführt. Abbildung 13 zeigt die Verteilung der Themen, die von den identifizierten BMBF-Projekten behandelt werden. Die meisten Projekte konzentrieren sich auf ein Thema, während eine kleine Anzahl von Projekten entsprechend der angegebenen Ziele und Ansätze zwei Themen behandelt.

Abbildung 13: Verteilung der Themen in den 62 identifizierten, vom BMBF geförderten Projekten.



Wie die Abbildung zeigt, befasst sich ein großer Teil (40 %) der Projekte mit QKD-Themen. Zu den wichtigsten Unterthemen gehören QKD-Netzwerke (44 % der QKD-Projekte), Freistrahl-QKD (25 % der QKD-Projekte), allgemeines QKD (22 % der QKD-Projekte) und QKD-Nachbearbeitung. Photonenquellen, photonische integrierte Schaltungen (engl. photonic integrated circuit - PIC), Quantenspeicher, Quantenrepeater und Photonendetektoren machen etwa 5 bis 15 Prozent der identifizierten Projekte aus. Themen wie hochdimensionale Quanteninformation, Quanten-Token, allgemeine Konzepte der Quantenkommunikation, Schlüsselverwaltungssysteme usw. werden in einer kleinen Anzahl von Projekten (1 bis 4 %) behandelt.

Abbildung 14 zeigt die Verteilung der Themen in den identifizierten EU-Projekten, die im Rahmen von H2020 finanziert werden. Wie die Abbildung zeigt, machen Quantennetzwerke, Photonenquellen und QKD zusammen mehr als die Hälfte der von H2020-Projekten behandelten Themen aus. Die zweite Gruppe von Themen umfasst Quantenspeicher, Protokolle und Zertifizierung, theoretische Themen, Quantenzufallszahlengeneratoren (engl. quantum random number generator – QRNG), Quantenrepeater, Photonendetektoren und Quantenoptik. Außerdem gibt es einige Projekte, die sich mit allgemeinen Konzepten der Quantenkommunikation, Transceivern für die Quantenkommunikation (ohne Photonenquellen und -detektoren), Quantensystemen auf Chips und dem Quanteninternet befassen. Es sei darauf hingewiesen, dass eine geringere Anzahl von Projekten nicht unbedingt auf eine geringere Bedeutung des Themas hinweist. So ist beispielsweise das Quanteninternet ein Thema mit hoher strategischer Priorität für die EU. Das entsprechende Projekt, das unter anderem in Abbildung 14 angegebene ist, bezieht sich auf die Quanteninternet-Allianz, [173] eine groß angelegte Initiative mit H2020-Mitteln in Höhe von etwa 10 Millionen Euro.

Abbildung 14: Verteilung der Themen in den 57 identifizierten Horizont 2020 Projekten.

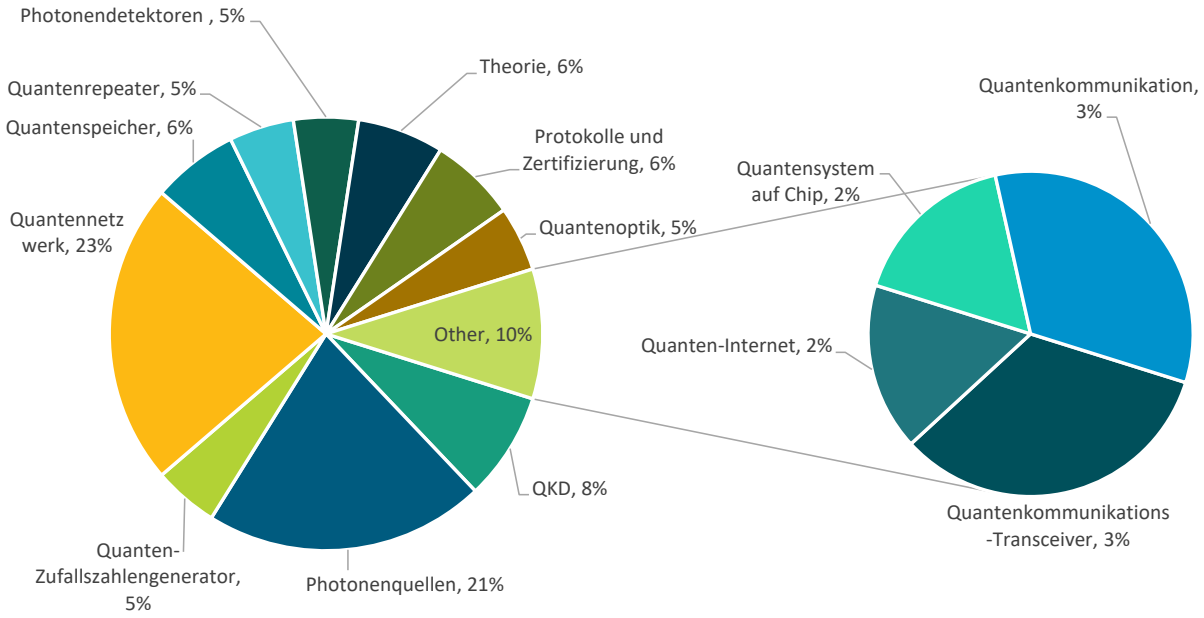
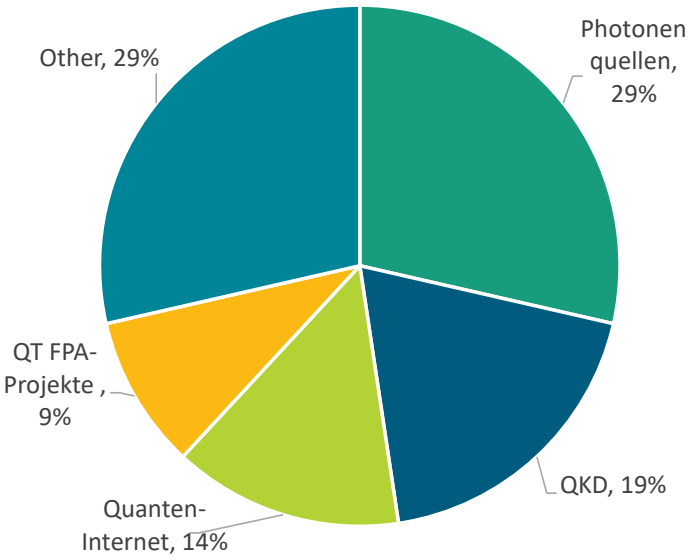


Abbildung 15 zeigt die Themen, die in den identifizierten HE-Projekten (Aufforderungen 2021-2022) behandelt werden. Wie die Abbildung zeigt, machen Photonenquellen, QKD und das Quanteninternet über 60 Prozent der Themen aus. Es gibt auch zwei geförderte Projekte, die auf dem Modell des Partnerschaftsrahmenvertrags ("Framework Partnership Agreement" – FPA) für die Pilotlinienproduktion und -erprobung von Quantentechnologien einschließlich Quantenkommunikation basieren. Diese Projekte umfassen unter anderem eine Photonik-Pilotlinie, photonische integrierte Schaltungen (PIC), verschränkte Photonenquellen und QRNGs. [174] Andere Themen machen etwa 30 Prozent aus und umfassen QRNG, Quantenmodems, Quantensysteme auf Chips, Quantenspeicher und optische Fasern, die jeweils von einem Projekt behandelt werden.

Abbildung 15: Verteilung der Themen in den 21 identifizierten Horizont Europa Projekten.



5.5 Internationale Situation und Initiativen

5.5.1 Internationale Förderinitiativen

Dieser Abschnitt gibt einen Überblick über die Förderinitiativen und strategischen Ziele für die QCom-Technologien der wichtigsten internationalen Akteure Deutschland, EU, China, USA, Vereinigtes Königreich, Japan, Kanada, Südkorea und Indien.[4]

Deutschland: Die F&E-Aktivitäten von QCom in Deutschland werden derzeit durch zwei Rahmenprogramme des Bundesministeriums für Bildung und Forschung (BMBF) gefördert: "Quantentechnologien" und "Vernetzung und Sicherheit digitaler Systeme". "Quantentechnologien" wurde 2018 gestartet, nachdem das BMBF angekündigt hatte, 650 Millionen Euro für Quantentechnologien zur Verfügung zu stellen. Das Programm umfasst verschiedene Quantentechnologien, darunter Quantencomputing und -simulation, quantenbasierte Messverfahren, Basistechnologien für Quantensysteme sowie Quantenkommunikation. Das Programm "Vernetzung und Sicherheit digitaler Systeme" konzentriert sich auf drei Hauptthemen: IT-Sicherheit, Kommunikationssysteme und Leben in einer digitalisierten Welt. QCom gilt als eine Schlüsseltechnologie zur Verbesserung der IT-Sicherheit.

Obwohl unsere vergleichende Analyse keine spezifischen Daten enthält, ist es erwähnenswert, dass auch Landesregierungen in Deutschland eine Rolle bei der Unterstützung von Projekten spielen. So hat die Thüringer Landesregierung dem Fraunhofer IOF 11 Millionen Euro für den Aufbau einer Quantenkommunikationsinfrastruktur zur Verfügung gestellt. [175] Zusätzlich zu den bestehenden Programmen hat das BMBF im April 2023 ein neues Strategiepapier "Handlungskonzept Quantentechnologien" [176] veröffentlicht, in dem für die Jahre 2023 bis 2026 Fördermittel in Höhe von ca. 2,18 Milliarden Euro für Quantentechnologien angekündigt werden.

Strategische Ziele für QCom in Deutschland: Im Rahmen von "Quantentechnologien" soll der Übergang von der wissenschaftsgeleiteten Quantenforschung zu neuartigen Anwendungen unterstützt werden. Das neue Handlungskonzept beschreibt zudem das langfristige Ziel, im Jahr 2036 Spitzentechnologien mit einem breiten Anwendungsspektrum zu etablieren. In der "Vision 2036" des Aktionskonzepts wird QCom als ein Mittel erwähnt, das zusätzliche Sicherheit für sensible Daten bietet.

In dem Strategiepapier werden auch die folgenden Meilensteine bis 2026 für QCom genannt:

- „Etablierung von ersten abhörsicheren, das heißt quantenverschlüsselten, Kommunikationsteststrecken zwischen ausgewählten Behördenstandorten."
- „Realisierung eines bundesweiten Glasfaser-Backbones für die Quantenkommunikation und die Zeit- und Frequenzverteilung."
- "Demonstration erster Quantenrepeater-Teststrecken."
- "Start erster Testsatelliten zur Quantenschlüsselverteilung."

Europäische Union: Für die EU wird QCom durch die Programme Horizont 2020/Horizont Europa (mit Schwerpunkt auf Forschung und Entwicklung) und EuroQCI [37] (mit Schwerpunkt auf Infrastruktur und Technologieeinsatz) finanziert. Detaillierte Informationen zu den Projekten im Rahmen der Horizont-Programme befinden sich im Abschnitt 5.4.

Die identifizierten EuroQCI-Aufrufe sehen folgendes Budget für das terrestrische Segment vor:

[4] In diesem Abschnitt wurde bei den Berechnungen von folgenden Umrechnungskursen ausgegangen: 1 Euro = 0,86 GBP; 156,25 JPY; 1,11 USD; 1,46 CAD; 91,17 INR und 7,77 CNY.

- 154 Millionen Euro im Rahmen des Programms "Digitales Europa", das Industrieprojekte, nationale Projekte und eine Koordinierungs- und Unterstützungsmaßnahme zur Verknüpfung aller Projekte umfasst. [177]
- 90 Millionen Euro im Rahmen der Fazilität "Connecting Europe" (Connecting Europe Facility) zur Förderung des Verbunds der nationalen Quantenkommunikationsinfrastrukturnetze zwischen Nachbarländern sowie des Verbunds der Boden- und Weltraumsegmente von EuroQCI. [178]

Die Europäische Weltraumorganisation (ESA) sowie nationale Fonds tragen ebenfalls zu der Initiative bei, auch wenn keine konkreten Haushaltsangaben gemacht werden.

Strategische Ziele für QCom in der EU: Die langfristige Vision der EU ist die Entwicklung eines Quanteninternets in ganz Europa. Um dieses Ziel zu erreichen, wurden die Initiativen Quantum Flagship und EuroQCI gestartet.

Die Quantum Flagship-Finanzierung wird im Rahmen von Horizont 2020 und Horizont Europa vergeben. Die Prioritäten sind in einer strategischen Forschungsagenda dargelegt, die kurzfristige (3 Jahre) und mittel-/langfristige (6-10 Jahre) Ziele für jeden Technologiebereich, einschließlich QCom, festlegt.

Ziel des EuroQCI ist es, eine sichere Quantenkommunikationsinfrastruktur für die gesamte EU zu schaffen. Dabei werden innovative Technologien genutzt, die im Rahmen von Horizont-Projekten entwickelt wurden, insbesondere das OpenQKD-Projekt im Rahmen von Horizont 2020. Darüber hinaus arbeiten die Europäische Kommission und die ESA zusammen, um eine Konstellation der ersten Generation von EuroQCI-Satelliten zu spezifizieren. Der erste Prototypsatellit, Eagle1, soll Ende 2024 gestartet werden.

China: Eines der wichtigsten Förderprogramme zur Unterstützung der Quanteninformationsforschung im Zeitraum des 13. Fünfjahresplans (2016-2020) war das "National Key R&D Program" des Ministeriums für Wissenschaft und Technologie (MoST). Pan et al. berichteten, dass im Rahmen des Programms von 2016 bis 2019 ca. 337 Millionen USD für "Quantum Control and Quantum Information"-Projekte ausgegeben wurden, aber es war nicht möglich, den Anteil der Mittel für die QCom-Forschung zu bestimmen. [179]

Darüber hinaus wurde 2017 das National Laboratory of Quantum Information Science mit einer Anfangsinvestition von 7 Milliarden CNY (ca. 900 Millionen Euro) eröffnet. Darüber hinaus sind weitere Investitionen in Höhe von 100 Milliarden CNY (ca. 13 Milliarden Euro) über einen Zeitraum von fünf Jahren geplant, [180] was den Großteil der geschätzten Gesamtinvestitionen in Quantentechnologien (QT) in China ausmacht.

Während des 14. Fünfjahresplans (2021-2025) wird die Quantenforschung in China durch "Mega-Projekte" im Rahmen des Programms Innovation 2030 weiter gefördert werden. Zum Zeitpunkt der Durchführung dieser Analyse waren die Finanzierungsrichtlinien jedoch noch nicht öffentlich zugänglich, und die Einzelheiten nicht transparent.

Auch die Provinzregierungen in China spielen eine wichtige Rolle bei der F&E-Finanzierung. So hat der 2017 eingerichtete neue Anhui Quantum Science Industry Development Fund angekündigt, 10 Milliarden CNY für Quantencomputing, Kommunikation und Metrologie bereitzustellen. [180]

Auch wenn der genaue Gesamtbetrag der öffentlichen Mittel in China noch unklar ist, besteht kein Zweifel daran, dass China erhebliche Anstrengungen unternommen und bemerkenswerte Meilensteine in der QCom-Technologie erreicht hat. So hat China im August 2016 den weltweit ersten Quantenkommunikationssatelliten namens "Micius (Mozi)" gestartet und 2017 die erste interkontinentale QKD erreicht. Der erste Micius-Satellit wurde mit geschätzten Kosten von 100 Millionen

USD im Rahmen von Chinas strategischem Prioritätsprogramm für Weltraumwissenschaften [181] als Teil des Projekts "Quantum Experiments at Space Scale" (QUESS) entwickelt. Eine weitere wichtige Errungenschaft ist die Einrichtung eines Quantenkommunikationsnetzes, das eine 2000 Kilometer lange Glasfaserverbindung zwischen verschiedenen Städten (Shanghai, Hefei, Ji-nan und Peking) und eine 2600 Kilometer lange Satellitenverbindung zwischen zwei Observatorien umfasst.

Strategische Ziele für QCom in China: Die Quantentechnologie ist als eine der vorrangigen Spitzentechnologien in den 14. Fünfjahresplan in China [182]aufgenommen worden, obwohl ein QCom-spezifisches strategisches Ziel in dem Plan nicht direkt erwähnt wird.

Im Jahr 2014 erklärte der einflussreiche chinesische Quantenforscher Prof. Jian-Wei Pan, der den Start des Micius-Satelliten leitete, dass China im Jahr 2020 eine interkontinentale QKD zwischen Asien und Europa demonstrieren würde, was 2017 tatsächlich realisiert wurde. Damals sagte Prof. Pan auch, dass China bis 2030 ein globales Quantenkommunikationsnetz aufbauen will. [183]

USA: Im Dezember 2018 wurde der National Quantum Initiative (NQI) Act verabschiedet, um die Quantenforschung und -entwicklung zu beschleunigen und die wirtschaftliche und nationale Sicherheit der USA zu gewährleisten. Ursprünglich wurden über einen Zeitraum von fünf Jahren mehr als 1,2 Milliarden USD zugesagt, doch laut dem jüngsten Haushaltsbericht sollten im Rahmen der Strategie bis zum Haushaltsjahr 2023 bereits rund 2 Milliarden USD bereitgestellt werden, wobei etwa 1,7 Milliarden USD des Haushalts für grundlegende F&E-Aktivitäten im Bereich der Quantentechnologien in den zuständigen Behörden vorgesehen sind. [184]

Das NQI-Gesetz genehmigt das Budget für die National Science Foundation (NSF), das Department of Energy (DOE) und das National Institute of Standards and Technology (NIST). Im Jahr 2023, zur Halbzeit der 10-Jahres-Initiative, hörte der Wissenschaftsausschuss des Repräsentantenhauses Stellungnahmen zu Ideen für eine Erweiterung der NQI an. Eine der diskutierten Optionen war die Einbeziehung weiterer Behörden, insbesondere der National Aeronautics and Space Administration (NASA), um den Rückstand Chinas bei der Entwicklung von Quantenkommunikationssatelliten aufzuholen. [185]

Die NQI kategorisiert ihre Aktivitäten in fünf verschiedene Komponentenbereiche, von denen einer "Quantum Networks and Communications (QNET)" ist. Diese Analyse wurde auf QNET fokussiert, um QCom-relevante Programme und Projekte zu identifizieren. Aus dem NQI-Budgetbericht geht hervor, dass ca. 10 Prozent des F&E-Budgets für Quantum Information Science (QIS) für QNET ausgegeben wurden.[5] Beispiele für die NQI-Instrumente für QNET-F&E sind:

- Die NSF wählte die Universität von Arizona für einen fünfjährigen Zuschuss in Höhe von 26 Millionen USD mit einer zusätzlichen Fünfjahresoption über 24,6 Millionen USD aus, um das Zentrum für Quantennetze einzurichten und zu leiten.
- Das DOE vergab insgesamt 25 Millionen USD an zwei Testprojekte zur Entwicklung eines Quanteninternets.

Strategische Ziele für QCom in den USA: "A Strategic Vision for America's Quantum Network", das als eines der strategischen Dokumente im Rahmen der NQI veröffentlicht wurde, umreißt die kurz- bis mittelfristige Vision der USA für Quantennetzwerktechnologien: [186]

[5] Die veröffentlichten Haushaltsdaten umfassen sowohl die Finanzierung im Rahmen der NQI als auch die Basisfinanzierung; es ist unklar, wie viel QNET-Forschung im Rahmen der NQI durchgeführt wird. Daher wurde die Finanzierung im Rahmen der NQI durch Multiplikation des QNET-Forschungsbudgets mit dem Verhältnis der NQI-Finanzierung für alle Quantenthemen für jedes Jahr geschätzt. Etwa die Hälfte des gesamten Quantenforschungsbudgets wird im Rahmen der NQI ausgegeben.

- In den nächsten fünf Jahren werden Unternehmen und Labors in den USA die wissenschaftlichen Grundlagen und Schlüsseltechnologien für Quantennetze demonstrieren und die potenziellen Auswirkungen und verbesserten Anwendungen aufzeigen.
- In den nächsten zwanzig Jahren werden Quanteninternetverbindungen vernetzte Quantengeräte nutzen, um neue Fähigkeiten zu ermöglichen, die mit herkömmlicher Technologie nicht möglich sind.

Um einen Technologiefahrplan zu entwickeln, veranstaltete das DOE im Jahr 2020 den Quantum Internet Blueprint Workshop, in dem wissenschaftliche Anwendungsbereiche, vorrangige Forschungsrichtungen und wichtige Meilensteine für ein mögliches nationales Quanteninternet festgelegt wurden. [187]

Vereinigtes Königreich: Das Nationale Programm für Quantentechnologien (National Quantum Technologies Programme – NQTP) des Vereinigten Königreichs wurde 2014 ins Leben gerufen und stellt eine 1 Milliarde GBP schwere Partnerschaft zwischen Regierung, Wissenschaft und Industrie dar. Auf der NQTP-Website wurden QCom-bezogene Projekte und Programme identifiziert, die einen Einblick in den Forschungsschwerpunkt des Programms geben. [4] Dazu gehören das Quantum Communication Hub (2014-2024 mit 49,8 Millionen GBP), ein Quantensatellitenprojekt mit Singapur (mit 10 Millionen GBP) und 26 Projekte, die vom Industrial Strategy Challenge Fund unterstützt werden.

Darüber hinaus veröffentlichte die britische Regierung 2023 ihre neue Strategie für den Zeitraum 2024-2033 mit Plänen, mehr als 2,5 Milliarden GBP in QT zu investieren. Dies ist mehr als das Doppelte des in der vorherigen Strategie vorgesehenen Betrags. Dies bedeutet, dass das Finanzierungsbudget im Vereinigten Königreich in naher Zukunft voraussichtlich erheblich steigen wird. [188]

Strategische Ziele für QCom im Vereinigten Königreich: Die neue Strategie hat vier Ziele festgelegt: 1) weltweit führende Forschung und Kompetenzen; 2) Unterstützung der Wirtschaft; 3) Förderung der Einführung von Quantentechnologien und 4) führende Quantenregulierung und Schutz des Sektors. Für diese Ziele gibt es klar definierte Vorgaben, die bis 2033 erreicht werden sollen (z. B. "Bis 2033 wird das Vereinigte Königreich bei der Qualität wissenschaftlicher Veröffentlichungen einen Platz unter den ersten drei einnehmen und gleichzeitig das Volumen erhöhen").

Allerdings enthalten weder das NQTP des Vereinigten Königreichs noch die neue Strategie ein spezifisches Ziel für QCom. In der neuen Strategie heißt es, dass der Schwerpunkt auf der Ausschöpfung des Potenzials von QCom für die sichere Kommunikation liegt, wo eindeutige Vorteile nachgewiesen werden können sowie auf den Möglichkeiten, die QCom für die Vernetzung von Quantencomputern, den Informationsaustausch und die Datenspeicherung bietet.

Japan: Die japanische Regierung hat ihre Innovationsstrategie für Quantentechnologie im Jahr 2020 (Haushaltsjahr 2019[6]) als ressortübergreifende Strategie veröffentlicht. Obwohl das Dokument selbst keine spezifischen Informationen über die erwartete Höhe der öffentlichen Mittel für einen bestimmten Zeitraum enthält, hat die Regierung eine Liste relevanter Programme/Projekte zusammen mit der jährlichen Mittelzuweisung veröffentlicht. Für diese Analyse haben wir uns auf die Programme/Projekte konzentriert, die als "Quantenkryptografie" oder "Quantensicherheit" kategorisiert sind, und ihre Budgets vom Haushaltsjahr 2018 bis zum Haushaltsjahr 2023 summiert.

Der Großteil der öffentlichen Mittel für QCom in Japan, etwa 73 Prozent, wird für Projekte unter der Leitung des Ministeriums für innere Angelegenheiten und Kommunikation (MIC) bereitgestellt. Seit

[6] Das japanische Haushaltsjahr 2019 beginnt im April 2019 und endet im März 2020

dem Haushaltsjahr 2018 hat das MIC sieben Projekte unterstützt, die sich auf verschiedene Bereiche wie die Entwicklung von Testbeds, Quantenkryptografie in der Satellitenkommunikation, F&E für den Aufbau eines globalen Quantennetzwerks und elementare Technologien für das Quanteninternet konzentrieren.

Ein weiteres wichtiges Programm ist das ressortübergreifende strategische Innovationsförderungsprogramm (Cross-ministerial Strategic Innovation Promotion Program - SIP). In der aktuellen Phase des SIP liegt der Schwerpunkt auf der Entwicklung der "Quantum Secure Cloud" und ihrer Anwendungsfälle, die die Integration von Quantenkryptografie, Geheimnisteilung und geheimer Berechnung beinhaltet. [189]

Strategische Ziele für QCom in Japan: Die Quanteninnovationsstrategie umfasst Technologie-Roadmaps für Schlüsselbereiche. Für QCom gibt es drei Roadmaps: eine Roadmap für Kommunikation und Kryptografie, eine für Quantenrepeater und eine für Netzwerktechnologien. Die Ziele für jeden Bereich sind:

- Demonstration einer quantenkryptografischen Kommunikation mit 10 Mbit/s in einem Großstadtgebiet bis 2025, Ausweitung auf den Intercity-Bereich (Fernanwendung) bis 2030.
- Verteilung der Quantenverschränkung zwischen drei Punkten bis 2030, Schlüsselgenerierung über 1 kbps mithilfe der Quantenverschränkung bis 2040, Realisierung eines Quantencomputernetzes bis 2040.
- Demonstration eines Netzes in städtischen Gebieten bis 2030, Realisierung eines globalen Quantenkryptografie-Netzes bis 2040, Demonstration der Quantenkommunikation im Weltraum und eines Quanteninternets bis 2040.

Südkorea: Im Jahr 2023 stellte Südkorea seine erste umfassende Quantenstrategie vor und versprach, bis 2035 mehr als 3 Billionen Won (ca. 2,1 Milliarden Euro) in öffentlich-private Ko-Investitionen zu investieren, um sich als globales Zentrum der Quantenwirtschaft zu etablieren. Im Hinblick auf QCom zielt die Strategie darauf ab, in den 2030er Jahren ein 100 Kilometer langes Quantennetz zu entwickeln und städteübergreifende Experimente zu fördern. [190]

Das National Convergence Network Project ist ein Beispiel für die jüngsten Erfolge in Südkorea. Im Jahr 2022 haben SK Broadband und IDQ, ein in Genf ansässiger Anbieter von Quantenkommunikationssystemen, die erste Phase dieses Projekts abgeschlossen. Ziel des Projekts ist die Sicherung des Kommunikationsnetzes von 48 koreanischen Regierungsorganisationen, die über das ganze Land verteilt sind. In dieser ersten Phase entwickelten die Unternehmen eine QKD-Netzwerkinfrastruktur mit einer Gesamtlänge von 800 Kilometer. [191] Für das Projekt werden insgesamt 82 Milliarden Won (ca. 58 Millionen Euro) benötigt, davon 54,1 Milliarden Won für die erste Phase und 28,6 Milliarden Won für die zweite Phase. Das Endziel des Projekts ist der Aufbau eines Netzes von bis zu 2000 Kilometer Länge. [192]

Kanada: Die kanadische Regierung hat im Jahr 2022 eine neue nationale Quantenstrategie veröffentlicht, in der eine der drei Missionen auf die Entwicklung von QCom-Technologien und Post-Quanten-Kryptografie ausgerichtet ist. [193]

Vor der Veröffentlichung dieser Strategie hatte Kanada zwischen 2012 und 2022 bereits über 1 Milliarde CAD (ca. 680 Millionen Euro) in die Quantenwissenschaft investiert. Eines der wichtigsten nationalen QCom-Projekte in Kanada ist die Quantenverschlüsselungs- und Wissenschaftssatellitenmission (Quantum Encryption and Science Satellite Mission - QEYSSat), die 2017 unter der Leitung der kanadischen Weltraumbehörde gestartet wurde. Obwohl die Gesamtinvestition in das Projekt

nicht klar ist, wurde berichtet, dass das amerikanische Unternehmen Honeywell einen Auftrag im Wert von über 30 Millionen CAD für die Entwurfs- und Implementierungsphasen der QEYSSat-Mission erhalten hat. [194] Der Satellit soll 2024/2025 gestartet werden und über BB84- und BBM92-Protokolle Bodenstationen in mehr als 400 Kilometer Entfernung miteinander verbinden. [195]

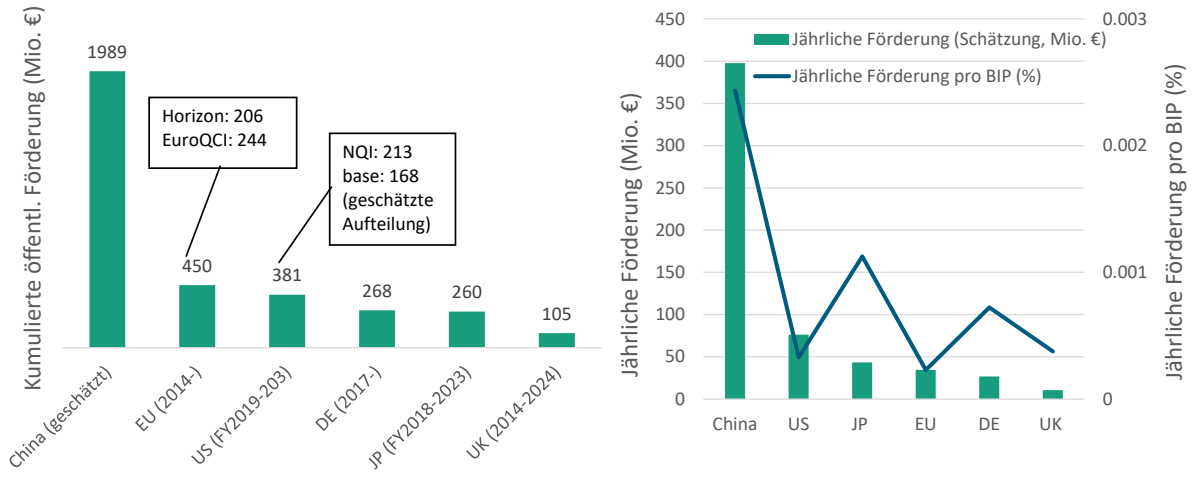
Indien: Im April 2023 genehmigte das indische Unionskabinett die Nationale Quantenmission (National Quantum Mission) mit Gesamtkosten von 60 Milliarden INR (ca. 677 Millionen Euro) für den Zeitraum 2023/24 bis 2030/31. Zu den erwarteten Ergebnissen der Mission gehören satellitengestützte sichere Quantenkommunikation zwischen Bodenstationen über eine Reichweite von 2000 Kilometer innerhalb Indiens, sichere Quantenkommunikation über große Entfernungen mit anderen Ländern, QKD zwischen Städten über 2000 Kilometer sowie ein Quantennetzwerk mit mehreren Knoten und Quantenspeichern. Die Mission plant auch die Einrichtung von vier thematischen Zentren in führenden akademischen und nationalen Forschungs- und Entwicklungsinstituten, wobei eines der Zentren sich auf die Quantenkommunikation konzentriert. [196]

5.5.2 Vergleich der internationalen QCom-Finanzierung

In diesem Abschnitt werden die öffentlichen Mittel untersucht, die zur Unterstützung der Forschung, Entwicklung und Einführung von QCom-Technologien bereitgestellt werden, um den Grad des Engagements der wichtigsten internationalen Akteure zu bewerten. Wir analysierten die geschätzte Höhe der öffentlichen Mittel, die durch nationale Projekte/Programme in den USA, dem Vereinigten Königreich, Japan, der EU, Deutschland und China investiert wurden. Diese Länder wurden auf der Grundlage ihrer F&E-Produktivität und der Verfügbarkeit von Haushaltsinformationen ausgewählt (Details in Abschnitt 2).

Abbildung 16 vergleicht den Gesamtbetrag der für die identifizierten nationalen QCom-Programme/Projekte bereitgestellten Mittel. Trotz der oben erwähnten Einschränkungen ermöglicht dieser Vergleich eine Einschätzung des F&E-Interesses verschiedener Länder an QCom.

Abbildung 16: Kumulierter Betrag der öffentlichen Mittel in QCom, angekündigt bis August 2023 (links) und jährlicher Gesamtbetrag der öffentlichen Mittel in QCom (Balkendiagramm) und pro BIP (Liniendiagramm) (rechts).



Nach unserer Schätzung[7] scheint China das bei Weitem aktivste Land bei der Finanzierung von QCom-Forschung zu sein, gefolgt von den USA und der EU. Im Falle der EU trägt die Finanzierung im Rahmen des EuroQCI mehr zur Gesamtfinanzierung bei als die Horizont-Programme. Deutschland und Japan befinden sich in Bezug auf QCom auf einem ähnlichen Niveau, obwohl Deutschland schätzungsweise viel mehr in QT im Allgemeinen investiert (3,5 Milliarden Euro in Deutschland gegenüber 1,6 Milliarden in Japan[8]). Die Investitionen des Vereinigten Königreichs sind niedriger als die der anderen untersuchten Länder, können aber aufgrund der geringeren Verfügbarkeit von Informationen unterschätzt werden.

Aufgrund der unterschiedlichen Zeithorizonte der Förderprogramme in den untersuchten Ländern kann sich beim Vergleich der Gesamtfördervolumina ein leicht verzerrtes Bild ergeben. Daher haben wir die jährliche Förderung berechnet (Balkendiagramm auf der rechten Seite von Abbildung 16), indem wir die kumulierten Fördermittel durch den Zeitraum der jeweiligen Strategie geteilt haben. Auch bei diesem Vergleich liegt China an der Spitze, gefolgt von den USA, Japan, Deutschland und dem Vereinigten Königreich. Im Fall von Deutschland ist das Ende des Förderprogramms unklar, sodass der Zeitraum von 2017 (Beginn des ersten betrachteten Projekts) bis 2026 (Ende des letzten Projekts) verwendet wurde. Da neue Projekte nach 2023 beginnen könnten, ist die jährliche Förderung für Deutschland zwangsläufig zu niedrig angesetzt.

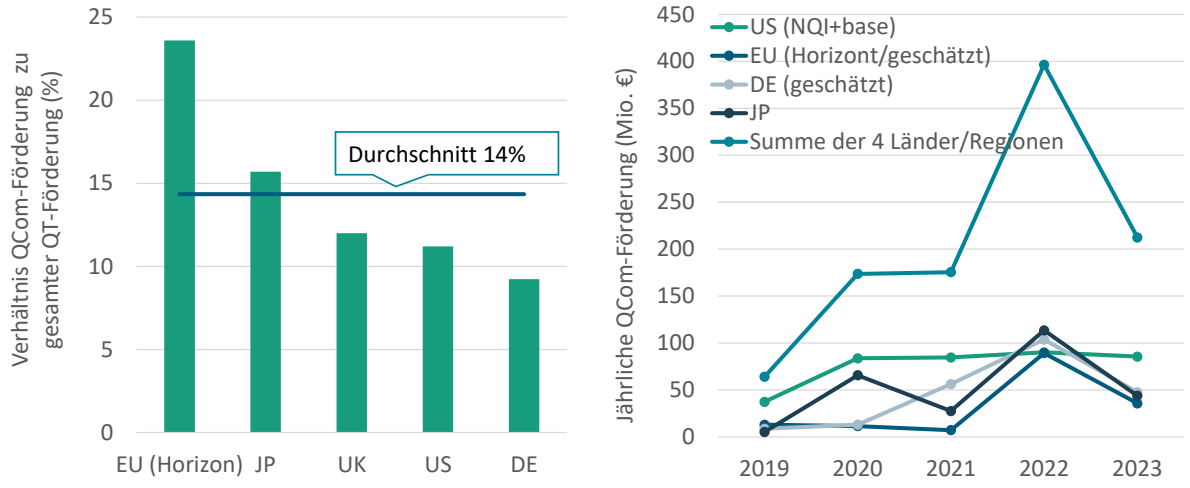
Um trotz der unterschiedlichen Größe und finanziellen Basis einen fairen Vergleich der QCom-Förderung zu ermöglichen, haben wir die jährliche QCom- Förderung ins Verhältnis zum Bruttoinlandsprodukt (BIP) des Landes gesetzt (Liniendiagramm auf der rechten Seite von Abbildung 16). China ist zwar immer noch führend, aber die Zahlen für Deutschland und Japan nähern sich China an und übertreffen sogar die der USA. Da die EU-Förderung nur EU-weite Initiativen und keine nationalen Mittel umfasst, sollte die Zahl für die EU als "zusätzliche" Finanzierung für die Mitgliedstaaten (einschließlich Deutschland) und nicht als Indikator für die EU-Aktivitäten in QCom interpretiert werden. Berücksichtigt man den Beitrag der EU-Förderung, so liegt Deutschlands Förderung im Verhältnis zum BIP näher an der von Japan.

Das Thema Quantentechnologien im Allgemeinen hat in letzter Zeit bei Regierungen und in der Industrie große Aufmerksamkeit erregt und wird derzeit von öffentlichen Stellen gut finanziert. Einige Länder scheinen sich mehr auf bestimmte QT (z. B. Quantencomputer) zu konzentrieren als andere. Um zu analysieren, ob einige Länder einen besonderen Schwerpunkt auf QCom legen, haben wir das Verhältnis von QCom zu den gesamten angekündigten Finanzmitteln für Quantentechnologien verglichen.

[7] Die Schätzung der Investitionen Chinas in die QCom erfolgt durch Multiplikation der angekündigten staatlichen Investitionen Chinas in alle Quantentechnologien (Mckinsey&Co. 2023) [7] mit dem durchschnittlichen Verhältnis der QCom-Förderung zur QT-Förderung in anderen analysierten Ländern (Abbildung 17, links).

[8] Der Gesamtbetrag der Finanzierung bezieht sich auf den CIFAR-Bericht (2021) und die in unserer Analyse erhobenen Daten

Abbildung 17: Geschätztes Verhältnis der QCom-Finanzierung zu den gesamten staatlichen Investitionen in Quantentechnologien (links). Trend der jährlichen Verteilung der QCom-Mittel in den USA, der EU, Deutschland und Japan (2019-2023) (rechts).



Gemäß Abbildung 17 (links) scheint die EU fast ein Viertel ihrer QT-Mittel auf QCom zu konzentrieren (23,6 %). Insbesondere zwei SGA-Projekte unter dem Partnerschaftsrahmenvertrag (Quantum Secure Networks Partnership und Quantum Internet Alliance) leisten einen bedeutenden Beitrag. SGA-Projekte haben oft ein größeres Budget als andere Projekte, und zwei der sieben SGAs unter dem Quantum Technologies Flagship sind mit der QCom-Forschung verbunden, was zu dem relativ hohen QCom-Anteil an der EU-Finanzierung führt.

Nach der EU weist Japan den zweithöchsten Anteil auf (15,7 %). Das Vereinigte Königreich, die USA und Deutschland konzentrieren sich mit rund 10 Prozent der Gesamtfinanzierung in ähnlichem Umfang auf QCom. Diese Länder stellen mehr Mittel für das Quantencomputing als für QCom bereit.

Um die Entwicklung im Zeitverlauf zu untersuchen, wurden die Daten zur jährlichen Verteilung der geschätzten Fördermittel für Deutschland und die EU aus unserem Projekt-Monitoring abgeleitet. Das Vereinigte Königreich wurde hier mangels geeigneter Daten nicht analysiert. Trotz der unterschiedlichen Definition des Begriffs "Jahreshaushalt" (Details in Abschnitt 2, Methoden), zeigt Abbildung 17 (rechts) die allgemeine Entwicklung der Finanzierung über diese fünf Jahre in den USA, der EU, Deutschland und Japan. Insgesamt haben alle vier ihre Mittel für QCom seit 2019 erhöht. Betrachtet man die Summe der Mittel für die drei Länder und die EU, so ist die Zahl im Jahr 2023 mehr als dreimal so hoch wie die Zahl im Jahr 2019. Während die USA seit der Gründung der NQI konstant rund 90-100 Millionen Euro (50-60 Millionen Euro pro Jahr) ausgegeben haben, schwankten die Mittel in der EU, Deutschland und Japan von Jahr zu Jahr.

Der plötzliche Anstieg der Fördermittel in Deutschland seit 2021 spiegelt den Start vieler neuer Projekte ab diesem Jahr wider. Im Gegensatz dazu ist der Anstieg der EU-Mittel auf ein höheres durchschnittliches Projektbudget in Horizont Europa als in H2020 zurückzuführen. Da der Rückgang der Beiträge im Jahr 2023 vor allem darauf zurückzuführen ist, dass die gemeldeten Werte nur die erste Jahreshälfte umfassen, wird sich der Trend zu höheren Investitionen voraussichtlich auch nach 2023 fortsetzen (siehe Abschnitt 5.4 für weitere Details). Im Falle Deutschlands wird diese Erwartung auch durch die neue Strategie gestützt, die bereits vorsieht, zwischen 2023 und 2026 mehr als 2 Milliarden Euro für QT bereitzustellen.

Die plötzlichen Sprünge in der japanischen Finanzierung im Haushaltsjahr 2020 und 2022 sind in erster Linie auf die einjährige Finanzierung aus dem Nachtragshaushalt zurückzuführen, der für dringende Bedürfnisse reserviert ist. Insbesondere die Einrichtung des Quantum Security Research Hub (mit ca. 51 Millionen Euro) und die beiden Testbed-Projekte (mit ca. 89 Millionen Euro) durch das Ministerium für Innere Angelegenheiten und Kommunikation (MIC) haben erheblich zu diesen Steigerungen beigetragen. Gleichzeitig hat das MIC kürzlich sein Budget für längerfristige (fünfjährige) Projekte aufgestockt, sodass die öffentliche Finanzierung in Japan auch nach dem Haushaltsjahr 2023 auf einem höheren Niveau bleiben dürfte, zumindest im Vergleich zum Haushaltsjahr 2019.

Methodische Einschränkungen

- Der Umfang der verfügbaren Informationen ist von Land zu Land unterschiedlich, was dazu führen kann, dass die QCom-Mittel in einigen Ländern unterschätzt werden. Die USA beispielsweise stellen jährliche Haushaltsinformationen sowohl für die NQI als auch für die Basisfinanzierung der relevanten Agenturen zur Verfügung. Für Deutschland ist es z. B. schwierig, den Betrag der DFG (Deutsche Forschungsgemeinschaft) herauszufinden, der speziell für QCom bereitgestellt wird. Im Vereinigten Königreich umfasst das NQTP auch Mittel für Qualifikation und Ausbildung. Hier ist es schwierig, ausreichende Daten zu finden, um QCom-spezifische Projekte zu identifizieren.
- Aufgrund der begrenzten Verfügbarkeit von Informationen über China kann unsere Analyse nur eine grobe Schätzung der chinesischen Finanzierung auf der Grundlage der Gesamtfinanzierung der Quantentechnologie aus früheren Untersuchungen und unserer Schätzung des QCom-Verhältnisses liefern.
- In unserer Analyse der Entwicklung der Finanzierung im Laufe der Zeit variiert die Definition der "jährlichen Verteilung" notwendigerweise zwischen den Ländern aufgrund der unterschiedlichen Verfügbarkeit von Informationen. Da die EU und Deutschland nur das Projektbudget für den gesamten Zeitraum offenlegen, wird die jährliche Verteilung auf der Grundlage der Anzahl der Projekte und ihres durchschnittlichen Budgets geschätzt.
- Unsere Untersuchung berücksichtigt nur die öffentliche Finanzierung, aber es ist wahrscheinlich, dass es neben der staatlichen Finanzierung noch andere Finanzquellen gibt, wie z. B. private Investitionen, insbesondere in den USA. Laut dem McKinsey Quantum Technology Monitor 2023 erhielten US-amerikanische QT-Startups zwischen 2001 und 2022 fünfmal mehr Investitionen von privaten Investoren als Unternehmen in der EU insgesamt. [7]

5.6 Testbeds für QKD in Deutschland

Testbed-Infrastrukturen sind für QKD-Anbieter und -Entwickler von entscheidender Bedeutung, da sie es ihnen ermöglichen, neue Technologien, Protokolle und Anwendungsfälle zu testen und zu verifizieren sowie die Entwicklung und den Einsatz neuer und standardisierter QKD-Komponenten zu beschleunigen. Bei mehreren der derzeit geförderten Projekte ist die Entwicklung von Testbeds ein wesentliches Element oder das Hauptziel. Prominente Beispiele sind die von der EU und dem BMBF geförderten Projekte im Bereich der Quantenkommunikation in Deutschland wie das QuNET-Konsortium und die Q-net-Q-Initiative – dem deutschen Zweig der EuroQCI-Initiative. Weitere Testbed-Infrastrukturen wurden im QR.X-Konsortium sowie in Projekten der sogenannten Länder-Initiativen und darüber hinaus wie im Münchner Quantennetzwerk (MuQuaNet) aufgebaut und genutzt.

Testbeds ermöglichen den Betrieb und die Bewertung von Geräten in realen Testumgebungen. Die meisten der in Deutschland verfügbaren QKD-Testbeds konzentrieren sich auf die Übertragung von QKD-Signalen. So gibt es mehrere, nicht parallel zu Telekommunikationszwecken genutzten Glasfaser-Verbindungen (Dark Fiber). Diese ermöglichen es, Geräte ohne optische Verstärker und den Einfluss der Rückstreuung von kopropagierenden klassischen Kanälen zu untersuchen. Darüber hinaus sind auch Freistrahlverbindungen und optische Bodenstationen für satelliten- oder flugzeuggestützte QKD verfügbar. Das Schirmprojekt Quantenkommunikation Deutschland (SQuaD), das vom BMBF im Rahmen des Innovationshubs für Quantenkommunikation gefördert wird, hat mit der Zusammenstellung der in Deutschland verfügbaren QKD-Testbeds begonnen und eine Testbed-Karte auf seiner Website veröffentlicht (Abbildung 18). [197]

Abbildung 18: Erste Übersicht über bestehende und geplante Testbed-Infrastrukturen in Deutschland im Bereich Qcom. Bei den meisten Testbeds handelt es sich um Glasfaser- oder Freistrahlverbindungen. Die Testbeds sind entweder Punkt-zu-Punkt-Verbindungen oder Netzwerke. Beispiele sind das Berlin Quantum Communication Testbed (oben rechts) und das MuQuaNet (unten rechts).

Quelle: Kartendaten von OpenStreetMap (2024).

Bislang umfasst die Karte 14 Testnetze in Berlin, Thüringen, Niedersachsen, Sachsen, dem Saarland und Nordrhein-Westfalen. Durch Heranzoomen werden die detaillierten Netzarchitekturen sichtbar, die in den meisten Fällen aus einfachen Punkt-zu-Punkt-Verbindungen bestehen, jedoch auch einige komplexere Netze umfassen. Das Berliner Quantenkommunikations-Testbed (Abbildung 18, rechts oben) besteht aus Glasfasern und einer Freistrahlverbindung. Rechts unten in Abbildung 18 ist das Quanten-Netzwerk im Großraum München (MuQuaNet) abgebildet. Die Spezifikationen der Glasfaser-Testbeds sind in Tabelle 7 aufgeführt. Die Länge der Glasfaser-Testbeds reicht von einigen hundert Metern des hausinternen Dresden Qcom Fiber Testbeds in Sachsen bis zu etwa 78 Kilometer des Niedersachsen Quantum Link, was die derzeitige obere Grenze für die glasfaserbasierte optische Übertragung von QKD-Signalen ohne Trusted Nodes oder Quantenrepeater darstellt. Letztere Technologie befindet sich noch in der Forschung und ist noch nicht verfügbar. Die Übertragungsdistanz von QKD-Signalen ist aufgrund der Dämpfung des optischen Signals innerhalb der Glasfaser begrenzt. Einige der Glasfaserverbindungen sind hausintern, aber die meisten sind Intercity- und Intracity-Verbindungen und damit nahe an den Bedingungen für spätere Anwendungen. Intracity- und Intercity-Dark-Fibers werden von kommerziellen Anbietern gemietet. Wie Tabelle 7 zeigt, konzentrieren sich die fasergebundenen Testbeds auf den Telekommunikati-

onswellenlängenbereich des O-Bandes (um 1310 nm) und des C-Bandes (um 1550 nm). Das sichtbare Spektrum wird jedoch auch für Freistrahloptiken und insbesondere für optische Bodenstationen in Betracht gezogen.

Die meisten der gezeigten Verbindungen stammen aus speziellen Projekten und haben individuelle Merkmale, Infrastruktur und nachgewiesene Meilensteine. Das Saarbrücker Qcom Fiber Testbed und der Niedersachsen Quantum Link sind beide in das QR.X-Projekt eingebettet, das sich auf die Entwicklung von Quantenrepeatern konzentriert. Ein Meilenstein, den das Saarbrücker Qcom Fiber Testbed demonstriert hat, ist die Verteilung von Photon-Photon- und Qubit-Photon-Verschränkung über eine 14 Kilometer lange Faser und die Quantenteleportation von einem Ionen-Qubit zu einem photonischen Qubit. Die niedersächsische Quantenverbindung besteht aus einem Paar von Dunkelfasern, so dass auch eine gleichzeitige Zeit- und Frequenzübertragung zwischen der Physikalisch-Technischen Bundesanstalt (PTB) und der Leibniz Universität Hannover (LUH) möglich ist: Eine Faser kann für Quantenanwendungen genutzt werden, während die andere für die Übertragung von Zeit- und Frequenzreferenzen sowie klassischen Kommunikationssignalen verwendet werden kann. In ersten Experimenten wird hier QKD mit hoher Wiederholrate mit Halbleiter-Quantenpunkt-Einzelphotonenquellen getestet. Das Berlin Quantum Communication Testbed wurde bereits für mehrere Proof-of-Principle-Experimente zu QKD über Freistrahl und Glasfaser sowie zur Verschränkungsverteilung genutzt. Im QuNET Schlüsselexperiment 1, das 2023 in Jena durchgeführt wurde, demonstrierte das Konsortium die vollständige QKD auf einer heterogenen Verbindung, die aus einer 1,7 Kilometer langen Freistrahlverbindung und einer mehrere hundert Meter langen Glasfaserverbindung über das lokale Campusnetz Beutenberg bestand. Ein weiteres Testbed, das Jena und Erfurt über 76 Kilometer Glasfaser verbindet, wird nicht nur vom Fraunhofer IOF für interne Experimente genutzt, sondern auch von Quantum Optics Jena, um ihre Geräte zu testen. Das MuQuaNet-Testbed soll unter anderem die Quantenkommunikation für zivile und militärische Anwendungen demonstrieren. Mit der Optischen Bodenstation (Optical Ground Station – OGS) Oberpfaffenhofen wurden Luft-Boden-Kommunikationsexperimente durchgeführt und optische Verbindungsmessungen mit mehreren Satelliten erzielt.

Ein Netzwerk, das sich als wertvoll für die Entwicklung von QKD herausstellen kann, ist das F&E SASER-Netzwerk, das aus dem gleichnamigen BMBF-geförderten SASER-Projekt entstanden ist. Im Rahmen des Projektes wurde ein deutschland-weites Fasernetzwerk aufgebaut und kontinuierlich weiterentwickelt mit dem Ziel, Tests von Technologien der optischen Faserkommunikation zu unterstützen. Das F&E SASER Netzwerk, das seinen Ursprung in der Forschung und Entwicklung klassischer Kommunikationstechnologien hat, wurde ursprünglich nicht für QKD Anwendungen ausgelegt. Innerhalb Berlins hat das SASER-Testnetz eine sternartige Netzwerkarchitektur mit dem zentralen Knoten bei der Deutschen Telekom Winterfeldstraße (WFD) und umfasst Dunkelfasern zu verschiedenen Orten wie z.B. dem Fraunhofer HHI, der Humboldt Universität und diversen anderen Orten mit einer Gesamtlänge von mehr als 500 km. Die voll verknüpfte Netzwerkarchitektur beinhaltet mindestens 12 Knoten und erlaubt sowohl dichtes Wellenlängen Multiplexing (DWDM) sowie wellenlängenunabhängiges optisches Schalten, was die Übertragung von Quantenkanälen ermöglicht.

Neben den QKD-Übertragungsprüfständen gibt es auch Prüfstände, die sich auf einzelne Schlüsselkomponenten von QKD-Geräten konzentrieren, die noch nicht auf der Landkarte verzeichnet sind. In der PTB gibt es zum Beispiel Testbeds zur Charakterisierung von Einzelphotonenquellen und Einzelphotonendetektoren. Für eine zuverlässige und sichere Anwendung von QKD ist die Prüfung der einzelnen Komponenten von QKD-Aufbauten ebenso wichtig wie die Übertragung der Signale.

Zwar gibt es über ganz Deutschland verteilt Testbeds für QKD Tests, doch handelt es sich dabei meist um Einzelverbindungen. Ein durchgängiges QKD-Backbone in ganz Deutschland existiert

noch nicht. Im Rahmen des nationalen QCI-Projekts innerhalb von EuroQCI Q-net-Q, der QuNET-Initiative und der Länder-Initiativen werden längere Testbed-Verbindungen in Erwägung gezogen, die mehrere Bundesländer wie Berlin, Hessen, Sachsen, Thüringen und Bayern miteinander verbinden sollen (z. B. Dresden – Erfurt – Nürnberg oder Berlin – Erfurt – Frankfurt). Die meisten Testbeds sind jedoch Teil kurzfristiger Projekte und ihr Bestehen ist auf höchstens ein paar Jahre begrenzt. Daher ist davon auszugehen, dass sich die Karte der Testbeds laufend ändern wird.

Tabelle 7: Überblick über die QKD-Link-Testbeds, die in der Testbed-Karte des SQuaD-Projekts enthalten sind. Die meisten QKD-Verbindungen sind glasfaserbasiert, wobei auch Verbindungen basierend auf Freistrahloptik (FSO) und über optische Bodenstationen (OGS) existieren:

Name	Bundesland	Typ	Länge	Wellenlänge	Status
Saarbrücken QCom Fiber Testbed	Saarland	Faser	14 km	O-Band (1310 nm) bis C-Band (1550 nm)	betriebsbereit
Jena – Erfurt Fiber Link	Thüringen	Faser	76 km	C-Band (1550 nm)	betriebsbereit
Campus Network Beutenberg	Thüringen	Faser	<1 km	O-Band (1310 nm), C-Band (1550 nm)	betriebsbereit
Berlin Quantum Communication Testbed	Berlin	Faser	bis zu 26 km	unbeschaltete Glasfaser	betriebsbereit
Niedersachsen Quantum Link	Niedersachsen	Faser	78 km	C-Band (1530-1565 nm)	betriebsbereit
PhoQSNet	Nordrhein-Westfalen	Faser	9 km	O-Band (1310 nm), C-Band (1550 nm)	geplant
Dresden QCom Fiber Testbed	Sachsen	Faser	bis zu 20 km	O-Band (1310 nm), C-Band (1550 nm)	betriebsbereit
Dresden QCom Fiber Testbed (in-house)	Sachsen	Faser	200 m	810 nm, O-Band (1310 nm) bis C-Band (1550 nm)	betriebsbereit
Munich Quantum Network (MuQuaNet)	Bayern	Faser und FSO	<1 km < 23 km	800 nm, C-Band (1550 nm)	teilweise betriebsbereit
tubLAN Q.0	Berlin	Faser und FSO	<1 km	780-950 m, O-Band, C-Band	geplant
Free-space Link Jena	Thüringen	FSO	1,7 km	500 nm - 2 µm	betriebsbereit
FSO testbed Oberpfaffenhofen	Bayern	FSO	7 km	VIS, 589, 850, 1064, 1550 nm	betriebsbereit
Optical Ground Station Oberpfaffenhofen	Bayern	OGS	k. A.	VIS, 589, 850, 1064, 1550 nm	betriebsbereit
Optical Ground Station Jena	Thüringen	OGS	k. A.	k. A.	geplant

6 Überlegungen zu Technologiesouveränität

Entsprechend dem "Handlungskonzept Quantentechnologien" der Bundesregierung strebt Deutschland in Zusammenarbeit mit seinen europäischen Partnern Technologiesouveränität in den Quantenkommunikationstechnologien an. [176] Technologiesouveränität hat jedoch viele Facetten und Aspekte, die wir in diesem Kapitel in Bezug auf das Thema Quantenkommunikation diskutieren wollen. Wir stützen uns dabei auf das Policy Paper "Technologiesouveränität – Vom Anspruch zum Konzept" des Fraunhofer ISI. [8] Darauf und auf Expertenmeinungen aufbauend wird die Notwendigkeit zur Erreichung von Technologiesouveränität in der QCom diskutiert (Abschnitt 6.2), aktuelle Herausforderungen dargestellt (Abschnitt 6.3) und mögliche Maßnahmen zu deren Bewältigung aufgezeigt (Abschnitt 6.4).

6.1 Kontext und Hintergrund

Die Diskussion über die Notwendigkeit der Sicherung der technologischen Souveränität für kritische Technologien in Deutschland und Europa hat in den letzten Jahren an Dynamik gewonnen. Geopolitische Spannungen, das Wiederaufflammen internationaler Konflikte, Kriege auf dem europäischen Kontinent und die Umstrukturierung der Weltwirtschaft haben dazu geführt, dass Politiken und Strategien immer wichtiger werden, die darauf abzielen, die eigenen Fähigkeiten und die Wertschöpfung innerhalb der Europäischen Union zu sichern.

Das Ziel der Technologiesouveränität wird in deutschen Förderprogrammen für Technologien formuliert, die als kritisch für die aktuellen und kommenden Transformationen identifiziert werden. Zu diesen Schlüsseltechnologien gehören Elektronik der nächsten Generation, Kommunikationstechnologien, KI und Software, Datentechnologien, Quantencomputer, Technologien, die für die Verwirklichung der Kreislaufwirtschaft benötigt werden oder Materialinnovationen ermöglichen, Batterien für Elektrofahrzeuge und stationäre Speichersysteme, Wasserstofftechnologien und Immunisierungstechnologien. [198] Die jüngste Betonung der Technologiesouveränität ist nicht nur in Deutschland und der Europäischen Union, sondern auch in anderen Ländern auf der ganzen Welt zu beobachten. So beinhaltet der in den USA verabschiedete Inflation Reduction Act weitreichende Maßnahmen, die auf das Ziel der Sicherung der inländischen Wertschöpfung ausgerichtet sind. Dieses Gesetz wird daher oft als prominentes Beispiel für ein Mittel zur Förderung eines hohen Maßes an technologischer Souveränität genannt.

Technologiesouveränität kann definiert werden als "die Fähigkeit eines Staates oder eines Staatenverbundes, die für seine Wohlfahrt, Wettbewerbsfähigkeit und Handlungsfähigkeit als entscheidend erachteten Technologien bereitzustellen und diese ohne einseitige strukturelle Abhängigkeit entwickeln oder aus anderen Wirtschaftsräumen beziehen zu können". [199] Da diese Definition eher konservativ ist im Vergleich zu dem, was oft gemeint ist, wenn Politiker und Politik diesen Ausdruck verwenden, wurden weitere Souveränitätsgrade eingeführt, die über die Technologie hinausgehen: Innovations- und Wirtschaftssouveränität. Während die Technologiesouveränität die Fähigkeit umfasst, eine Technologie zu erforschen und das entsprechende Produkt zumindest im Labormaßstab herzustellen, beinhaltet die Innovationssouveränität zusätzlich die Fähigkeit, die Technologie zu nutzen, um neue Lösungen für den Markt oder innerhalb der Gesellschaft zu realisieren. Das Erreichen wirtschaftlicher Souveränität beinhaltet die Fähigkeit, wirtschaftlichen Nutzen aus der Technologie zu ziehen (Tabelle 8).

Tabelle 8: Ausmaß der technologischen Souveränität:

Grad technologischer Souveränität	Bedeutet, dass man in der Lage ist,...	Notwendige Voraussetzung für...
Technologie-souveränität	...weltweit relevante Impulse für die technologische Entwicklung zu setzen	...das Aufrechterhalten von Technologieführerschaft
Innovations-souveränität	...Pilotlösungen unter realen Bedingungen und marktreifer Produkte zu entwickeln	...das Gestalten von Zukunfts-märkten
Wirtschaftliche Souveränität	...relevante Komponenten und Sys-teme entlang der Wertschöpfungs-kette zu produzieren	...das Schaffen von inländischer Wertschöpfung

Für die Länder, die der Europäischen Union angehören, sollte die technologische Souveränität nicht auf nationaler, sondern auf EU-Ebene betrachtet werden, da sie wirtschaftlich und politisch stark miteinander verflochten sind. So konzentriert sich auch dieser Bericht auf die europäische Technologiesouveränität. Dennoch sollte nicht vergessen werden, dass einige Aspekte stets auch auf nationaler Ebene diskutiert werden sollten.

Mit dem Aufkommen des Quantencomputers könnten Verschlüsselungen, die auf bestimmten herkömmlichen Algorithmen (z. B. AES-256) beruhen, innerhalb angemessener Zeiträume entschlüsselt werden, wodurch große Mengen ausgetauschter Daten anfällig für Lauschangriffe werden. Auch wenn es nicht einfach ist vorherzusagen, wann diese Bedrohung Realität werden könnte, steht die Notwendigkeit erheblicher technologischer Fortschritte bei den Verschlüsselungsalgorithmen außer Zweifel. Das Bundesministerium für Bildung und Forschung (BMBF) hat ausdrücklich das Ziel formuliert, Technologiesouveränität in der Quantenkommunikation zu erreichen und strebt sogar die weltweite Führung in den Kommunikationstechnologien an. [200] In Zusammenarbeit mit anderen Ministerien hat es einen Aktionsplan für Quantentechnologien veröffentlicht, um die Zuständigkeiten zu koordinieren. Weitere Akteure aus Wissenschaft, Wirtschaft und Politik haben bereits ihre Perspektiven für mögliche Maßnahmen formuliert. [201, 202]

Welche konkreten Fähigkeiten in Europa erhalten oder entwickelt werden sollen, ist jedoch noch offen. Die Einschätzungen, wie weit diese Fähigkeiten reichen sollten, können je nach Perspektive aus der Wissenschaft, der Industrie, der Politik oder der Gesellschaft unterschiedlich sein. Die folgende Diskussion soll einen Überblick über diese unterschiedlichen Perspektiven geben. Da sie auf mehreren Experteninterviews basiert, wie in Abschnitt 2 beschrieben, erhebt sie keinen Anspruch auf Vollständigkeit, sondern dient lediglich als Ausgangspunkt für weitere Analysen von Bedürfnissen, Motivationen, Herausforderungen und möglichen Maßnahmen zur Erreichung von technologischer Souveränität in der Quantenkommunikation in Deutschland und Europa.

Die Abschnitte 6.2, 6.3 und 6.4 spiegeln die Sichtweise der befragten Expert:innen wider und geben nicht zwingend den Standpunkt der Autoren wieder.

6.2 Bedürfnisse und Anforderungen

Sichere Kommunikation ist ein zentraler Pfeiler für demokratische Systeme und Gesellschaften, da sie eine Voraussetzung für die nationale Sicherheit, den Schutz von Geheimnissen auf staatlicher, betrieblicher und individueller Ebene, die Privatsphäre des Einzelnen, wirtschaftliche Transaktionen, Wahlen usw. ist. Die Sicherheit der genutzten Kommunikationskanäle ist daher Teil der kritischen Infrastruktur einer Nation. [203]

Die befragten Expert:innen und öffentlichen Akteure sehen die dringende Notwendigkeit, sich mit den kryptografischen Herausforderungen zu befassen, die der Aufstieg der Quantencomputer mit sich bringt, auch wenn verschiedene technologische Wege Lösungen bieten können. Außerdem sind die verschiedenen Interessengruppen unterschiedlicher Meinung darüber, ob diese Fähigkeiten im Inland aufgebaut oder lediglich über internationale Handelsbeziehungen zugänglich gemacht werden sollten.

Ein Ansatz, um die Kommunikation gegen kryptoanalytische Angriffe durch Quantencomputer zu sichern, ist die Verwendung von Algorithmen der Post-Quanten-Kryptografie" (PQK). In der Theorie könnte eine ideale PQK-Verschlüsselung die Ansätze der Quantenkommunikation in Bezug auf die Sicherheit der Kommunikation überflüssig machen. Allerdings gibt es derzeit keinen Beweis (oder Gegenbeweis), dass PQK-Algorithmen Angriffen von Quantencomputern widerstehen können. Daher sehen die befragten Expert:innen eine hohe Relevanz für die Ergänzung der F&E und Einführung von Post-Quanten-Kryptografie mit der Entwicklung von QCom-Technologien, wie QKD. Während sich konventionelle Algorithmen immer an den Fortschritten der (Quanten-)Computertechnologien orientieren müssen (es sei denn, es sei mathematisch bewiesen, dass sie völlig sicher vor Angriffen sind), könnten Quantenkommunikationsansätze potenziell Verschlüsselungen bieten, die auf fundamentaler Physik beruhen und auf den jeweiligen Übertragungswegen nicht entschlüsselbar sind. Hier sind zwei wichtige Anmerkungen zu machen: Erstens ist nicht auszuschließen, dass PQK-Algorithmen entwickelt werden könnten, die eine perfekte mathematische Sicherheit bieten, die dem Potenzial von QKD entspricht. Zweitens ist die oft behauptete perfekte Sicherheit von Quantenkommunikationstechnologien mit Vorsicht zu genießen, da potenzielle Sicherheitsbedrohungen (Implementierungsangriffe auf QKD-Systeme) noch zu adressieren sind. Dennoch werden QCom-Technologien oft als eine „peace-of-mind"-Lösung mit perfekter Sicherheit auf dem Übertragungsweg beschrieben. Und mindestens können sie in Ergänzung zu PQK-Ansätzen zusätzliche Sicherheit bieten. Die befragten Expert:innen waren sich einig, dass die Weiterentwicklung von QCom-Technologien daher notwendig ist, um Hochsicherheitsbereiche auf die zu erwartenden Zukunftsszenarien vorzubereiten.

Darüber hinaus sollten die heimischen Kompetenzen über die im Grundkonzept der Technologiesouveränität formulierten Aspekte hinausgehen. Das Vorhandensein des für die Entwicklung und Produktion von Technologien erforderlichen Fachwissens wurde von den befragten Expert:innen bis zu einem gewissen Grad als notwendig erachtet. Generell wurde der Import von Komponenten für QCom-Technologien als tolerierbar erachtet, solange genügend inländische Kompetenzen vorhanden sind, um alle Komponenten kritisch zu prüfen und auf die geforderten Sicherheitsstandards zu testen. Dies setze jedoch aufgrund der technischen Komplexität ein so tiefes Verständnis der betreffenden Technologien voraus, dass es den Fähigkeiten gleichkäme, die für eine inländische Produktion erforderlich sind. Die meisten Expert:innen würden auch den Import von Technologien auf Systemebene (z. B. QKD-Systeme) tolerieren, wenn ebendiese Voraussetzungen gegeben wären. Dennoch halten alle befragten Expert:innen die Fähigkeit, die Technologien zumindest auf Systemebene zu produzieren, aus unterschiedlichen Gründen für Europa für unverzichtbar: Erstens ist mit der heimischen Produktion eines QKD-Systems ein erhebliches wirtschaftliches Potenzial verbunden, das ein entscheidendes Sprungbrett für die zukünftige Wertschöpfung in verwandten Technologiefeldern mit potenziell noch größeren Märkten sein könnte (z. B. die Kommunikation

zwischen Quantencomputern). Zweitens könnte diese Fähigkeit erforderlich sein, um einseitige Abhängigkeiten zu vermeiden und mehrere Beschaffungsmöglichkeiten zu bieten, zumal sich derzeit einige Länder, wie die USA, eher auf PQK-basierte Ansätze zu konzentrieren scheinen. Darüber hinaus könnte Europa eine technologische Führungsrolle bei den Quantentechnologien oder verwandten Grundlagentechnologien anstreben, was die wechselseitigen Abhängigkeiten stabilisieren und den Weg für technologische Souveränität bei nicht verwandten Technologien ebnen könnte. Schließlich empfahlen auch einige Expert:innen den Import von Technologien auf Systemebene überhaupt nicht in Betracht zu ziehen, um Sicherheitsrisiken zu minimieren.

Tabelle 9: Bedarf an Kompetenzen in der Quantenkommunikation:

	Bedarf	Motivation
F&E	• Fähigkeit, Technologien zumindest auf Systemebene zu verstehen und zu entwickeln • Fähigkeit, (importierte) Komponenten und Systeme auf ihre Sicherheit hin zu prüfen	Gewährleistung der Sicherheit der implementierten Kommunikationsnetze
Herstellung	• Fähigkeit zur Herstellung von Technologien zumindest auf Systemebene • Möglichkeit, benötigte Komponenten ohne einseitige Abhängigkeiten zu importieren	• Vermeidung von Abhängigkeiten durch diversifizierte Beschaffungsstrategien • Vermeidung des Sicherheitsrisikos, das von nicht-europäischen Technologien ausgeht • Wertschöpfung ermöglichen

Insgesamt betonten alle befragten Expert:innen nachdrücklich die Notwendigkeit der Technologiesouveränität in der QCom. Einige gingen darüber hinaus und unterstrichen explizit das wirtschaftliche Potenzial, das Quantenkommunikationstechnologien in Zukunft entfalten könnten.

6.3 Status quo und Herausforderungen

Da es sich bei QCom um ein verhältnismäßig junges Technologiefeld handelt, sind Europa und Deutschland noch in der Lage, Strategien für alle Grade der Technologiehoheit und Technologieführerschaft zu realisieren. Im Folgenden stellen wir die wichtigsten Herausforderungen, die es zu bewältigen gilt, und ggf. den Status quo dar. In Anlehnung an die vom OECD-Ausschuss für Wissenschafts- und Technologiepolitik vorgeschlagenen Faktoren und Dimensionen haben wir die Expert:innen gebeten, entlang von vier Dimensionen Faktoren zu identifizieren, die die Innovationsaktivitäten des QCom hemmen. [9] Diese Dimensionen sind Kostenfaktoren, Wissensfaktoren, Marktfaktoren und institutionelle Faktoren. Da die Ergebnisse ausschließlich auf den Meinungen der Expert:innen beruhen, besteht für die Liste der diskutierten hemmenden Faktoren kein Anspruch auf Vollständigkeit.

Tabelle 10: Ausgangspunkt für die Erlangung der Technologiesouveränität im Bereich der Quantenkommunikationstechnologien in Europa:

Dimension	Leitfrage	Status quo
Kostenfaktoren	Kann Europa in eine wettbewerbsfähige QCom-Industrie investieren, um diese zu entwickeln und mit außereuropäischen Akteuren zu konkurrieren und/oder kooperieren?	+ Öffentliche Mittel – Private Investitionen
Wissensfaktoren	Kann Europa sich das Wissen aneignen, das für die Entwicklung von QCom-Technologien, die Ausbildung von Fachkräften und die Sicherung von Arbeitsplätzen (im erforderlichen Umfang) erforderlich ist?	+ Ermöglichende Technologien – Schnittstelle zu klassischen Technologien
Marktfaktoren	Kann Europa in Lieferketten eintreten oder diese aufbauen und einen relevanten Markt schaffen?	+ Potenzieller Markt (öffentliche Einrichtungen) – Endnutzer aus der Industrie
Institutionelle Faktoren	Sind die relevanten Rahmenbedingungen innnovationsfördernd (politisch, regulatorisch, gesellschaftlich, ökologisch usw.)?	+ Engagement der Behörden – Zulassungen und Zertifizierungen

Kostenfaktoren

Gegenwärtig werden die Herausforderungen, die mit den Kosten für die Innovation von QCom verbunden sind, durch die öffentliche Finanzierung in Europa in angemessener Weise angegangen. Die in den Abschnitten 5.4 und 5.5 beschriebenen europäischen und nationalen Förderprogramme (einschließlich EuroQCI) bieten eine gute Ausgangsbasis, um das Risiko und die Kosten der Entwicklung von QCom-Technologien zu decken. Dennoch fordern einige Expert:innen umfangreichere Förderprogramme, insbesondere für die Einrichtung von Großprojekten in Europa. Die privaten Investitionen hingegen sind derzeit sehr begrenzt. Um die Entwicklung von QCom voranzutreiben, sind weitere Investitionen der Industrie in Europa dringend erforderlich.

In den kommenden Jahren sind erhebliche Investitionen in die europäische QKD-Infrastruktur erforderlich, um eine großangelegte Umsetzung zu ermöglichen. QKD-Systeme, die derzeit kommerzialisiert werden, sind immer noch teuer und erfordern oft eine spezielle Infrastruktur, wie z. B. Dark Fibers. Die damit verbundenen hohen Investitionen bergen ein hohes wirtschaftliches Risiko für private Akteure.

Da die öffentlichen Mittel derzeit für Projekte mit begrenztem Zeitrahmen ausgegeben werden, die wiederum mit Strategien mit begrenztem Zeithorizont verbunden sind, kann nicht gesichert von einer kontinuierlichen Finanzierung ausgegangen werden. Die Schwerpunkte der Regierungen können sich im Laufe der Zeit verschieben, insbesondere wenn diese nach Wahlen wechseln. Diese Ungewissheit stellt ein Investitionsrisiko für jene Institutionen und Unternehmen dar, die von öffentlichen Mitteln abhängig sind.

Wissensfaktoren

Die europäische QCom-Forschung ist international gut etabliert und ein breites Wissen über die erforderlichen Technologien (z. B. Photonik) wird von Universitäten, Forschungseinrichtungen und Technologieunternehmen bereitgestellt (siehe auch Abschnitt 5.1). Insbesondere das Fachwissen in den Grundlagentechnologien wird als großer Vorteil für Europa angesehen. Das Wissen, das für die Entwicklung der meisten wesentlichen Komponenten für QCom-Technologien benötigt wird, ist in Europa vorhanden, wenn auch nicht für das gesamte Spektrum der Ansätze für QCom und verwandte Technologien. Während Europa über Fachwissen in der Optik verfügt (z. B. Technologieführerschaft bei photonischen Chips), könnte es noch an Kompetenz in der Entwicklung und Produktion von Mikroelektronik mangeln. Qualifikationen sind möglicherweise nicht in allen europäischen Ländern gleichermaßen vorhanden, was zu potenziellen Herausforderungen bei der Schaffung einer europäischen Technologiesouveränität in der Zukunft führen könnte. Nichtsdestotrotz bewerteten die Expert:innen den Status quo des europäischen Wissens in QCom als die am wenigsten problematische der vier diskutierten Dimensionen.

Auch wenn sich in Europa QCom damit in einer guten Ausgangsposition befindet, sind in einigen Bereichen noch tiefere Kenntnisse erforderlich. Die wichtigsten Parameter, mit denen man sich befassen muss, sind die Robustheit und die Schlüsselrate der jeweiligen Technologien. Das Design und die Implementierung der Schnittstelle von QCom-Technologien mit klassischen Technologien ist eine weitere große Herausforderung, die bisher möglicherweise noch nicht ausreichend beachtet wurde. Vertieftes Wissen über die relevanten Sicherheitsaspekte und potenziellen Sicherheitsrisiken von QCom-Technologien könnte noch erforderlich sein. Darüber hinaus befinden sich einige Technologien für spezifische QCom-Ansätze, wie z. B. Quantenrepeater, noch in einem sehr niedrigen Reifegrad und benötigen für die weitere Entwicklung wissenschaftliche Durchbrüche.

Neben der Bewältigung dieser Herausforderungen in Forschung und Entwicklung ist der Wissenstransfer in die Industrie erforderlich und stellt eine zentrale Herausforderung bei der Kommerzialisierung von QCom-Technologien dar. Dazu gehört die Ausbildung von qualifizierten Arbeitskräften und QCom-Spezialisten, was sich als besonders schwierig erweisen kann, da dies gleichzeitig tiefgreifende technische und interdisziplinäre Kompetenzen erfordert, in z. B. Quantenphysik, Informatik und Kommunikationstechnologien. Darüber hinaus muss die Aufklärung potenzieller Endnutzer in der Industrie (z. B. Banken, medizinische Einrichtungen usw.) und in öffentlichen Einrichtungen (z. B. Ministerien) über die Notwendigkeit einer sicheren Kommunikation, die Bedrohung durch die Entwicklungen im Quantencomputing und die potenziellen Lösungen, die die PQK- und QCom-Technologien bieten, intensiviert werden. Diese Wissensverbreitung sollte in der gesamten Gesellschaft weiter ausgebaut werden, um das Bewusstsein zu schärfen und die Akzeptanz der Technologie zu fördern. Da Quantentechnologien oft als "spukhaft" oder nicht-intuitiv beschrieben werden, könnten ihre konkreten Realisierungen und Auswirkungen auf die Gesellschaft von uninformierten Interessengruppen übersehen oder nicht antizipiert werden.

Schließlich ist die Frage, welche Rolle die Quantenkommunikation in der künftigen Kommunikationslandschaft spielen kann, noch offen. Es sind weitere Erkenntnisse darüber erforderlich, welche Art von QCom-Technologien in welchen Anwendungen und in welchem Umfang benötigt werden. Eine fundiertere Vorstellung davon, wie die europäische QCom-Wertschöpfung aussehen könnte und wie sich potenzielle Märkte entwickeln werden, ist für die Entwicklung entsprechender Strategien von entscheidender Bedeutung.

Marktfaktoren

Aktuell ist noch nicht abzusehen in welchem Zeitrahmen sich Märkte für QCom-Technologien entwickeln werden. Da staatliche Einrichtungen auf sichere Kommunikationsnetze angewiesen sind, gibt es hier bereits ein erhebliches Marktpotenzial für QCom-Technologien in Europa. Außerdem

stellen die vielen aktiven Akteure in der QCom-Wertschöpfungskette eine gute Ausgangsbasis für den Aufbau von Zulieferstrukturen für die entsprechenden Komponententechnologien in Europa dar. Eine Marktdurchdringung ist jedoch nur möglich, wenn die bestehenden Herausforderungen bewältigt werden können.

Staatliche Einrichtungen und öffentliche Organisationen können QCom-Technologien nur einsetzen, wenn diese von der jeweiligen Behörde (in Deutschland: Bundesamt für Sicherheit in der Informationstechnik, BSI) zugelassen sind. Derzeit ist noch keine QCom-Technologie von diesen Akteuren zugelassen, da noch kein zufriedenstellender Sicherheitsnachweis erbracht werden konnte. Da die Entstehung dieses zulassungspflichtigen Marktes von einigen wenigen nationalen Behörden gesteuert wird, ist die Vorhersage seiner Größe mit großer Unsicherheit verbunden, da er durch nationale Grenzen fragmentiert bleiben wird.

Dennoch ist QCom derzeit stark von dem Markt abhängig, der sich auf der Grundlage der europäischen öffentlichen Finanzierung im Aufbau befindet. Öffentliche Institutionen als potenzielle "Early Adopters" spielen in diesem Technologiefeld eine sehr wichtige Rolle, da ein substanzieller privater Markt noch nicht erkennbar ist. Das Fehlen eines solchen Marktes beraubt die QCom-Technologien der Möglichkeit, "am Markt zu lernen", d. h. die mit den frühen Generationen gemachten Erfahrungen für die Weiterentwicklung der jeweiligen Technologien zu nutzen.

Darüber hinaus ist die Rolle, die die verschiedenen Akteure bei der Wertschöpfung spielen, nach wie vor unklar. Dies führt zu Unsicherheiten hinsichtlich der Fähigkeiten, die von den verschiedenen Akteuren entwickelt werden sollten, und könnte gleichzeitig die Übernahme der Technologie durch die Endnutzer behindern (z. B. Wer wird das System dem Endnutzer zur Verfügung stellen – Systementwickler oder Telekommunikationsunternehmen?)

Telekommunikationsunternehmen können recht groß sein, und in einigen Ländern gibt es daher nur wenige Anbieter. Wenn ein solches Unternehmen eine beträchtliche Marktmacht entwickelt, könnte es potenziell die konzertierten Bemühungen anderer Interessengruppen, wie z. B. die europäischen Normungsaktivitäten, untergraben.

Institutionelle Faktoren

Wie oben diskutiert, hängt das Entstehen eines relevanten Marktes stark von den Entscheidungen und der Politik der Regierungen und öffentlichen Einrichtungen ab. Der politische Wille auf nationaler und europäischer Ebene ist insbesondere für QCom-Technologien erforderlich, da sie kritische Infrastrukturen betreffen.

Die Zulassungen, die von den entsprechenden Behörden erteilt werden müssen, wirken wie ein Gatekeeper für große Teile des potenziellen QCom-Marktes. Die Definition von Zertifizierungen für QCom-Systeme und -Komponenten, die von Prüflaboren ausgestellt werden könnten, könnte mehr Klarheit für Technologieanbieter und potenzielle Endnutzer schaffen. Für die Entwicklung von Zertifizierungen und Zulassungsprotokollen sind jedoch zuverlässige Sicherheitsnachweise erforderlich. Solange diese Nachweise nicht entwickelt werden oder von den jeweiligen Behörden nicht akzeptiert werden, stellen sie einen kritischen Engpass für die Einführung von QCom-Technologien dar.

Darüber hinaus wirken sich Vorschriften, die den Einsatz von im Ausland entwickelten QCom-Systemen verhindern, direkt auf die Marktzugänglichkeit aus. Obwohl inländische Unternehmen hiervon grundsätzlich profitieren könnten, schränken sie das exportbezogene Wertschöpfungspotenzial ein. Auch für die inländische Wertschöpfung inländischer Unternehmen kann dies eine Herausforderung darstellen, wenn die Verwendung von Komponenten bestimmter Anbieter verboten ist.

Normen für QCom-Technologien befinden sich noch in der Entwicklung. [204] Einerseits kann der derzeitige Mangel an Normen die Entwicklung von Technologien auf Systemebene und die Systemintegration hemmen. Andererseits erschwert dies den Vergleich verschiedener Technologien, Prototypen und Produkte in allen Reifestadien.

Die nationalen und europäischen öffentlichen Förderprogramme müssen wettbewerbsrechtliche Bestimmungen einhalten. Dieser und andere bürokratische Abläufe können die Realisierung von Großprojekten verzögern oder verhindern.

6.4 Maßnahmen

Viele der oben genannten Herausforderungen müssen von den Akteuren aus Wissenschaft, Industrie und Politik angegangen werden, um den Weg zur Erreichung der Technologiesouveränität im QCom zu ebnen. In den Experteninterviews wurde die Liste der Herausforderungen genutzt, um Maßnahmenempfehlungen für die jeweiligen Akteure zu formulieren. Auch hier erhebt die Liste der Maßnahmen keinen Anspruch auf Vollständigkeit, da sie ausschließlich auf den Interviewergebnissen basiert.

Tabelle 11: Herausforderungen und Maßnahmen zur Erreichung der Technologiesouveränität bei den Quantenkommunikationstechnologien in Europa

Dimension	Herausforderungen	Maßnahmen
Kostenfaktoren	• Hohe Investitionskosten für Infrastruktur und QCom-Technologien • Hohes Risiko für Investitionen • Verlässlichkeit der Investitionen	• Fortführung der öffentlichen Finanzierung • Kaufanreize für Endnutzer in der Industrie • Investitionen in europäische Infrastruktur
Wissensfaktoren	• Verständnis der Sicherheitsaspekte • Quantenrepeater • Bewusstsein für Sicherheitsrisiken in der Kommunikation und Wahrnehmung von QCom	• Bildungsprogramme für Interessenvertreter aus den relevanten Fachbereichen • Öffentlichkeitsarbeit • Förderung des Technologietransfers in die Industrie
Marktfaktoren	• Erste Marktdurchdringung zur Steigerung der Innovationsdynamik • Entstehen von Märkten jenseits öffentlicher Institutionen • Stark regulierte Märkte • Geschäftsmodelle	• Kaufanreize für Endnutzer aus der Industrie • Zusammenarbeit entlang der Wertschöpfungskette • Beseitigung von Hürden für Zulassungen
Institutionelle Faktoren	• Politische Strategien • Regulierungen • Sicherheitsnachweis	• Normungs- und Zertifizierungsaktivitäten • Investitionen in die Infrastruktur (EuroQCI)

Dimension	Herausforderungen	Maßnahmen
	• Bürokratie	• Zusammenarbeit der Behörden der europäischen Mitglieds-staaten • Verschlankung und Abbau der Bürokratie

Kostenfaktoren

Die meisten der befragten Expert:innen gaben an, dass das Niveau der öffentlichen Finanzierung im kommenden Jahrzehnt beibehalten werden sollte, um die Risiken für Wissenschaft und Industrie zu minimieren. Da große und stabile Finanzierungsprogramme die Hauptantriebskraft der derzeitigen Innovationsaktivitäten sind, ist ihre Fortsetzung von großer Bedeutung.

Darüber hinaus wurde eine stärkere Einbeziehung der industriellen Akteure für notwendig erachtet. Öffentliche Mittel könnten genutzt werden, um Anreize für Industrieaktivitäten zu schaffen und Märkte jenseits öffentlicher Einrichtungen zu öffnen. Eine Möglichkeit wäre die Einführung von Subventionen für Endnutzer, die QCom-Technologien kaufen.

Die Ausweitung der Produktion von QCom-Systemen wird für viele Start-ups und Unternehmen in diesem Bereich der nächste Schritt sein. Dies bietet die Möglichkeit, die Produktionskosten zu senken und die entsprechenden Produkte zu niedrigeren Preisen anzubieten.

Öffentliche Mittel sollten für Investitionen in QCom-relevante Infrastruktur in Europa verwendet werden, wie sie auch gegenwärtig den Aufbau von Testumgebungen fördert. Da eine sichere Kommunikationsinfrastruktur für Europa und seine Mitgliedsstaaten von entscheidender Bedeutung ist, kann sie nicht allein auf Investitionen des privaten Sektors beruhen.

Wissensfaktoren

Da für die Innovation und Einführung von QCom-Technologien qualifizierte Arbeitskräfte benötigt werden, sollten Ausbildungsprogramme entwickelt werden. Diese Programme sollten dem breiten Spektrum der benötigten Fähigkeiten Rechnung tragen. Sie könnten sich speziell an Fachleute bestimmter Disziplinen richten und darauf ausgelegt sein, eine interdisziplinäre Zusammenarbeit zu ermöglichen.

Weiteres Wissen über alle relevanten Sicherheitsaspekte kompletter QCom-Systeme, insbesondere der Schnittstellen zu konventionellen Technologien, sollte entwickelt und in Wissenschaft und Industrie verbreitet werden. Auf dieser Basis müssen relevante Sicherheitsnachweise entwickelt werden. Zusätzlich sollte der Bildungsbedarf weiterer Akteure der potenziellen QCom-Wertschöpfungskette, wie z. B. (potenziell zertifizierte) Prüflabore, identifiziert und entsprechende Schulungsprogramme entwickelt werden.

Darüber hinaus sollte in der Gesellschaft ein allgemeines Bewusstsein für QCom geschaffen werden, um potenzielle künftige Arbeitskräfte zu gewinnen. Diese Aufklärungsarbeit sollte sich auch mit dem weitverbreiteten Missverständnis befassen, dass es sich bei den Quantentechnologien um ein schlecht verstandenes Technologiefeld handelt und dass QCom auf „unerklärbaren" Effekten beruht, indem konkretere Diskussionen und Technologiedemonstrationen angeboten werden.

Die Akteure der Industrie sollten mehr investieren, um sich das entsprechende Wissen über Kommunikationssicherheit und die entsprechenden potenziellen Bedrohungen sowie über QCom im

Besonderen anzueignen. Dies sollte zu einem besseren Verständnis dafür führen, wo Maßnahmen ergriffen werden können oder sollten. Potenzielle Endnutzer sollten identifiziert und gezielt über den Mehrwert von QCom-Technologien informiert werden.

Marktfaktoren

Wie bereits erwähnt, sind gezielte Maßnahmen zur Schaffung von Märkten für „Early Adopters" für Technologieanbieter von großem Interesse. Zu diesen Maßnahmen könnten Investitionsanreize für potenzielle Endanwender aus der Industrie gehören. So könnten diese Erfahrungen mit den Technologien aus erster Hand sammeln. Außerdem würde dies Technologieanbietern eine Bühne bieten, um für ihre Dienstleistungen zu werben und Absatzmöglichkeiten eröffnen. Darüber hinaus könnte so die Schaffung von Referenztechnologien vorangetrieben werden. Die Nachfrage öffentlicher Einrichtungen nach QCom-Technologien sollte ebenfalls gefördert werden, sobald die Voraussetzungen für die entsprechenden Zulassungen der jeweiligen Behörden geschaffen sind.

Mögliche Geschäftsmodelle für alle Akteure in der QCom-Wertschöpfungskette sollten diskutiert und ihre Zusammenarbeit gefördert werden. Die Vernetzung zwischen Wissenschaft, Industrie und Politik sollte gefördert werden, um die Kommunikationskanäle für die Bedürfnisse der verschiedenen Akteure aneinander zu öffnen.

Institutionelle Faktoren

Transparente Anforderungen für Zulassungen sind für alle europäischen Mitgliedsstaaten wichtig. Die Schaffung von Zertifikaten könnte eine wichtige Rolle dabei spielen, klar definierte Richtlinien für weitere Technologieentwicklungen und die für die Systemproduktion zu schaffen.

Komplexe bürokratische Verfahren zur Erlangung von Fördermitteln oder auf anderen Stufen der QCom-Wertschöpfungskette sollten überarbeitet und, wo dies sinnvoll erscheint, vereinfacht, ersetzt oder ganz abgeschafft werden. Der regulatorische Rahmen sollte eine flexible Zusammenarbeit zwischen den relevanten Akteuren in Wissenschaft und Industrie in ganz Europa ermöglichen. Die Zuständigkeiten der politischen Akteure, insbesondere im Hinblick auf die Finanzierung der QCom-Infrastruktur (z. B. Welche Rolle spielen die jeweiligen Ministerien?), sollten geklärt werden. Die Harmonisierung der Aktivitäten der europäischen Mitgliedsstaaten sollte weiter gefördert werden, einschließlich eines engen Austauschs zwischen den nationalen Behörden über anstehende Entscheidungen und Strategien. Die Aktivitäten im Rahmen von EuroQCI sollten weitergeführt und ausgebaut werden mit dem Ziel, eine europäische QCom-Infrastruktur zu schaffen. Auch wenn nationale Strategien nicht vollständig durch europäische Strategien in diesem Bereich ersetzt werden können, sollte ein europäischer Flickenteppich von Regelungen und Zertifikaten möglichst vermieden werden.

Die Vernetzung aller Akteure entlang der Wertschöpfungskette sollte von den politischen Entscheidungsträger:innen gefördert werden, um das Bewusstsein für die anstehenden technologischen Entwicklungen zu schärfen. Darüber hinaus sollten QCom-Start-ups unterstützt werden, da sie der Technologieentwicklung und -umsetzung neue Impulse geben können.

7 Schlussfolgerungen

Die Quantenkommunikation stellt eine Gruppe strategisch wichtiger Technologien zur Gewährleistung sicherer Kommunikation und darüber hinaus gehende Anwendungen, wie z. B. zukünftig die Verbindung von Quantencomputern, dar. Einige der Technologien sind bereits kommerziell erhältlich, z. B. die Quantenschlüsselverteilung (QKD), wohingegen andere noch Gegenstand der Forschung sind.

Die Technologien der Quantenkommunikation lassen sich in drei Generationen einteilen: QKD nach dem "Prepare & Measure"-Prinzip, QKD mittels verschränkter Photonen und Quantenrepeater mit Verschränkungsverteilung. QKD kommt dabei dem Bedarf nach "quantensicherer" Kommunikation nach und stellt eine Möglichkeit des physikalischen sicheren Austauschs von kryptografischen Schlüsseln für eine sichere Kommunikation dar. QKD könnte insbesondere im Hochsicherheitsbereich (z. B. Bundesbehörden, Regierungen, Finanzwesen, Militär) Anwendung finden. Verschiedene Ausführungen dieser Technologie sind bereits kommerziell erhältlich. Herausforderungen auf dem Weg zu einem breiten Einsatz sind jedoch noch ausstehende Sicherheitsbeweise, hohe Kosten für neue Hardware und fehlendes Wissen bei potenziellen Anwendern über die Gefahren des Quantencomputings für etablierte Verschlüsselungsverfahren und potenzielle Lösungen (wie z. B. QKD). Über QKD hinaus stellen Quantenrepeater eine wichtige Technologie dar. Zum einen um die Reichweitenlimitation von QKD aufzulösen bzw. unabhängig von potenziell unsicheren "Trusted Nodes" zu werden und zum anderen um mittels Verschränkungsverteilung verteilte Quantensensorik zu ermöglichen und über längere Distanzen Quantencomputer miteinander zu verbinden. Letzteres könnte die Leistungsfähigkeit und Einsatzmöglichkeiten von Quantencomputern drastisch erhöhen.

Insgesamt ist in einigen Technologien (wie z. B. beim Quantenrepeater) noch einige Forschungs- und Entwicklungsarbeit nötig, um marktreife Produkte zu erhalten und die Potenziale der Quantenkommunikation voll ausnutzen zu können. Darüber hinaus müssen die Hindernisse zu einem breiten Einsatz auf dem Markt beseitigt werden, inkl. Sicherheitsbeweise, Zertifizierung und Zulassung. Dazu ist eine enge Zusammenarbeit verschiedener Akteure aus Wissenschaft, Wirtschaft und öffentlicher Akteure (Behörden, Politik) nötig.

Aus diesen Gründen wurde die Quantenkommunikation international als strategisch relevantes Forschungsfeld anerkannt. In der Folge haben zahlreiche Länder entsprechende Forschungs- und Förderungsstrategie und -programme aufgesetzt. Deutschland und Europa nehmen hier im internationalen Vergleich eine wichtige Rolle ein und befinden sich in Forschung und Entwicklung auf Augenhöhe, was sich an hohen Publikations- und Patentierungsaktivitäten zeigt. Aufgrund der hohen strategischen Relevanz der Quantenkommunikation spielen Überlegungen zu technologischer Souveränität eine zunehmend wichtige Rolle. Auch Deutschland und die EU sollte hier weiterhin reflektieren und diskutieren, welche Ziele erreicht werden sollen und welche Maßnahmen ergriffen werden müssen, um das anvisierte Maß an technologischer Souveränität zu erreichen.

Die Quantenkommunikation stellt ein strategisch wichtiges Thema dar und es besteht großes Interesse von zahlreichen Ländern und Regionen an diesen Technologien. Auch Deutschland und Europa müssen weiterhin reflektieren, in welchem Rahmen die Technologienentwicklung kontinuierlich unterstützt werden sollte, um das selbstgesteckte strategische Ziel der technologischen Souveränität in der Quantenkommunikation zu erreichen.

8 Danksagungen

Die Autoren bedanken sich für die Förderung durch das Bundesministerium für Bildung und Forschung (BMBF), Deutschland sowie für die Koordination durch den Projektträger VDI/VDE Innovation und Technik GmbH.

Förderkennzeichen: 16KISQ116, 16KISQ115, 16KISQ112K

Wir möchten uns bei allen Expert:innen aus Wissenschaft und Industrie bedanken, die uns durch ihre Teilnahme an Interviews unterstützt haben. Darüber hinaus möchten wir uns bei unseren Kolleg:innen vom Fraunhofer ISI bedanken: Karin Herrmann für das Layouten; Paul Städter für Recherchen zu Marktstudien; Gillian Bowman-Köhler für englische Sprachkorrekturen und Übersetzungen; und Prof. Ulrich Schmoch für die Patent- und Publikationsrecherche.

Wir danken unseren Kollegen Sebastian Koke, Nino Walenta, Thorsten A. Goebel, Ralf-Peter Braun und Nicolas Spethmann für wertvollen Input in Bezug auf die Testbedinfrastruktur in Deutschland.

Referenzen

[1] Bundesministerium für Bildung und Forschung 2024 *Startseite — Vernetzung und Sicherheit digitaler Systeme* https://www.forschung-it-sicherheit-kommunikationssysteme.de/ (accessed 12 May 2024)

[2] Cordis 2024 *Projects & results | CORDIS | European Commission* https://cordis.europa.eu/projects (accessed 12 May 2024)

[3] National Quantum Initiative 2021 *National Quantum Coordination Office (NQCO)* https://www.quantum.gov/ (accessed 12 May 2024)

[4] UKRI 2024 *UK National Quantum Technologies Programme* https://uknqt.ukri.org/ (accessed 12 May 2024)

[5] Cabinet Office Home Page 2024 *Quantum Technology Innovation* https://www8.cao.go.jp/cstp/ryoshigijutsu/ryoshigijutsu.html (accessed 16 May 2024)

[6] Parker E *et al* 2022 *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*

[7] McKinsey & Company 2023 *McKinsey Quantum Technology Monitor 2023 | McKinsey & Company* https://www.mckinsey.com/de/news/presse/quantum-technology-monitor-2023-marktanalyse-quantencomputer-quantenkommunikation-quantensensorik (accessed 15 May 2024)

[8] Edler J *et al* 2020 *Technologiesouveränität. Von der Forderung zum Konzept (Policy Brief 02 / 2020)*

[9] OECD Publishing *The Measurement of Scientific and Technological Activities, Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data* (Paris)

[10] Bundesamt für Sicherheit in der Informationstechnik 2020 *Entwicklungsstand Quantencomputer* (Bundesamt für Sicherheit in der Informationstechnik)

[11] Bundesministerium für Bildung und Forschung 2018 *Quantentechnologien – von den Grundlagen zum Markt: Rahmenprogramm der Bundesregierung* (Bundesministerium für Bildung und Forschung)

[12] Bundesamt für Sicherheit in der Informationstechnik *Post-Quanten-Kryptografie* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Post-Quanten-Kryptografie/post-quanten-kryptografie_node.html (accessed 4 Jun 2024)

[13] Müller R and Greinert F 2023 *Quantentechnologien: Für ingenieure (De Gruyter Studium)* (Berlin, Boston: De Gruyter)

[14] Bundesamt für Sicherheit in der Informationstechnik 2024 *Daten quantensicher verschlüsseln: BSI bewertet verfügbare Technologien* https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240126_QKD-Positionspapier.html (accessed 12 Jun 2024)

[15] Hannes Hübel, Fabian Laudenbach, Martin Suda, Martin Stierle 2018 *Strategische Analyse der Möglichkeiten zur stärkeren Industrialisierung der Ergebnisse der österreichischen Quantenforschung* (Studie für das bmvit)

[16] Ralph T C 1999 Continuous variable quantum cryptography *Phys. Rev. A* **61**

[17] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states *Physical review letters* **88** 57902

[18] Kikuchi K 2016 Fundamentals of Coherent Optical Fiber Communications *J. Lightwave Technol.* **34** 157–79

[19] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 Experimental demonstration of long-distance continuous-variable quantum key distribution *Nature Photon* **7** 378–81

[20] Defense Advanced Research Projects Agency *Quantum Key Distribution Network* https://www.darpa.mil/about-us/timeline/quantum-key-distribution-network (accessed 6 Jun 2024)

[21] CORDIS - Forschungsergebnisse der EU *Development of a Global Network for Secure Communication based on Quantum Cryptography* (CORDIS - Forschungsergebnisse der EU)

[22] Stucki D *et al* 2011 Long-term performance of the SwissQuantum quantum key distribution network in a field environment *New J. Phys.* **13** 123001

[23] Xu F *et al* 2009 Field experiment on a robust hierarchical metropolitan quantum cryptography network *Chin. Sci. Bull.* **54** 2991–7

[24] Sasaki M *et al* 2011 Field test of quantum key distribution in the Tokyo QKD Network *Optics express* **19** 10387–409

[25] Steve Dent 2013 *Los Alamos National Lab has had quantum-encrypted internet for over two years* https://www.engadget.com/2013-05-06-quantum-encrypted-internet-los-alamos.html?guccounter=1 (accessed 6 Jun 2024)

[26] Deutsches Zentrum für Luft- und Raumfahrt 2021 *Erste quantengesicherte Videokonferenz zwischen zwei Bundesbehörden* https://www.dlr.de/de/aktuelles/nachrichten/2021/03/20210810_erste_quantengesicherte_videokonferenz_zwischen_bundesbehoerden (accessed 6 Jun 2024)

[27] Chen Y-A *et al* 2021 An integrated space-to-ground quantum communication network over 4,600 kilometres *Nature* **589** 214–9

[28] QuantumXchange *Continuously Monitor & Manage Cryptographic Risk in the Enterprise Today and in the Post-Quantum Future* https://quantumxc.com/ (accessed 6 Jun 2024)

[29] Chicago Quantum Exchange *Chicago Quantum Exchange Homepage* https://chicagoquantum.org/ (accessed 11 Jun 2024)

[30] Brookhaven National Laboratory *Quantum Network Facility* https://www.bnl.gov/instrumentation/quantum/index.php (accessed 6 Jun 2024)

[31] Center for Quantum Networks *Building the Quantum Internet* https://cqn-erc.org/ (accessed 6 Jun 2024)

[32] Denis Sukachev and Mihir Bhaskar 2022 *Announcing the AWS Center for Quantum Networking* https://aws.amazon.com/de/blogs/quantum-computing/announcing-the-aws-center-for-quantum-networking/ (accessed 12 Jun 2024)

[33] QuTech *Division of Quantum Internet* https://qutech.nl/research-engineering/quantum-internet/ (accessed 6 Jun 2024)

[34] Lord A *et al* 2023 London Quantum-Secured Metro Network *2023 Optical Fiber Communications Conference and Exhibition (OFC) 2023 Optical Fiber Communications Conference and Exhibition (OFC) (San Diego, CA, USA, 5 Mar 2023 - 9 Mar 2023)* (IEEE) pp 1–4

[35] Dynes J F *et al* 2019 Cambridge quantum network *npj Quantum Inf* **5**

[36] Woodward R I, Dynes J F, Wright P, White C, Parker R C, Wonfor A, Yuan Z L, Lord A and Shields A J Quantum Key Secured Communications Field Trial for Industry 4.0 *Optical Fiber Communication Conference (OFC) 2021 Optical Fiber Communication Conference (Washington, DC)* (Washington, D.C.: Optica Publishing Group) Th4H.4

[37] European Commission 2024 *Europäische Quantenkommunikationsinfrastruktur (EuroQCI)* https://digital-strategy.ec.europa.eu/de/policies/european-quantum-communication-infrastructure-euroqci (accessed 12 Jun 2024)

[38] Liu Y *et al* 2023 Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance *Physical review letters* **130** 210801

[39] Li W *et al* 2023 High-rate quantum key distribution exceeding 110 Mb s–1 *Nature Photon* **17** 416–21

[40] Grünenfelder F *et al* 2023 Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems *Nature Photon* **17** 422–6

[41] Tian Y, Zhang Y, Liu S, Wang P, Lu Z, Wang X and Li Y 2023 High-performance long-distance discrete-modulation continuous-variable quantum key distribution *Optics letters* **48** 2953–6

[42] Zhang Y, Bian Y, Li Z, Yu S and Guo H 2023 *Continuous-variable quantum key distribution system: past, present, and future* (arXiv)

[43] QuNET *Die QuNET-Initiative. Hochsichere Kommunikation durch Quantenphysik* https://qunet-initiative.de/start/ (accessed 6 Jun 2024)

[44] Schirmprojekt Quantenkommunikation Deutschland *Innovationen für die Quantenkommunikation in Deutschland* https://www.squad-germany.de/ (accessed 6 Jun 2024)

[45] Bundesministerium für Bildung und Forschung *Q-net-Q Mehr Sicherheit in bestehenden Netzen durch Quantenkommunikation* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/q-net-q (accessed 6 Jun 2024)

[46] Bundesministerium für Bildung und Forschung *Forschung Agil - Innovative Verfahren für Quantenkommunikationsnetze* https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/agil-call-6 (accessed 12 Jun 2024)

[47] Zatoukal B *et al* 2021 OpenQKD Use-case for Securing Sensitive Medical Data at rest and in transit *2021 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC) 2021 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC) (Munich, Germany, 21.06.2021 - 25.06.2021)* (IEEE) p 1

[48] Bundesministerium für Bildung und Forschung *DemoQuanDT: Quantenschlüsselaustausch im deutschen Telekommunikationsnetz für höhere IT-Sicherheit* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/demoquandt (accessed 6 Jun 2024)

[49] Bundesministerium für Bildung und Forschung *Projekt 6G-QuaS: Ein quantensicheres Industrienetzwerk* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/6g-quas (accessed 6 Jun 2024)

[50] Bundesministerium für Bildung und Forschung *Projekt DE-QOR: Leistungsfähige Übertragungskomponenten für quantensichere Glasfaserkommunika-tion im urbanen Raum* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/de-qor (accessed 6 Jun 2024)

[51] Bundesministerium für Bildung und Forschung *Projekt QUIET: Ein Quanteninternet der Dinge* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/quiet (accessed 6 Jun 2024)

[52] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Physical review letters* **67** 661–3

[53] Bennett C H, Brassard G and Mermin N D 1992 Quantum cryptography without Bell's theorem *Physical review letters* **68** 557–9

[54] Heindel T, Kim J-H, Gregersen N, Rastelli A and Reitzenstein S 2023 Quantum dots for photonic quantum information technology *Adv. Opt. Photon.* **15** 613

[55] Weedbrook C 2013 Continuous-variable quantum key distribution with entanglement in the middle *Phys. Rev. A* **87**

[56] Du S, Wang P, Liu J, Tian Y and Li Y 2023 Continuous variable quantum key distribution with a shared partially characterized entangled source *Photon. Res.* **11** 463

[57] Kang D, Anirban A and Helmy A S 2016 Monolithic semiconductor chips as a source for broadband wavelength-multiplexed polarization entangled photons *Optics express* **24** 15160–70

[58] Joshi S K *et al* 2020 A trusted node-free eight-user metropolitan quantum communication network *Science advances* **6**

[59] Wengerowsky S, Joshi S K, Steinlechner F, Hübel H and Ursin R 2018 An entanglement-based wavelength-multiplexed quantum communication network *Nature* **564** 225–8

[60] Yin J *et al* 2020 Entanglement-based secure quantum cryptography over 1,120 kilometres *Nature* **582** 501–5

[61] Basso Basset F *et al* 2021 Quantum key distribution with entangled photons generated on demand by a quantum dot *Science advances* **7**

[62] Schimpf C, Reindl M, Huber D, Lehner B, Da Covre Silva S F, Manna S, Vyvlecka M, Walther P and Rastelli A 2021 Quantum cryptography with highly entangled photons from semiconductor quantum dots *Science advances* **7**

[63] Quantum Communications Hub *Quantum security at all distance scales* https://www.quantumcommshub.net/research-community/about-the-hub/phase-2/ (accessed 6 Jun 2024)

[64] Pelet Y, Sauder G, Cohen M, Labonté L, Alibart O, Martin A and Tanzilli S 2022 *Operational entanglement-based quantum key distribution over 50 km of real-field optical fibres*

[65] Wengerowsky S *et al* 2019 Entanglement distribution over a 96-km-long submarine optical fiber *Proceedings of the National Academy of Sciences of the United States of America* **116** 6684–8

[66] Neumann S P, Buchner A, Bulla L, Bohmann M and Ursin R 2022 Continuous entanglement distribution over a transnational 248 km fiber link *Nature communications* **13** 6134

[67] Yicheng Shi, Soe Moe Thar, Hou Shun Poh, James A. Grieve, Christian Kurtsiefer and Alexander Ling 2020 Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber *Applied Physics Letters*

[68] Bundesministerium für Bildung und Forschung *Projekt Q-Sec-Pro: Neuartige IT-Sicherheit auf Quantenbasis* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/q-sec-pro (accessed 6 Jun 2024)

[69] Bundesministerium für Bildung und Forschung *Projekt Q-Fiber: Neue Lichtleitkabel für mehr Leistung, Bandbreite und Effizienz bei der Quantenkom-munikation* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/q-fiber (accessed 6 Jun 2024)

[70] Zapatero V, van Leent T, Arnon-Friedman R, Liu W-Z, Zhang Q, Weinfurter H and Curty M 2023 Advances in device-independent quantum key distribution *npj Quantum Inf* **9**

[71] Liu W-Z, Zhang Y-Z, Zhen Y-Z, Li M-H, Liu Y, Fan J, Xu F, Zhang Q and Pan J-W 2022 Toward a Photonic Demonstration of Device-Independent Quantum Key Distribution *Physical review letters* **129** 50502

[72] Nadlinger D P *et al* 2022 Experimental quantum key distribution certified by Bell's theorem *Nature* **607** 682–6

[73] Zhang W *et al* 2022 A device-independent quantum key distribution system for distant users *Nature* **607** 687–91

[74] Briegel H-J, Dür W, Cirac J I and Zoller P 1998 Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication *Physical review letters* **81** 5932–5

[75] Bundesministerium für Bildung und Forschung *Souverän. Digital. Vernetzt.: Forschungsprogramm Kommunikationssysteme* (Bundesministerium für Bildung und Forschung)

[76] Dias J and Ralph T C 2017 Quantum repeaters using continuous-variable teleportation *Phys. Rev. A* **95**

[77] Seshadreesan K P, Krovi H and Guha S 2020 Continuous-variable quantum repeater based on quantum scissors and mode multiplexing *Phys. Rev. Research* **2**

[78] Wu B-H, Zhang Z and Zhuang Q 2022 Continuous-variable quantum repeaters based on bosonic error-correction and teleportation: architecture and applications *Quantum Sci. Technol.* **7** 25018

[79] Bundesministerium für Bildung und Forschung *Projekt QR.X: Sichere faserbasierte Quantenkommunikation* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qr.x (accessed 6 Jun 2024)

[80] Krutyanskiy V *et al* 2023 Entanglement of Trapped-Ion Qubits Separated by 230 Meters *Physical review letters* **130** 50803

[81] Luo X-Y *et al* 2022 Postselected Entanglement between Two Atomic Ensembles Separated by 12.5 km *Physical review letters* **129** 50503

[82] van Leent T *et al* 2022 Entangling single atoms over 33 km telecom fibre *Nature* **607** 69–73

[83] Knaut C M *et al* 2024 Entanglement of nanophotonic quantum memory nodes in a telecom network *Nature* **629** 573–8

[84] Liu J-L *et al* 2023 *A multinode quantum network over a metropolitan area* (arXiv)

[85] Rakonjac J V, Grandi S, Wengerowsky S, Lago-Rivera D, Appas F and Riedmatten H de 2023 Transmission of light-matter entanglement over a metropolitan network

[86] Zhou Y, Malik P, Fertig F, Bock M, Bauer T, van Leent T, Zhang W, Becher C and Weinfurter H 2024 Long-Lived Quantum Memory Enabling Atom-Photon Entanglement over 101 km of Telecom Fiber *PRX Quantum* **5**

[87] Shen S *et al* 2023 Hertz-rate metropolitan quantum teleportation *Light, science & applications* **12** 115

[88] Lago-Rivera D, Rakonjac J V, Grandi S and Riedmatten H de 2023 Long distance multiplexed quantum teleportation from a telecom photon to a solid-state qubit *Nature communications* **14** 1889

[89] Kucera S *et al* 2024 *Demonstration of quantum network protocols over a 14-km urban fiber link* (arXiv)

[90] Langenfeld S, Thomas P, Morin O and Rempe G 2021 Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution *Physical review letters* **126** 230506

[91] Bergerhoff M, Elshehy O, Kucera S, Kreis M and Eschner J 2023 *Quantum repeater node with free-space coupled trapped ions* (arXiv)

[92] Hermans S L N, Pompili M, Beukers H K C, Baier S, Borregaard J and Hanson R 2022 Qubit teleportation between non-neighbouring nodes in a quantum network *Nature* **605** 663–8

[93] Kamin L, Shchukin E, Schmidt F and van Loock P 2023 Exact rate analysis for quantum repeaters with imperfect memories and entanglement swapping as soon as possible *Phys. Rev. Research* **5**

[94] Wallnöfer J, Hahn F, Wiesner F, Walk N and Eisert J 2022 ReQuSim: Faithfully simulating near-term quantum repeaters

[95] Da Silva F F, Avis G, Slater J A and Wehner S 2023 *Requirements for upgrading trusted nodes to a repeater chain over 900 km of optical fiber* (arXiv)

[96] Beukers H K C, Pasini M, Choi H, Englund D, Hanson R and Borregaard J *Tutorial: Remote entanglement protocols for stationary qubits with photonic interfaces* (arXiv)

[97] Beukers H K, Pasini M, Choi H, Englund D, Hanson R and Borregaard J 2024 Remote-Entanglement Protocols for Stationary Qubits with Photonic Interfaces *PRX Quantum* **5**

[98] Bassoli R, Boche H, Deppe C, Ferrara R, Fitzek F H P, Janssen G and Saeedinaeeni S (eds) 2021 *Quantum Communication Networks (Foundations in Signal Processing, Communications and Networking)* (Cham: Springer International Publishing)

[99] Azuma K, Economou S E, Elkouss D, Hilaire P, Jiang L, Lo H-K and Tzitrin I 2023 Quantum repeaters: From quantum networks to the quantum internet *Rev. Mod. Phys.* **95**

[100] National Quantum Initiative *The Federal Source and Gateway to Quantum R&D across the U.S. Government* https://www.quantum.gov/ (accessed 6 Jun 2024)

[101] Cabinet Office *Moonshot Research and Development Program* https://www8.cao.go.jp/cstp/english/moonshot/top.html (accessed 6 Jun 2024)

[102] Quantum Internet Alliance *The QIA Story* https://quantuminternetalliance.org/qia-story/ (accessed 6 Jun 2024)

[103] 24 Market Reports 2023 *Quantum Key Distribution (QKD) Market, Global Outlook and Forecast 2023-2030* (24 Market Reports)

[104] 360 Market Updates 2022 *GLOBAL QUANTUM KEY DISTRIBUTION (QKD) MARKET RESEARCH REPORT 2022(STATUS AND OUTLOOK)* (360 Market Updates)

[105] 360 ResearchReports 2022 *GLOBAL QUANTUM KEY DISTRIBUTION (QKD) MARKET RESEARCH REPORT 2022* (360 ResearchReports)

[106] 360 ResearchReports 2023 *GLOBAL QUANTUM COMMUNICATION MARKET GROWTH (STATUS AND OUTLOOK) 2023-2029* (360 ResearchReports)

[107] Adroit Market Research 2020 *Quantum Cryptography Market By Component (Hardware, Software, Services), Algorithm Type (Symmetric Key, Asymmetric Key), Enterprise Size (Small*

and Medium Enterprise (SMEs), Large Enterprise), Encryption Type (Network Encryption, Database Encryption, Application Security, Cloud Encryption), Deployment Protocol (TSL/SSL Protocol, BB84 Protocol), Application (Simulation, Optimization, Sampling) and Region Global Forecast 2021 to 2028 (Adroit Market Research)

[108] Adroit Market Research 2023 *Quantum Key Distribution (QKD) Market by Security Type (Network Security, Application Security), by Application (Financial, Government, Military and Defense, and Others) and by Region (North America, Europe, Asia Pacific, Middle East and Africa, and South America), Global Forecast 2021 to 2031* (Adroit Market Research)

[109] Allied Market Research 2023 *Quantum Cryptography Market by Organizational Size (Small Medium Enterprise, Large Enterprise), by Component (Solution, Service, Solutions), by Security Type (Application Security, Network Security) and by Industry Vertical (IT Telecom, BFSI, Healthcare and life science, Healthcare, Automotive, Retail, Government Defense, Others): Global Opportunity Analysis and Industry Forecast, 2023-2032* (Allied Market Research)

[110] ASD Reports 2023 *Quantum Cryptography Market - Global Forecast to 2028* (ASD Reports)

[111] astute analytica 2023 *Global Quantum Secure Communication Market: By Component (Hardware, Software, Services); Type: Quantum Key Distribution, Quantum Teleportation); Application: (Banking Industry, Financial Industry, Government and defense industry, Lotteries and online gaming, Business, Others), and By Region - Market Size, Industry Dynamics, Opportunity Analysis and Forecast for 2023-2031* (astute analytica)

[112] astute analytica 2023 *Quantum Cryptography and Network Market: By Component (Solutions, Solutions); Security Type (Network security, Application security); Network Type (Quantum Key Distribution, Quantum Teleportation, Others); Cryptography Encryption Types (Symmetric, Symmetric); Cryptography Encryption Algorithms (Triple Data Encryption Standard (DES), RSA Encryption, Advanced Encryption Standards (AES), Hash algorithm); Enterprise Size (Small and Medium Enterprises, Large Enterprises); End User (BFSI, IT and Telecom, Retail, Media and Entertainment, Government and Public Sector, Manufacturing, Healthcare, Others) and By Region - Market Size, Industry Dynamics, Opportunity Analysis and Forecast for 2023-2031* (astute analytica)

[113] bcc Research 2019 *Global Market for Quantum Cryptography* (bcc Research)

[114] Business Growth Reports 2022 *Global Quantum Communication Market Size, Status and Forecast 2022-2028* (Business Growth Reports)

[115] Data Bridge 2021 *Global Quantum Cryptography Market – Industry Trends and Forecast to 2028* (Data Bridge)

[116] Data Intelo 2022 *Quantum Secure Communication Market Research Report* (Data Intelo)

[117] FactMR 2021 *Quantum Cryptography Market* (FactMR)

[118] FIOR MARKETS 2019 *Global Quantum Cryptography Market by Component (Solutions, Services), Services (Consulting and Advisory, Deployment and Integration, Support and Maintenance), Vertical, Application, Region, Global Industry Analysis, Market Size, Share, Growth, Trends, and Forecast 2018 to 2025* (FIOR MARKETS)

[119] Fusion Market Research 2021 *Quantum Key Distribution (QKD) Market - Global Outlook and Forecast 2021-2027* (Fusion Market Research)

[120] Glob Market Reports 2023 *2023-2031 Report on Global Quantum Key Distribution (QKD) Market by Player, Region, Type, Application and Sales Channel* (Glob Market Reports)

[121] Global Information 2023 *Global Quantum Communication Market Size, Status and Forecast 2023-2029* (Global Information)

[122] Global Market Estimates 2023 *Global Quantum Cryptography Market, Size, Trends & Analysis - Forecasts To 2026 By Component (Solutions, Services), By Application (Network Encryption, Database Encryption, Application Security, Cloud Encryption), By Industry (BFSI, Healthcare & Life Sciences, Government and Defense, IT & Telecom, Energy & Utility, Retail & Ecommerce, Others), By Region (North America, Europe, Asia Pacific and Rest of the World); Vendor Landscape, End User Landscape and Company Market Share Analysis & Competitor Analysis* (Global Market Estimates)

[123] GlobalInfoResearch 2023 *Global Quantum Key Distribution (QKD) Market 2023 by Company, Regions, Type and Application, Forecast to 2029* (GlobalInfoResearch)

[124] HTF Market Intelligence 2022 *Quantum Communication Device Market, Global Outlook and Forecast 2022-2028* (HTF Market Intelligence)

[125] IMR Reports 2023 *Global Quantum Key Distribution (QKD) Market by Solution, Services, Application, and Region - Global Forecast to 2028* (IMR Reports)

[126] Industry ARC 2023 *Quantum Cryptography Market - Forecast(2023 - 2028)* (Industry ARC)

[127] Industry Growth Insight 2022 *Global Quantum Key Distribution (QKD) Market by Type (Rigid 1-2Sided, Standard Multilayer, HDI, IC Substrate, Flexible Circuits, Rigid Flex, Others, Quantum Key Distribution (QKD), By Application (Financial, Government, Military & Defense, Others) And By Region (North America, Latin America, Europe, Asia Pacific and Middle East & Africa), Forecast From 2022 To 2030* (Industry Growth Insight)

[128] Industry Research 2022 *GLOBAL QUANTUM CRYPTOGRAPHY MARKET SIZE, STATUS AND FORECAST 2022* (Industry Research)

[129] Industry Research 2022 *GLOBAL QUANTUM KEY DISTRIBUTION (QKD) MARKET RESEARCH REPORT 2022(STATUS AND OUTLOOK)* (Industry Research)

[130] Ken Research 2021 *Global Quantum Cryptography Market Outlook: Ken Research* (Ken Research)

[131] Knowledge Sourcing Intelligence 2022 *Quantum Cryptography Market Size, Share, Opportunities, COVID-19 Impact, And Trends By Component (Hardware, Software, Services), By Enterprise Size (Small, Medium, Large), By Application (Network Security, Database Encryption, Application Security, Others), By End-User Industry (Communication And Technology, Government, Military And Defence, Retail, Healthcare, BFSI, Others), And By Geography - Forecasts From 2021 To 2026* (Knowledge Sourcing Intelligence)

[132] Market Growth Reports 2021 *Global Quantum Communication Market Size, Status and Forecast 2021-2027* (Market Growth Reports)

[133] Market Growth Reports 2022 *Global Quantum Key Distribution (QKD) Market 2022 by Company, Regions, Type and Application, Forecast to 2028* (Market Growth Reports)

[134] Market Growth Reports 2022 *Global Quantum Key Distribution (QKD) Market Research Report 2022* (Market Growth Reports)

[135] Market Growth Reports 2023 *Global Quantum Key Distribution (QKD) Industry Research Report 2023, Competitive Landscape, Market Size, Regional Status and Prospect* (Market Growth Reports)

[136] Market Growth Reports 2023 *Global Quantum Key Distribution (QKD) Market Research Report 2023* (Market Growth Reports)

[137] Market Reports world 2021 *GLOBAL QUANTUM COMMUNICATION MARKET REPORT, HISTORY AND FORECAST 2016-2027, BREAKDOWN DATA BY COMPANIES, KEY REGIONS, TYPES AND APPLICATION* (Market Reports world)

[138] Market Reports world 2021 *Global Quantum Communication Market Size, Status and Forecast 2021-2027* (Market Reports world)

[139] Market Reports world 2023 *GLOBAL QUANTUM KEY DISTRIBUTION (QKD) AND QUANTUM CRYPTOGRAPHY (QC) MARKET GROWTH (STATUS AND OUTLOOK) 2023-2029* (Market Reports world)

[140] Market Reports world 2023 *GLOBAL QUANTUM KEY DISTRIBUTION (QKD) MARKET RESEARCH REPORT 2023* (Market Reports world)

[141] Market Research Future 2023 *Quantum Cryptography Market Research Report By Service (Support and Maintenance, Deployment and Integration, Consulting), by Application (Database Encryption, Application Security, Network Security), Vertical and by Component– Global Forecast till 2030* (Market Research Future)

[142] Market Research intellext 2023 *Global Quantum Cryptography Services Market Size By Product, By Application, By Geography, Competitive Landscape And Forecast* (Market Research intellext)

[143] Market Research Update 2023 *Quantum Key Distribution (QKD) Market Size Report By Type (Rigid 1-2Sided, Standard Multilayer, IC Substrate, Flexible Circuits, Rigid Flex, Others), By Application (Financial, Government, Military & Defense, Others), By Region (North America, Latin America, Europe, Asia Pacific, Middle East, and Africa) - Share, Trends, Outlook and Forecast 2023-2028. Read more at: https://www.marketresearchupdate.com/industry-growth/quantum-key-distribution-qkd-market-size-409367* (Market Research Update)

[144] Market Research world 2022 *GLOBAL QUANTUM KEY DISTRIBUTION QKD MARKET RESEARCH REPORT 2022(STATUS AND OUTLOOK)* (Market Research world)

[145] Market Research.com 2022 *Global Quantum Key Distribution (QKD) Market Size, Status and Forecast 2022-2028* (Market Research.com)

[146] Market Research.com 2023 *Global Quantum Key Distribution QKD Market Research Report 2023(Status and Outlook)* (Market Research.com)

[147] Market Research.com 2023 *Quantum Cryptography Market by Offering (Solutions and Services), Security Type (Network Security and Application Security), Vertical (Government, Defense, BFSI, Healthcare, Retail, and eCommerce) and Region - Global Forecast to 2028* (Market Research.com)

[148] Market Stats Ville 2022 *Quantum Secure Communication Market 2022* (Market Stats Ville)

[149] Market.biz 2021 *Global Quantum Key Distribution (QKD) Market By Type (Rigid 1-2Sided, Standard Multilayer, HDI, IC Substrate, Flexible Circuits, Rigid Flex, By Application (Financial, Government, and Military & Defense), By Country, and Manufacture - Industry Segment, Competition Scenario and Forecast by 2030* (Market.biz)

[150] Markets and Markets 2023 *Quantum Cryptography Market by Offering (Solutions and Services), Security Type (Network Security and Application Security), Vertical (Government, Defense, BFSI, Healthcare, Retail, and eCommerce) and Region - Global Forecast to 2028* (Markets and Markets)

[151] MMR 2022 *Quantum Cryptography Market – Global Industry Analysis And Forecast (2022-2029)* (MMR)

[152] Mobility Foresights 2023 *Global Quantum Key Distribution Market 2022-2030* (Mobility Foresights)

[153] Mordor Intelligence 2023 *QUANTUM CRYPTOGRAPHY MARKET SIZE & SHARE ANALYSIS - GROWTH TRENDS & FORECASTS (2023 - 2028)* (Mordor Intelligence)

[154] Persistence Market Research 2023 *Quantum Cryptography Market* (Persistence Market Research)

[155] Precision Research 2022 *2022-2029 GLOBAL QUANTUM CRYPTOGRAPHY PROFESSIONAL MARKET RESEARCH REPORT, ANALYSIS FROM PERSPECTIVE OF SEGMENTATION (COMPETITOR LANDSCAPE, TYPE, APPLICATION, AND GEOGRAPHY)* (Precision Research)

[156] Prof Research 2023 *Quantum Key Distribution (QKD) Market Report 2023 -Global and Chinese Market Size, Share & Trends Analysis, by Manufacturers (ID Quantique, SeQureNet, Quintessence Labs), Products, Applications (Financial, Government, Military& Defense)* (Prof Research)

[157] Prudence Markets 2020 *Quantum Cryptography Market By Component (Hardware, Service), By Enterprise (Large Enterprises, Small Enterprises), By Application (Database Encryption, Network Layer Encryption, Application Security), Industry Trends, Estimation & Forecast, 2017-2025* (Prudence Markets)

[158] Reports & Markets 2021 *Global Quantum Key Distribution (QKD) Industry Market Research Report* (Reports & Markets)

[159] Research and Markets 2022 *Quantum Cryptography Market - Forecasts from 2021 to 2026* (Research and Markets)

[160] Research Napster 2023 *Quantum Cryptography Market Segmentation By Application (Application Security, Network Security & Database Encryption); By Component (Hardware and Services); By Organization Size (Small, Medium and Large Enterprises); By Industry Vertical (BFSI, IT and Telecommunications, Government and Defense, Healthcare and Life Sciences, Manufacturing and Retail) – Global Demand Analysis & Opportunity Outlook 2027* (Research Napster)

[161] Research Reportsworld 2022 *GLOBAL QUANTUM COMMUNICATION MARKET SIZE, STATUS AND FORECAST 2022-2028* (Research Reportsworld)

[162] Research Reportsworld 2022 *GLOBAL QUANTUM KEY DISTRIBUTION (QKD) MARKET GROWTH (STATUS AND OUTLOOK) 2022-2028* (Research Reportsworld)

[163] SDMR International 2022 *Global Quantum Key Distribution (QKD) Market 2021-2031 by Component (Hardware, Software, Services), Security Type (Application, Network), Industry Vertical, and Region: Trend Forecast and Growth Opportunity* (SDMR International)

[164] technavio 2021 *Quantum Cryptography Solutions Market by End-user and Geographic Landscape - Forecast and Analysis 2021-2025* (technavio)

[165] TechSci Research 2023 *Quantum Cryptography Market – Global Industry Size, Share, Trends, Competition, Forecast & Opportunity, 2018-2028 Segmented By Component (Hardware and Software), By Organization Size (SME and Large Organization), By Application (Database Encryption, Network Layer Encryption, Application Security, and Others), By End User (BFSI, IT & Telecom, Government & Military and Others), By Region* (TechSci Research)

[166] Tramsparency Market Research 2019 *Quantum Key Distribution Market* (Tramsparency Market Research)

[167] Verified Market Research 2022 *Global Quantum Cryptography Market Size By Service (Consulting and Advisory, Deployment and Integration), By Security Type (Network Security, and Application Security), By Vertical (Government and Defense, Banking, Financial Services), By Geographic Scope & Forecast* (Verified Market Research)

[168] Verified Market Research 2023 *Global Quantum Key Distribution (QKD) Market By Type (Rigid 1-2Sided, Standard Multilayer), By Application (Financial, Government), By Geographic Scope And Forecast* (Verified Market Research)

[169] Visiongain 2021 *Quantum Cryptography Market Report 2021-2031* (Visiongain)

[170] we market research 2022 *Global Quantum Secure Communication Market* (we market research)

[171] Bundesministerium für Bildung und Forschung 2024 *Research and Innovation - BMBF's Data Portal* https://www.datenportal.bmbf.de/portal/en/research.html (accessed 12 May 2024)

[172] Eurostat 2024 *Statistics Explained* https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Main_Page (accessed 12 May 2024)

[173] Quantum Flagship 2022 *Quantum Internet Alliance has started a seven-year program* https://qt.eu/news/2022/quantum-internet-alliance (accessed 12 May 2024)

[174] Heinrich-Hertz-Institut, Fraunhofer 2023 *Qu-Test and Qu-Pilot elevate quantum technologies to a new level* https://www.hhi.fraunhofer.de/en/news/nachrichten/2023/qu-test-and-qu-pilot-elevate-quantum-technologies-to-a-new-level.html (accessed 12 May 2024)

[175] Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF 2022 *Erstmals erfolgreich Quantenschlüssel zwischen Erfurt und Jena via Glasfaser ausgetauscht: Faserstrecke über 75 km ermöglicht neue QKD-Experimente* https://www.iof.fraunhofer.de/de/presse-medien/pressemitteilungen/2022/quantenschluessel-erfolgreich-ausgetauscht.html (accessed 12 May 2024)

[176] Bundesministerium für Bildung und Forschung *Handlungskonzept Quantentechnologien der Bundesregierung* (Bundesministerium für Bildung und Forschung)

[177] European Commission 2021 *Call for proposals: Digital Europe Programme (DIGITAL)* https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/wp-call/2021/call-fiche_digital-2021-qci-01_en.pdf (accessed 12 Jun 2024)

[178] European Commission 2022 *European Quantum Communication Infrastructure - The EuroQCI initiative - Works* https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2022-euroqci-works-cancelled (accessed 12 Jun 2024)

[179] Zhang Q, Xu F, Li L, Liu N-L and Pan J-W 2019 Quantum information research in China *Quantum Sci. Technol.* **4** 40503

[180] Kania E B and Costello J K 2018 *Quantum Hegemony?: China's ambitions and the challenge to US innovation leadership* https://www.cnas.org/publications/reports/quantum-hegemony (accessed 12 May 2024)

[181] Aerospace Technology 2016 *Micius Quantum Communication Satellite (QUESS)* https://www.aerospace-technology.com/projects/micius-quantum-communication-satellite (accessed 12 May 2024)

[182] The State Council, the People´s Republic of China 2024 *China to include quantum technology in its 14th Five-Year Plan* https://english.www.gov.cn/news/videos/202010/22/content_WS5f90e700c6d0f7257693e3fe.html (accessed 12 May 2024)

[183] Costello J 2017 *Chinese Efforts in Quantum Information Science- Drivers, Milestones, and Strategic Implications* https://www.uscc.gov/sites/default/files/John%20Costello_Written%20Testimony_Final2.pdf (accessed 12 May 2024)

[184] Allison, G., Klyman, K., Barbesino, K. and Yen H *The great tech rivalry: China vs. the US*

[185] House Committee on Science Space & Tech - Republicans 2023 *Full Committee Hearing - Advancing American Leadership in Quantum Technology* https://science.house.gov/hearings?ContentRecord_id=7684AFE7-D1EB-4079-B9A8-3941F0CCAF24 (accessed 15 May 2024)

[186] United States Government 2020 *A Strategic Vision for America's Quantum Network* (Product of the White House National Quantum Coordination Office)

[187] Awschalom D 2020 *From Long-distance Entanglement to Building a Nationwide Quantum Internet:: Report of the DOE Quantum Internet Blueprint Workshop, Upton, NY (United States)*

[188] Department for Science, Innovation & Technology 2023 *National Quantum Strategy* (Department for Science, Innovation & Technology)

[189] qst *SIP FY 2023 Funding Guideline* https://www.qst.go.jp/uploaded/attachment/33030.pdf (accessed 16 May 2024)

[190] Ministry of Science and ICT 2023 *In 2035, Korea Becoming the Global Hub for Quantum Economy!* https://www.korea.net/Government/Briefing-Room/Press-Releases/view?articleId=6930&insttCode=A110439&type=O (accessed 15 May 2024)

[191] ID Quantique 2022 *IDQ & SK Broadband complete phase one of Korean QKD Network* https://www.idquantique.com/idq-and-sk-broadband-complete-phase-one-of-nation-wide-korean-qkd-network/ (accessed 15 May 2024)

[192] Korea IT News 2020 *SK Broadband to Become the First Telecommunications Company to Apply Quantum Cryptography Technology to Public Network* https://english.etnews.com/20201022200001 (accessed 15 May 2024)

[193] Government of Canada 2024 *Canada's National Quantum Strategy* https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy (accessed 15 May 2024)

[194] Government of Canada and Canadian Space Agency 2019 *Cybersecurity from space: the Government of Canada invests in quantum technology* https://www.canada.ca/en/space-agency/news/2019/06/cybersecurity-from-space-the-government-of-canada-invests-in-quantum-technology.html (accessed 15 May 2024)

[195] H. Podmore, I. D'Souza, J. Cain, T. Jennewein, B. L. Higgins, Y. S. Lee, A. Koujelev, D. Hudson and A. McColgan 2020 QKD terminal for Canada's Quantum Encryption and Science Satellite (QEYSSat) *International Conference on Space Optics-ICSO. SPIE* 203–12

[196] Cabinet of India 2023 *Cabinet approves National Quantum Mission to scale-up scientific & industrial R&D for quantum technologies* https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1917888 (accessed 15 May 2024)

[197] Schirmprojekt Quantenkommunikation Deutschland 2024 *Testbed-Karte zur Quantenkommunikation in Deutschland* https://www.squad-germany.de/testbeds/ (accessed 12 Jun 2024)

[198] Bundesministerium für Bildung und Forschung 2020 *Technologische Souveränität* https://www.bmbf.de/bmbf/de/europa-und-die-welt/innovationsstandort-deutschland/technologische-souveraenitaet/technologische-souveraenitaet_node.html (accessed 15 May 2024)

[199] Edler J, Blind K, Kroll H and Schubert T 2023 Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means *Research Policy* **52** 104765

[200] Bundesministerium für Bildung und Forschung *Technologisch souverän die -Zukunft gestalten: BMBF-Impulspapier zur technologischen Souveränität* (Bundesministerium für Bildung und Forschung)

[201] QBN - Quantum Business Network 2023 *QBN's official statement on Germany's Action Plan on Quantum Technologies ▸ QBN - Quantum Business Network* https://qbn.world/qbn-official-statement-on-germanys-action-plan-on-quantum-technologies/ (accessed 15 May 2024)

[202] Bundesamt für Sicherheit in der Informationstechnik *Kryptografie quantensicher gestalten: Grundlagen, Entwicklungen, Empfehlungen* (Bundesamt für Sicherheit in der Informationstechnik)

[203] Bundesamt für Sicherheit in der Informationstechnik 2022 *Allgemeine Informationen zu KRITIS* https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html (accessed 15 May 2024)

[204] CEN-CENELEC Focus Group on Quantum Technologies 2023 *Standardization Roadmap on Quantum Technologies: Release 1*