QUANTEN-KOMMUNIKATION

für sichere digitale Infrastrukturen

Ein gemeinsames Papier der BMBF-geförderten Verbünde QR.X, QuNET und SQuaD zum Forum für die Quantenkommunikation in Deutschland

QR.X

QuNET

SQuaD
Schirmprojekt Quantenkommunikation Deutschland

EXECUTIVE SUMMARY

Sichere und leistungsfähige digitale Infrastrukturen sind die Grundpfeiler einer souveränen und selbstbestimmten Informationsgesellschaft. Die Quantenkommunikation bietet grundlegend neue Ansätze und Konzepte für eine gesicherte digitale Infrastruktur in Deutschland und Europa.

Die Verfügbarkeit immer leistungsfähigerer Informationstechnologien mit disruptivem Potential fordert eine noch umfangreichere Absicherung der IT-Infrastruktur in Deutschland mit zukunftweisenden Schlüsseltechnologien. Eine rigorose Netzwerksicherheit kann mit grundlegenden Prinzipien der Quantenphysik in neuen Kommunikationsprotokollen untermauert werden. Leistungsstarke Innovationsökosysteme der Forschung und Industrie sind zum Aufbau erster Netzwerkstrukturen für die Quantenkryptographie in Deutschland etabliert worden. Im Zusammenspiel mit klassischen IT-Sicherheitstechnologien werden neue Ansätze für die Sicherung kritischer Elemente der IT-Infrastruktur entwickelt, zum Schutz der Wirtschaft und Gesellschaft im digitalen Raum. Hierbei entstehen die ersten Bausteine für die langfristigen Ziele der Quantenkommunikation zur Realisierung skalierbarer Quantennetzwerke. Im Zeitraum der nächsten Dekade eröffnen diese Entwicklungen die Perspektive auf eine neue Qualität an Leistungsfähigkeit und Resilienz vernetzter Ressourcen des Quantencomputings und der Quantensensorik durch die Übertragung von verschränkten Zuständen – in voller Tragweite der Quanteninformation.

Aktuelle und zukünftige Herausforderungen im Bereich der Quantenkommunikation werden in der nachfolgenden Darstellung aus der Perspektive eines neuen Ökosystems an Forschungsinstitutionen und Industrieunternehmen in Deutschland skizziert. Diese Community verfolgt das gemeinsame Ziel einer zeitnahen Einführung und breiten Proliferation dieser neuen Schlüsseltechnologie.

Ausgehend von der erfolgreichen Strategie der Bundesregierung zur gezielten und breiten Förderung der Quantenkommunikation in Deutschland werden Empfehlungen für zukünftige Entwicklungen dargestellt. Es besteht die Chance, die vorteilhafte Ausgangslage der bisherigen Förderpolitik zu nutzen und die Quantenkommunikation zum Markenzeichen der Innovation am Wissenschafts- und Wirtschaftsstandort Deutschland zu etablieren. Mit vereinten Ressourcen der Forschung und Industrie können die weitläufigen Entwicklungen zur quantengesicherten IT-Infrastruktur in Deutschland langfristig bewältigen werden. Hieraus kann sich ein kompetitiver Industriezweig entwickeln, der sich zur Wertschöpfung in den globalen Märkten erfolgreich positionieren kann. Eine profilierte Industrie in diesem Sektor ermöglicht die aktive Mitgestaltung europäischer und globaler Netzwerke der nächsten Generation und leistet somit einen wichtigen Beitrag zur Sicherung der technologischen Souveränität Deutschlands und Europas.

Die Integration quantenbasierter Kommunikations- und Informationstechnologien in bestehende Netzwerkstrukturen ist ein kontinuierlicher und vielschichtiger Prozess. Der erhebliche Forschungsbedarf erfordert die Bereitschaft zu langfristigen, anspruchsvollen technologischen Entwicklungen der Forschung und Industrie für systematischem Fortschritt in drei Schwerpunkten:

• Initialer Aufbau quantengesicherter Konnektivität

Die Weiterentwicklung gegenwärtiger Protokolle und Ressourcen zu integrierten Technologien im höchsten Technologiereifegrad bietet die Bausteine für den Infrastrukturaufbau zur Quantenschlüsselverteilung im Zusammenspiel von terrestrischen und satellitenbasierten Netzwerken. Qualifizierung, Standardisierung und Zertifizierung im Zusammenhang mit rigorosen Sicherheitsbeweisen sind entscheidende Prozesse für die Industrie in der Realisierung erster Lieferketten zur Ausstattung und Sicherung prioritärer Kommunikationswege.

• Ausbau von heterogenen Netzwerkarchitekturen

Mit neuen Kommunikationsprotokollen, Ressourcen zur Verschränkungsverteilung und Entwicklungen zur multidimensionalen Kodierung von Quanteninformation wird eine neue Qualität an Konnektivität, Kapazität, Reichweite und Sicherheit ermöglicht. Das Etablieren zunehmend heterogener Netzwerke mit diesen neuen Fähigkeiten eröffnet signifikanten Mehrwert in der Realisierung hybrider Technologien in vielschichtigen Sicherheitsstrategien mit leistungsfähigen klassischen Netzwerkressourcen. Es bietet zudem neue Mechanismen der Vernetzung von Quantensensoren und Quantenspeichern zur rudimentären Quanteninformationsverarbeitung in exemplarischen Anwendungen lokaler Verschränkungsverteilung.

• Realisierung von Quantennetzwerken

Ausgereifte Protokolle zur Verschränkungsverteilung und Quantenspeicher bieten die Grundlage für leistungsfähige Quantenrepeater als Schlüsseltechnologie zum Aufbau skalierbarer Quantennetzwerke. Mit einer ununterbrochenen Sicherheit in der Verteilung von Quantenschlüsseln über regionale Distanzen hinweg und einer delokalisierten Verarbeitung von Information in verzweigten *multi-node* Konfigurationen wird der Zugang zur vollen Leistungsfähigkeit der Quanteninformation eröffnet. Erheblicher Mehrwert kann durch die Einbindung ausgereifter Technologien aus den Bereichen des Quantencomputings und der Quantensensorik in neuen Konstellationen von Quantennetzwerken erzielt werden.

Gegenwärtige Maßnahmen zur Erneuerung klassischer IT-Infrastruktur mit dem Ausbau von neuen digitalen Ressourcen stehen in hoher Synergie mit Infrastrukturanforderungen zur Einführung und Proliferation quantenbasierter Kommunikations- und Informationstechnologien.

Das gezielte Zusammenwirken klassischer und quantenbasierter Ressourcen kann eine nachhaltige Modernisierung gegenwärtiger Netzwerke bewirken. Hierdurch können die höchsten technischen Leistungsparameter in der Ausstattung klassischer digitaler Infrastrukturen als Wegbereiter für die besonderen Leistungsmerkmale der Quantenkommunikation dienen. Die breite Integration quantengeschützter Kommunikationslösungen in die digitale und physische Infrastruktur wird zu einem entscheidenden Faktor für die Zukunftsfähigkeit und Sicherheit unserer Gesellschaft.

I. HANDLUNGSBEDARF IN DER FORSCHUNG & ENTWICKLUNG

A. Initialer Aufbau quantengesicherter Konnektivität

Der aktuelle Antrieb für den Aufbau quantenbefähigter Infrastrukturen ist die Einführung von unterschiedlichen Protokollen zur Quantenschlüsselverteilung (QKD) in der gezielten Sicherung von prioritären Kommunikationswegen und kritischen Infrastrukturen.

Zentrale Herausforderungen dieser Entwicklung sind die Skalierbarkeit der Netzwerke und die Überwindung der begrenzten Reichweite verfügbarer Protokolle in ununterbrochenen Punkt-zu-Punkt Übertragungen. Der Nachweis der praktischen Sicherheit in realistischen Szenarien und die Sicherstellung der Authentifizierung der Kommunikationspartner sind hierbei von grundlegender Bedeutung. Verschiedene Lösungsmöglichkeiten zur begrenzten Reichweite umfassen den Ausbau terrestrischer und satellitenbasierter Infrastrukturen, sowie die Perspektive auf neue Protokolle und Quantenressourcen mit erweiterten Leistungsparametern. Die offene Frage nach der optimalen Netzwerkkonfiguration und Konnektivität in Deutschland und Europa wird von grundsätzlichen Leistungsmerkmalen unterschiedlicher Lösungen geleitet. Übertragungsraten und Kapazitäten sowie Zuverlässigkeit und Ökonomie im Rahmen unterschiedlicher Sicherheitsaspekte der Anwendungen sind wesentliche Kriterien zum initialen Aufbau erster Netzwerkstrukturen.

Die zeitnahe Einführung quantengesicherter Kommunikation über interregionale Distanzen basiert derzeit auf *trusted-node* Architekturen. Dieser Ansatz ermöglicht die sichere Kommunikation über größere Entfernungen, indem Quanteninformationen an Knotenpunkten klassisch verarbeitet und weitergeleitet werden. Verwaltungssysteme basierend auf klassischen Informationstechnologien sind kritische Elemente in der Gewährleistung einer sicheren Handhabung und Nutzung von Quantenschlüsseln im Betrieb von *trusted-node* Zwischenstufen und an Endpunkten der Nutzer. Gegenwärtige Teststrecken auf kurzen und mittleren Reichweiten mit ununterbrochener Übertragung von Quantenschlüsseln bieten den Nukleus zum Ausbau von Metropolnetzwerken mit einer Vielfalt an öffentlichen und privatwirtschaftlichen Anwendungsszenarien. Diese Ansätze sind der Ausgangspunkt für zukünftige Entwicklungen in zwei Richtungen: Einerseits motivieren Metropolnetzwerke die Forschung und Konzeption zu verzweigten *multi-user* Architekturen. Neben *trusted-node* Lösungen können verschränkungsbasierte Methoden oder *prepare-and-measure* Protokolle ergänzt durch Routing mit optischen Schaltern ununterbrochene Übertragungen von Quantenschlüsseln in verzweigten Metropolnetzwerken ermöglichen. Anderseits eröffnen Satellitennetzwerke die Perspektive auf erste intrakontinentale Reichweite, als vorteilhafter Weg zu Überbrückung lokaler Netzwerke. Sie bieten zudem eine grundlegende Konnektivität geographischer Endpunkte mit strategischer Bedeutung. Gegenwärtige Satellitenmissionen erfordern umfangreiche Entwicklungen in Herausforderungen zu Schlüsselraten, Verfügbarkeit und Stabilität optischer Übertragungen zu Bodenstationen sowie effiziente und sichere Konfigurationen für die Anbindung an terrestrische Netzwerke.

Entwicklungen im Zeitraum der nächsten Jahre und der nächsten Dekade zur Leistungsfähigkeit und Interoperabilität zukünftig heterogener Netzwerke sind für die grundlegende Verfügbarkeit dieser neuen IT-Sicherheitstechnologie entscheidend.

Der Aufbau von ersten Netzwerken zur Quantenschlüsselverteilung ist mit einer Vielzahl an Herausforderungen für die Industrie verbunden. Der Ausbau gegenwärtiger Netzwerke erfordert eine holistische Integrationsstrategie und die Konzertierung vielfältiger Ressourcen zur Quantenschlüsselverteilung in terrestrischen und satellitenbasierten Netzwerken sowie HAP *(High Altitude Platforms)*. Ein breites Spektrum an Entwicklungen zu hochintegrierbaren, miniaturisierten, kosteneffizienten Hardwarekomponenten und Softwareelemente zur Steuerung höherer Netzwerkebenen sind hierfür erforderlich. Im Vordergrund steht die sichere Verwaltung von Quantenschlüssel in *trusted-node* basierten Netzwerkarchitekturen. Diese Funktionen können durch KI-Ressourcen maßgeblich befördert werden. Als Voraussetzung für die Anwendung, muss die sichere Operation im Zusammenwirken aller Netzwerkelemente in Leuchtanwendungen demonstriert und verifiziert werden.

B. Ausbau von heterogenen Netzwerkarchitekturen

Die Entwicklung hybrider Ansätze fördert den Einsatz der Quantenschlüsselverteilung in zugangsbeschränkten Netzwerken, die rigorosen Sicherheitsregularien unterliegen. Hybride Ansätze ermöglichen die Einbettung von neuen Sicherheitsmechanismen quantenbasierter Methoden in etablierten, klassischen Sicherheitsprotokollen.

Hierdurch entsteht ein vorteilhafter Weg, die Integration von Protokollen zur Quantenschlüsselverteilung in Anwendungen mit Sicherheitsanforderungen erhöhter Geheimhaltungsstufen zu ermöglichen und zu beschleunigen. Techniken der Quantenkommunikation können mit etablierten Methoden der klassischen Kryptographie vorteilhaft in neuen Ansätzen vereint werden: Dazu gehören die Postquanten-Kryptographie und KI-Ressourcen in neuen Kombinationen mit Protokollen der Quantenkryptographie mit Quantenzufallsgeneratoren und Verschränkungsverteilung. Im Aufbau von zunehmend heterogenen Netzwerkarchitekturen können Mehrwerte hybrider Ansätze erprobt und evaluiert werden. Diese Strategie kann eine kontinuierliche Migration quantenbasierter Technologien in klassische digitale Infrastrukturen befördern. Vielschichtige Sicherheitsstrategien eröffnen die Aussicht auf eine neue Qualität an Resilienz gegenüber unterschiedlichsten Sicherheitsrisken.

Die Weiterentwicklung der Quantenkommunikation über die Quantenschlüsselverteilung hinaus basiert auf der effizienten und robusten Verteilung von verschränkten Quantenzuständen an die Kommunikationspartner. Hierdurch wird ein deutlich breiteres Feld von Anwendungen der Quanteninformation zugänglich.

Verschränkungsverteilung ist ein zentrales Element in der Realisierung verzweigter Netzwerkarchitekturen mit ununterbrochener Übertragung von Quantenzuständen in *multi-user* Szenarien, abseits der Notwendigkeit zu *trusted-node* Lösungen oder optisches Schalten von Punkt-zu-Punkt Übertragungen. Diese Funktionalität ist von hoher Bedeutung für die Industrie im Aufbau von Netzwerkstrukturen, die ein breites Spektrum an potentiellen

Anwendungsszenarien adressiert. In einem ersten Schritt zu Quanteninformationsnetzwerken kann die Realisierung einer verschränkungsbasierten Konnektivität im Format von Campus-Netzwerken richtungsweisende Mehrwerte gekoppelter Quantensensorik und elementare Funktionen delokalisierter Quanteninformationsverarbeitung aufzeigen. Hierdurch werden zukünftig verteilte Quantenrechnerarchitekturen vorbereitet. Gegenwärtige Protokolle zur Verschränkungsverteilung nutzen zumeist wenige, ausgewählte Freiheitsgrade des Lichts. Im Zusammenspiel der Nanophotonik und Quantenoptik eröffnen sich neue Möglichkeiten für die Entwicklung von Hardwareelementen und Systemen zur präzisen Manipulation einer Vielfalt an Quantenzuständen zur multidimensionalen Kodierung von Quanteninformation. Erhöhte Datenraten und Informationsdichte sowie Stabilität und Resilienz der quantenassistierten und quantenbasierten Kommunikation werden hierdurch ermöglicht. Diese Entwicklungen bieten eine neue Qualität an Konnektivität in Leistungsparametern für anspruchsvolle Anwendungen in terrestrischen und satellitenbasierten Netzwerken.

Von zentraler Bedeutung für den weiteren, konsequenten Aufbau heterogener Netzwerkarchitekturen sind Quantenressourcen, die eine ununterbrochene Sicherheit auf interregionalen Distanzen und in transnationalen Szenarien in Deutschland und Europa ermöglichen.

Forschungsbedarf besteht insbesondere bei der Entwicklung neuer Protokolle mit deutlich erhöhter Reichweite. Hier können Quantenspeicher mit erweiterten Kohärenzzeiten im Zusammenspiel mit kompakten Quantenlichtquellen verschränkungsbasierte Protokolle befähigen und sind zugleich ein wichtiger Schritt in der langfristigen Entwicklung hin zu Quantennetzwerken.

C. Realisierung von Quantennetzwerken

Die Verteilung von Verschränkung als Ressource, ihre Speicherung in langlebigen Quantenspeichern und die Manipulation der gespeicherten Quanteninformation durch Gatteroperationen ermöglichen den Aufbau von Quantennetzwerken, in denen Quantenzustände zwischen beliebigen Knoten übertragen werden können.

Verteilung und Verfügbarmachung von Verschränkung und der Aufbau von skalierbaren Quantennetzwerken basiert auf der Technologie der Quantenrepeater. In einer solchen Konstellation ersetzen Quantennetzwerke perspektivisch *trusted-node* Architekturen und erlauben ununterbrochene Quantenschlüsselverteilung über große Distanzen in ausgedehnten Infrastrukturen. Die Demonstration von Quantenrepeatern mit deutlichem Mehrwert in Reichweite ist eine kritische Entwicklung für die Industrie. Hierdurch wird eine abdeckende Konnektivität in skalierbaren Netzwerken für vielfältige öffentliche und privatwirtschaftliche Anwenderkreise zur Quantenschlüsselverteilung ermöglicht. In langfristigen Entwicklungen sind Quantenrepeater der Schlüssel zur sicheren Vernetzung von ausgereiften Quantencomputern und Quantensensoren. Hierdurch werden neue Möglichkeiten zur Skalierung von Ressourcen zum Quantencomputing geschaffen. Es bedarf jedoch einer Vielzahl technisch und konzeptionell anspruchsvoller Entwicklungen, um dieses weitreichende Ziel durch dezidierte Forschung in die allgemeine Praxis zu überführen.

Um eine kontinuierliche Weiterentwicklung dieser anspruchsvollen Methoden und Technologien langfristig voranzutreiben, ist die gezielte Verwertung von Zwischenstufen und leistungsfähigen Bausteinen von hoher Bedeutung.

Mittelfristige Perspektiven zu neuen Funktionalitäten aus der Verschränkungsverteilung und Quantenspeichern mit erweiterten Kohärenzzeiten können zuerst als Treiber in der Befähigung heterogener Netzwerke dienen. Langlebige Quantenspeicher erfordern eine Vielzahl an Hardwareelementen mit Leistungsparametern an den äußersten Grenzen gegenwärtiger Technologien und sind somit ein zentraler Forschungsbedarf. Diese Entwicklungen sind die Grundlage für eine kontinuierliche Skalierung von Netzwerken zur Verschränkungsverteilung in *multi-node* Architekturen über die Dimensionen von experimentellen Campus-Netzwerken hinaus, hin zu ersten anspruchsvollen Anwendungen von gekoppelten Quanteninformationssystemen. Mit systematischem Fortschritt entlang der oben skizzierten Meilensteine werden Grundlagen für die langfristen Ziele der Quantenkommunikation geschaffen. Kontinuierliche Weiterentwicklung von Quantenspeichern, Verschränkungsverteilung und Gatteroperationen zur Quantenfehlerkorrektur sind der Weg zu Quantenrepeater, als Schlüsseltechnologie der nächsten Dekade zur umfassenden Quantensicherheit in skalierbaren Netzwerken.

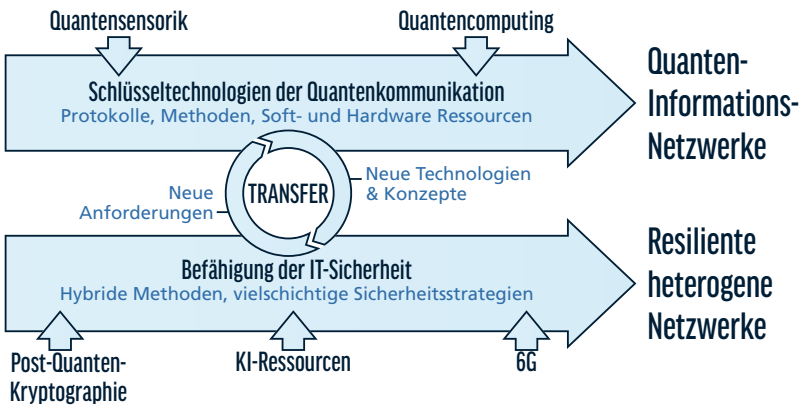
II. NEUE STRUKTUREN FÜR ZUKÜNFTIGE ENTWICKLUNGEN DES INNOVATIONSÖKOSYSTEMS

A. Forschungsschwerpunkte

Neue Netzstrukturen der Quantenkommunikation sind der Ausgangspunkt für signifikante Mehrwertbildung in hybriden Innovationen und in der Vernetzung von Entwicklungen aus verschieden Bereichen der Quantentechnologien.

Mit der Zusammenführung von Ressourcen klassischer und quantenbasierter Informationstechnologien werden die Weichen für Schwerpunkte und Strukturen in zentralen Forschungsthemen der Quantenkommunikation gestellt. Hierbei stehen drei wesentliche Bereiche im Vordergrund: (1) Fortschritt zu leistungsfähigen quantenbasierten Schüsseltechnologien für unterschiedliche Aufgabenbereiche, (2) die Beförderung innovativer Anwendungen in der IT-Sicherheit mit neuen Quantenressourcen und (3) ein dezidierter Transferbereich zur gegenseitigen Befähigung dieser Zielsetzungen.

Schema:
Die Optimierung der IT-Sicherheit durch hybride Ansätze und die Entwicklung von Quanteninformations-netzwerken mit erweiterter Funktionalität werden in zwei parallelen Entwicklungssträngen verfolgt, die sich gegenseitig befördern.



B. Transferstrukturen & Ausbildung

Um ein effektives Zusammenwirken der Forschung und Industrie zu erzielen und Fortschritt im Mehrwert der Community zu fördern, bedarf es einer systematischen Koordination der Aktivitäten in Deutschland.

Leistungsstarke Innnovationsökosysteme sind bereits in Deutschland erfolgreich etabliert worden. Ein konsequenter Ausbau dieser Aktivitäten ist von zentraler Bedeutung für eine kompetitive Weiterentwicklung der Quantenkommunikation. Wirksame Plattformen der Zusammenarbeit sind entscheidend, um Forschungsstrukturen und Zielstellungen der Quantenkommunikation durch effektive Transfermechanismen in dezidierten Innovationsräumen zu befördern. Hierbei können Reallabore und Netzwerkinfrastrukturen zur fokussierten Interaktion von Forschung und Industrie eine neue Form der Kooperation innerhalb der Community ermöglichen.

Ein breites Spektrum an Maßnahmen kann dazu beitragen, die Interessen und Perspektiven aus Forschung, Startups, KMU und Großindustrie zu vereinen. Geeignete Instrumente hierzu sind z.B. der gezielte Ausbau bestehender Verbundaktivitäten, ein rotierender Ausschuss von zentralen Akteuren aus prägenden Aktivitäten der Community, gemeinsame Gremien oder neue Kooperationsplattformen zwischen Verbünden sowie gänzlich neue Strukturen in Gesellschaften oder unterschiedliche Formen von *public-private* Unternehmen.

Der hohe Forschungsbedarf und zugleich erhebliche Infrastrukturausbau für die breite Einführung der Quantenkommunikation können durch ein gezieltes Zusammenwirken öffentlicher und privater Ressourcen langfristig bewältigt werden. Von besonderer Bedeutung sind flexible Fördermechanismen für kurz- bis mittelfristige Entwicklungen und zugleich langfristige Finanzierungsformate in einer ausgewogenen Verteilung öffentlicher und privater Investitionen. Wirksame Mechanismen zur Vernetzung und initialen Planung von Lieferketten spielen eine zentrale Rolle für einen systematischen Weg zur Wertschöpfung der Industrie. Diese Prozesse müssen an den Bedarf des Infrastrukturausbaus kontinuierlich angepasst werden. Hierbei kann die Innovationskraft von Startups und KMU gezielt in Ressourcen und Aktivitäten der gesamten Community eingebunden werden. Mit diesen Entwicklungen kann eine Interessensvertretung der Community in strategischen Entwicklungen und regulatorischen Aspekten etabliert werden. Eine Kompetenzbündelung der zentralen Akteure und Institutionen im öffentlichen und privaten Bereich kann das kohärente Vorgehen in strategisch bedeutenden Prozessen der Qualifizierung, Standardisierung sowie der konsequenten Ausarbeitung von Sicherheitsnachweisen und Zertifizierungskriterien befördern.

Bildung auf allen Qualifikationsstufen ist der Schlüssel zur international führenden Forschung und einer kompetitiven Industrie in den globalen Märkten der Quantenkommunikation. Die Einführung von neuen Hochtechnologien kann nur durch die Innovationskraft von qualifizierten Fachkräften und der breiten Akzeptanz einer informierten Gesellschaft erreicht werden.

Deutschlandweit sind erste Studiengänge an der Schnittstelle von Quantenphysik, Quantentechnologien und Ingenieurwissenschaften entstanden, z.B. in *Quantum Engineering* Studiengängen. Die Gründung neuer Lehrstühle und die Förderung von

Graduiertenschulen in den Quantentechnologien untermauern den konsequenten Weg zu hochqualifizierten Fachkräften. Neben einer gezielten Investition in etablierten Bildungswegen, kann die Gründung einer »Akademie der Quantentechnologien« den aktuell dringenden Bedarf an Arbeitskräften in Forschung und Industrie unmittelbar adressieren. Ausbildungsziele können in einer Akademie für spezifische Forschungsbereiche und Anwendungsgebiete der Industrie mit entsprechenden Inhalten konzipiert werden. Hierdurch können hochwertig akkreditierte Abschlüsse die Berufswege junger Fachkräfte fördern. Gegenwärtige Aktivitäten des Europäischen Flagships ergänzen die Initiativen zu höheren Bildungswegen mit der Ausarbeitung von Weiterbildungsprogrammen für spezifische Berufsklassen und Unterrichtsmaterial zur frühzeitigen Einführung der Quantenphysik in Schulen. Eine gesonderte Akademie in Deutschland bietet einen geeigneten Rahmen zur Vertiefung dieser Aktivitäten, um alle Bildungsstufen effektiv zu fördern.

C. Internationalisierung & Gesellschaftliche Missionen

Eine gezielte Koordination der Aktivitäten in Deutschland mit einer bundesweiten Bündelung von Ressourcen und Kompetenzen in wirksamen Kooperationsplattformen ist der Ausgangspunkt für die Beteiligung und maßgebliche Mitwirkung Deutschlands in den internationalen Entwicklungen zur Quantenkommunikation.

Die Basis hierfür ist eine abgestimmte Förderlandschaft im Bund und den Ländern. Eine nationale Koordinationsstelle basierend auf gegenwärtigen Verbundaktivitäten, ergänzt und verstärkt mit weiteren Strukturen des Zusammenwirkens in Deutschland, ist die Grundlage für ein kohärentes und vereintes Vorgehen in europäischen und globalen Aktivitäten. Von besonderer Bedeutung ist die konsequente Mitwirkung an europäischen Gremien zur verstärkten Vernetzung und maßgeblichen Erweiterung der digitalen Infrastruktur in Europa. Diese Entwicklungen beinhalten den Ausbau einer neuen Generation an resilienten Satellitennetzwerken und vernetzten Hochleistungsrechenzentren sowie gemeinsame europäische Initiativen zur Befähigung der Verteidigung mit Ressourcen der Quantenkommunikation. Aussichtsreiche Wege zur Wertschöpfung werden hierbei eröffnet, um eine kompetitive europäische Industrie in diesem Sektor zu stärken und weiter zu etablierten. Diese Entwicklungen sind entscheidend für die Gewährleistung der technologischen Souveränität Deutschlands und Europas. Die deutsche Forschung und Industrie ist bereits weitgehend am Aufbau europäischer Forschungsinfrastrukturen sowie an Netzwerken der Community zu regulatorischen Prozessen und Industrieverbänden zu den Quantentechnologien beteiligt. Eine konsequente Weiterführung und Ausbau dieser Aktivitäten sind der Schlüssel zur Prägung internationaler Standards und der Weg zur aktiven Mitgestaltung quantengesicherter Konnektivität internationaler Netzwerke. Die bisherige Förderstrategie der Bundesregierung zu internationalen Kooperationen in Themen der Quantenkommunikation in bi- und multilateralen Formaten hat eine vorteilhafte Ausgangslage in den internationalen Aktivitäten ermöglicht. Eine weitere Stärkung dieser und anderer Förderformate zur internationalen Zusammenarbeit ist ein wesentlicher Faktor für eine kontinuierliche Mitwirkung der Forschung und Industrie im entscheidenden Zeitpunkt zur internationalen Gestaltung der nächsten Generation digitaler Infrastrukturen. In diesem Kontext spielt die Quantenkommunikation eine wichtige Rolle in internationalen Abkommen zur wissenschaftlichen und wirtschaftlichen Zusammenarbeit mit strategischen Partnerländern.

Mit Plattformen zur verstärkten Zusammenarbeit in Deutschland und einer gezielten Beteiligung an europäischen Entwicklungen kann die Quantenkommunikation zu gesellschaftlichen Missionen und Herausforderungen der Digitalisierung konsequent in die Praxis überführt werden.

Die Untermauerung der IT-Sicherheit durch neue Möglichkeiten der Quantenkommunikation adressiert alle Aspekte der Gesellschaft; vom Schutz der Rechte und Identität der Bürger im digitalen Raum bis hin zur Bereitstellung vorteilhafter Standortfaktoren für eine leistungsfähige Industrie. Eine quantenbasierte Sicherung grundlegender Infrastrukturen in ihrer digitalen Anbindung eröffnet eine neue Resilienz für Energie-, Verkehrs- und Versorgungsnetzwerke sowie Internetknoten und Rechenzentren. Die Souveränität hoheitlicher Aufgaben der Ministerien, Behörden und internationalen Organisationen sind in diesem Kontext von höchster Priorität. Die Förderung von Leuchtturmanwendungen mit ersten prominenten Leitkunden und eine Vorreiterposition dezidierter Unternehmen in der Rolle von Dienstleistern sind wichtige Treiber, um die Quantenkommunikation zeitnah in Anwendungen zum gesellschaftlichen Vorteil zu überführen.

Aussichtsreiche Anwendungen für gesicherte Kommunikation durch Quantenschüsselverteilung sind mit dem grundlegenden Schutz von Daten und Übertragungen im Medizin- und Finanzsektor verbunden. Gleichwertig ist die Sicherung strategisch bedeutender Forschungsergebnisse und technologischer Entwicklungen der Wissenschaft und Wirtschaft. Der hohe Stellenwert von Datensicherheit in diesen Bereichen ist bereits durch die entsprechenden Datenschutzgesetze und Richtlinien der Bundesregierung verkörpert. Hierbei kann die Quantenkommunikation eine wesentliche Rolle in der zukünftigen technologischen Untermauerung dieser und weiterer Herausforderungen zur digitalen Sicherheit spielen. Langfristige Perspektiven der Quantenkommunikation werden durch die Realisierung ausgereifter Ressourcen verteilter Quantensensorik und Quantencomputer eröffnet. Im Zusammenspiel mit Protokollen zur Quantenteleportation entstehen die Bausteine für ausgeprägte Forschungsnetzwerke, die den Zugang zu grundlegenden und weitragenden Vorteilen der Quanteninformation eröffnen. Diese Entwicklung steht in hoher Synergie mit der Förderstrategie zur Ausstattung von Hochleistungsrechenzentren mit Quantenprozessoren und Quantensimulatoren durch europäische Unternehmen. Die Quantenkommunikation ist eine Schlüsseltechnologie für die gezielte Vernetzung von klassischen und quantenbeförderten Rechenkapazitäten in Deutschland und Europa.

Sichere Netzwerke bedeuten digitale Freiheit – in der Verfügbarkeit und zugleich in der sicheren Einbindung leistungsfähiger klassischer und quantenbasierter Ressourcen für die Wissenschaften und der Wirtschaft in Deutschland und Europa.

Gezeichnet am 17. Oktober 2024 in Berlin,
Fraunhofer Institut für Nachrichtentechnik,
Heinrich Hertz Institut HHI zum
Forum für die Quantenkommunikation in Deutschland,

von den Vertretenden der BMBF-geförderten Verbünde
QR.X, QuNET und SQuaD:

Prof. Dr. Christoph Becher
Universität des Saarlandes

Prof. Dr. Martin Schell
Fraunhofer-Institut für Nachrichtentechnik,
Heinrich-Hertz-Institut, HHI

Dr. Nicolas Spethmann
Physikalisch-Technische Bundesanstalt

Prof. Dr. Andreas Tünnermann
Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF

vom Vertretenden des Deutschen Industrieverbunds
für Quantensicherheit, DIVQSec:

Imran Khan
Geschäftsführer und Mitgründer, KEEQuant GmbH