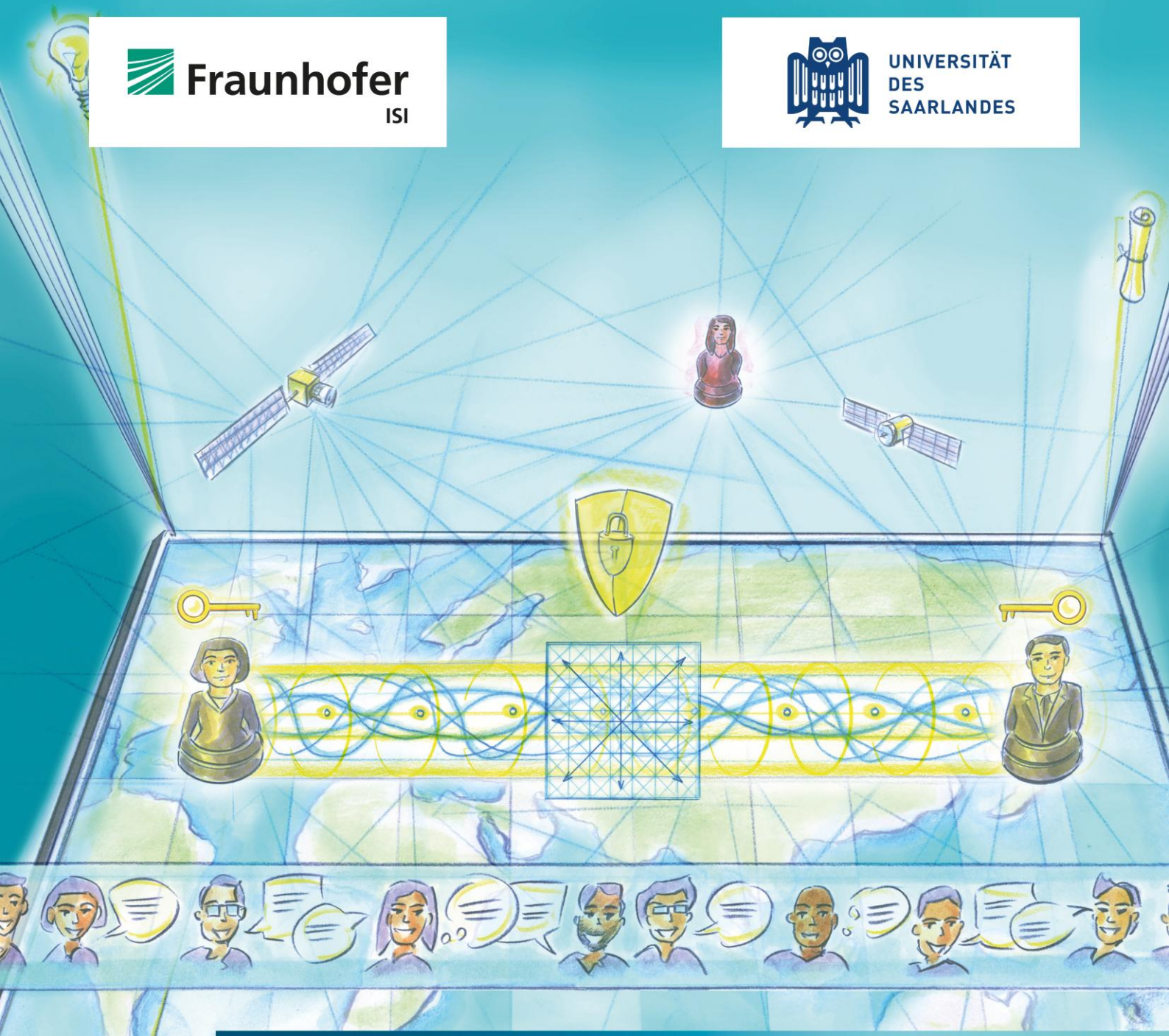
Fraunhofer ISI

UNIVERSITÄT DES SAARLANDES



July 2026

Monitoring Report 2 Quantum Communication

Publishing notes

Monitoring Report 2 – Quantum Communication

Report coordination

Fraunhofer Institute for Systems and Innovation Research ISI

Breslauer Straße 48, 76139 Karlsruhe, Germany
Dr. Lukas Weymann, Fraunhofer ISI, lukas.weymann@isi.fraunhofer.de
Dr. Thomas Schmaltz, Fraunhofer ISI, thomas.schmaltz@isi.fraunhofer.de

Saarland University

Department of Physics, Campus E2 6, 66123 Saarbrücken
Prof. Christoph Becher, christoph.becher@physik.uni-saarland.de

Responsible for content

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

Compiled in the context of

Umbrella Project for Quantum Communication in Germany
(Schirmprojekt Quantenkommunikation Deutschland – SQuaD),
funded by the Federal Ministry of Research, Technology and Space
(Bundesministerium für Forschung, Technologie und Raumfahrt – BMFTR)

With funding from the:

Federal Ministry of Research, Technology and Space

Picture credits

Cover page: Heyko Stöber, Hohenstein

Published

July 2026

DOI

10.24406/publica-8079

License

Notes

Table of Contents

Zusammenfassung und Kernergebnisse (German)

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 (Quantum Key Distribution, 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. Es werden die Entwicklungen in Forschung, Industrialisierung, Testinfrastruktur und Marktentstehung sowie die Bedeutung von Technologiesouveränität im Bereich der Quantenkommunikation analysiert. Die vorliegende Version stellt ein Update des Monitoring-Berichts 1 – Quantenkommunikation (veröffentlicht 2024) dar und basiert auf aktueller Fachliteratur über technologische Fortschritte, neuen quantitativen Daten zu Publikationen und Patenten, Marktstudien, Projekten, Förderungen und Testinfrastrukturen. Darüber hinaus beinhaltet der Bericht eine vertiefte Analyse von Technologietrends anhand neu erhobener Umfragedaten.

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. 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, ein Phänomen, bei dem quantenmechanische Teilchen so miteinander korreliert sind, dass ihre Zustände nicht unabhängig voneinander beschrieben werden können, 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.

Umfrage zur Trendanalyse in der Quantenkommunikation

Zur Identifikation aktueller Trends und von Einschätzungen aus der Forschungs- und Industriecommunity wurde im Juni und Juli 2025 eine Online-Befragung durchgeführt. Die Teilnehmenden wurden zudem gebeten, Forschungsfelder zu benennen, denen in diesem Update des Monitoring-Berichts besondere Aufmerksamkeit gewidmet werden sollte.

In der Umfrage wurden Expert:innen-Einschätzungen zum erwarteten Reifegrad, den Auswirkungen, der kommerziellen Verwertungsreife, den Anwendungsfeldern und Implementierungsherausforderungen zentraler Protokolle und Technologien der Quantenkommunikation sowie zur Entwicklung von Quantennetzwerken gesammelt.

Die Ergebnisse geben einen Überblick über zentrale technologische Trends und aufkommende Anwendungsfelder in der Quantenkommunikation. Die wichtigsten Erkenntnisse werden nachfolgend zusammengefasst.

1) Ausblick auf QCom-Protokolle:

Die Umfrage bestätigt das BB84-Protokoll als das etablierteste Protokoll der Quantenkommunikation. Für E91 sowie für kontinuierliche-Variablen-Quantenschlüsselverteilung (CV-QKD) wird in den kommenden zehn Jahren mit weiterwachsender Bedeutung gerechnet. Fortgeschrittene Ansätze wie messgerätesichere Quantenschlüsselverteilung (MDI-QKD), geräteunabhängige Quantenschlüsselverteilung (DI-QKD) und Twin-Field-Quantenschlüsselverteilung (TF-QKD) werden als vielversprechend eingeschätzt, gelten in Bezug auf den praktischen Einsatz jedoch noch als in Entwicklung.

2) Faserbasierte Quantenkommunikation und Quantenrepeater:

Faserbasierte Quantenkommunikation wird nach Einschätzung der Teilnehmenden eine Schlüsselrolle bei der kurzfristigen Implementierung von Systemen der Quantenkommunikation spielen. Ihre Skalierbarkeit und ihr Potenzial für Übertragungen über große Distanzen hängen jedoch maßgeblich von Fortschritten bei Quantenrepeatern ab, die als essenziell angesehen werden, um Distanzlimitierungen ohne „Trusted Nodes“ zu überwinden und großskalige Quantennetzwerke zu ermöglichen.

3) Marktpotenzial der Quantenkommunikation in verschiedenen Sektoren:

Der kurzfristige kommerzielle Nutzen von Quantenkommunikation wird in Sektoren mit besonders hohen Sicherheitsanforderungen erwartet, insbesondere im Regierungs- und Behördenbereich, in

der Verteidigung sowie im Finanzsektor. Langfristig wird mit einer wachsenden Nachfrage im Gesundheitswesen und in Energieinfrastrukturen gerechnet, da die Digitalisierung voranschreitet und der Schutz sensibler Daten und kritischer Systeme weiter an Bedeutung gewinnt.

4) Rolle von Quantennetzwerken:

Kurzfristig erwarten die Befragten, dass die Quantenschlüsselverteilung die dominierende Anwendung von Quantennetzwerken bleibt und damit den starken Fokus auf sichere Kommunikation widerspiegelt. Langfristig verschieben sich die Erwartungen jedoch hin zu breiteren Anwendungen wie verteiltem Quantencomputing und Quanten-Cloud-Computing. Dies deutet darauf hin, dass Quantennetzwerke künftig auf ein breiteres Ökosystem aus Computing-, Mess- und cloudbasierten Diensten ausgelegt sein sollen.

5) Zeithorizont für Anwendungen von Quantennetzwerken:

Die Antworten weisen auf eine stufenweise Entwicklung von Quantennetzwerken hin, bei der sichere Kommunikation im kommenden Jahrzehnt die kurzfristige Einführung vorantreiben dürfte. Weitergehende Fähigkeiten – etwa verteiltes Quantencomputing, verteilte Quantensensorik und cloudbasierte Quantendienste – werden über einen langfristigen Zeithorizont erwartet, sobald die erforderlichen Schlüsseltechnologien, insbesondere Quantenrepeater, höhere Reifegrade erreicht haben.

Ergebnisse des quantitativen Monitorings

Die Zahl der *Veröffentlichungen* zum Thema Quantenkommunikation ist in den letzten 20 Jahren deutlich und kontinuierlich gestiegen und erreichte im Jahr 2024 mehr als 2000 Publikationen. Die meisten Publikationen stammen aus China (40 % Anteil an globalen Publikationen), dicht gefolgt von der EU (30 %, 10 % aus Deutschland) und den USA (16 %). Eine Zitationsanalyse zeigt, dass Publikationen aus der EU im Durchschnitt 16-mal häufiger zitiert werden als Veröffentlichungen aus den anderen betrachteten Regionen/Ländern. Dies lässt auf eine hohe Relevanz der europäischen Beiträge schließen.

Auch die *Patentierungsaktivitäten* im Bereich der Quantenkommunikation haben in den letzten Jahren stark zugenommen und lagen im Jahr 2023 bei über 250 transnationalen Patentanmeldungen. Die meisten Patentanmeldungen der letzten Jahre kamen dabei aus der EU (34 % Anteil an den analysierten Patenten), gefolgt von den USA (30 %) und China (13 %). Die höchsten Patentaktivitäten verzeichnen Technologieunternehmen, große Telekommunikationsanbieter sowie Forschungsinstitutionen/-organisationen. Auch wenn die meisten Patentanmeldungen aus der Industrie kommen (rund 67 %), wird die Technologie weiterhin stark von Forschungsorganisationen vorangetrieben (rund 33 %).

Die Auswertung zahlreicher zwischen 2019 und 2025 veröffentlichter *Marktstudien* zu Quantenkommunikation, Quantenkryptografie und QKD deutet auf einen in den kommenden Jahren stark wachsenden Markt hin. Der Median der analysierten Marktschätzungen und -prognosen ergibt einen globalen Umsatz in Höhe von rund 1,4 Milliarden US-Dollar im Jahr 2024, der bis 2030 auf etwa 5,4 Milliarden US-Dollar ansteigen könnte. Die meisten Studien prognostizieren jährliche Wachstumsraten zwischen 15 und 25 Prozent.

In einer Analyse der *Förderprogramme* in Deutschland und Europa wurden 83 vom BMFTR geförderte Projekte im Bereich der Quantenkommunikation im Zeitraum 2017 bis 2025 identifiziert sowie 52 Projekte, die durch die EU-Rahmenprogramme Horizon Europe (HE) von 2022 bis 2025 gefördert werden. Die meisten Projekte beschäftigten sich dabei mit QKD, Lichtquellen und Quantennetzwerken. Darüber hinaus ist das Quanteninternet ein wichtiges Thema in HE und wird als strategische Priorität für die EU eingestuft.

Eine Analyse der *internationalen F&I-Strategien* zeigt, dass neben Deutschland und der EU auch viele weitere Länder die wesentliche Bedeutung der Quantenkommunikation in ihren Strategien zu Quantentechnologien hervorgehoben und entsprechende F&E-Programme aufgelegt haben. Zahlreiche Staaten haben ihre Quantenstrategien ausgearbeitet und aktualisiert und investieren signifikant in Quantenkommunikation. Insbesondere die Bedeutung industrieller Anwendungen und satellitengestützter Projekte wurde weiter verstärkt. Hervorzuheben sind hier vor allem China, die USA, das Vereinigte Königreich, Japan, Südkorea, Kanada und Indien.

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 bereiteren Anwendung der Quantenkommunikation. Mit dem Update im Laufe des Jahres 2025 umfasst unsere Übersicht derzeit 27 Testbeds in ganz Deutschland.

Insgesamt zeigen sich im Vergleich zum vorherigen Berichtszeitraum keine fundamentalen Veränderungen, sodass die globale Bedeutung der Technologien der Quantenkommunikation weiter beobachtet werden kann. Unsere Publikations- und Patentanalyse bestätigt, dass die aktivsten Länder – China, die EU und die USA – auch in diesem Berichtszeitraum die wichtigsten Akteure geblieben sind. BMFTR und EU investieren weiterhin in neue F&E-Projekte im Bereich der Quantenkommunikation. Obwohl in einigen Ländern die jährlichen Fördervolumina in den vergangenen Jahren schwankten, ist das insgesamt bereitgestellte Fördervolumen der untersuchten Staaten im Vergleich zum Jahr 2019 gestiegen. Zusammengenommen unterstreichen diese Ergebnisse die anhaltend hohe strategische Priorität und das wachsende globale Engagement für die Weiterentwicklung von Technologien der Quantenkommunikation.

Überlegungen zu Technologiesouveränität

Die Diskussion über die Notwendigkeit, die technologische Souveränität bei kritischen Technologien in Deutschland und Europa zu sichern, hat in den letzten Jahren erheblich an Dynamik gewonnen. Dies gilt insbesondere für sichere Kommunikation, da sie nationale Sicherheit, den Schutz von Geheimnissen und Privatsphäre sowie die Integrität wirtschaftlicher und politischer Prozesse gewährleistet und damit einen fundamentalen Bestandteil der kritischen Infrastruktur eines Staates darstellt. Im Rahmen dieser Studie wurde analysiert, wie deutsche Expert:innen für Quantenkommunikation Aspekte technologischer Souveränität einschätzen. In diesem Zusammenhang wurde häufig auch ein über die technologische Souveränität hinausgehendes Ziel betont, nämlich 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 technologischer Souveränität wurden bereits im vorherigen Bericht identifiziert und nun in unserer Umfrage quantitativ erfasst. Als besonders bedeutsam wurden vor allem hohe Kosten, ein mangelndes Bewusstsein potenzieller Endnutzer:innen, fehlende Kund:innen für QKD-Lösungen (sowohl im privaten als auch im öffentlichen Sektor) sowie das Fehlen von zertifizierten und zugelassenen Geräten und Normen in der Quantenkommunikation genannt.

Maßnahmen zur Erreichung von technologischer Souveränität könnten entsprechend die Fortführung der öffentlichen Finanzierung, Kaufanreize für Endnutzer:innen in der Industrie, Investitionen

in europäische Infrastruktur sowie Öffentlichkeitsarbeit und Bildungsprogramme für Interessenvertreter:innen 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 sowie eine Verschlankung und ein Abbau der Bürokratie dar.

Executive Summary

Secure communication forms a cornerstone of free societies and is essential for the reliable operation of critical infrastructures. Cryptographic methods play a central role in ensuring this. However, developments in quantum computing may allow current encryption protocols to be broken in the foreseeable future; therefore, "quantum-secure" approaches to encrypting communications are urgently needed. The emerging technology of quantum key distribution (QKD), which enables physically secure communication based on quantum mechanical principles, together with technologies that transport or exchange quantum states over longer distances, are encompassed by the term quantum communication.

This report provides an overview of the technologies and technological generations of quantum communication. It analyzes developments in research, industrialization, test infrastructure and the market, and discusses the relevance of technology sovereignty in quantum communication. It is an update of the previous version (Monitoring Report 1 – Quantum Communication, published in 2024) and is based on recent literature on technological advancements in this field, new quantitative data on publications and patents, market studies, projects, funding, and testbeds. Additionally, the report includes further analysis of technology trends based on newly collected survey data.

Overview of technologies by generation of quantum communication

Quantum communication can be systematically divided into three generations based on the development stage of the technologies:

First generation - quantum key distribution following the prepare-and-measure principle:
Qubits are prepared in different, randomly selected quantum states and sent to the receiver via communication channels. By preparing and measuring the quantum states, e.g., the polarization of the photons, and exchanging specific information about them, a secure key can be generated that is then used to encode the actual message. Any attempt by an attacker to eavesdrop or copy the quantum states results in changes in state that can be detected by the sender and the receiver. Prepare-and-measure QKD is already a market-ready technology for secure communication. However, its widespread use is currently being hampered by high costs, pending proofs of security, certification and approval.

Second generation - quantum key distribution with photonic entanglement sources:
Quantum entanglement, a phenomenon in which quantum mechanical particles are correlated in such a way that their states cannot be described independently, can be used for secure communication. The starting point is a source of entangled photons that are split between two communication partners. The two communication partners each measure their photon and can generate a common key bit or prove the entanglement of the photons by exchanging certain information about the measurement. Any interference or attempt to eavesdrop inevitably breaks the entanglement and is therefore detectable. Entanglement-based QKD is not yet as mature as prepare-and-measure QKD and only achieves low key rates at present, but could be advantageous for complex communication networks.

Third generation - quantum repeaters with entanglement distribution:
The third generation describes the development of quantum repeaters that enable entanglement distribution over long distances. The starting point is the limited range of QKD. To increase this range, research is being done on quantum repeaters, which divide a longer transmission link into shorter sections and use entanglement swapping to increase the range of quantum entanglement without measuring or copying quantum states. The entangled states generated by quantum re-

peaters can be used for second-generation entanglement-based QKD and for quantum teleportation over large distances. The latter makes distributed quantum computing possible and could increase the computing power of quantum computers. Quantum repeaters can therefore make an important contribution to the development of future quantum communication networks and are highly relevant for society in terms of IT security and the protection of critical infrastructure. However, at present, quantum repeaters are still undergoing research and are not yet technologically mature enough for commercial applications.

Survey on Trend Analysis in Quantum Communication

To identify current trends and gather insights from the research and industry community, an online survey was conducted in June and July 2025. Participants were also invited to highlight research areas that should receive particular attention in this update of the monitoring report.

The survey collected expert assessments on the anticipated maturity, impact, commercial readiness, application domains, and deployment challenges of major quantum communication protocols and technologies, as well as on the development of quantum networks.

The results provide an overview of key technological trends and emerging application areas in quantum communication. The main findings are summarized below.

1) Outlook for QCom Protocols:

The survey confirms BB84 as the most established quantum communication protocol, while E91 and Continuous-Variable Quantum Key Distribution are expected to gain further traction over the next decade. More advanced approaches such as Measurement-Device-Independent Quantum Key Distribution (MDI-QKD), Device-Independent Quantum Key Distribution (DI-QKD), and Twin-Field Quantum Key Distribution (TF-QKD), are perceived as promising but still emerging in terms of deployment.

2) Fiber-based QCom and Quantum Repeaters:

Fiber-based quantum communication is expected to play a key role in the early deployment of quantum communication systems. However, its scalability and long-distance potential depend strongly on advances in quantum repeaters, which are considered essential for overcoming distance limitations without the use of trusted nodes and enabling large-scale quantum networks.

3) Market Potential of QCom across Sectors:

Quantum communication is expected to generate its earliest commercial value in sectors with particularly high security requirements, notably government, defense, and financial services. In the longer term, demand is expected to grow in healthcare and energy infrastructures as digitalization increases and the protection of sensitive data and critical systems becomes more important.

4) Role of Quantum Networks:

Respondents expect Quantum Key Distribution to remain the dominant application of quantum networks in the short term, reflecting the strong focus on secure communication. In the longer term, however, expectations shift toward broader applications such as Distributed Quantum Computing and Quantum Cloud Computing, indicating that quantum networks are anticipated to support a wider ecosystem of computing, sensing, and cloud-based services.

5) Timeline for Quantum Network Applications:

The responses point to a staged development of quantum networks, with secure communication expected to drive early adoption in the coming decade. More advanced capabilities – such as Distributed Quantum Computing, Distributed Quantum Sensing, and cloud-based quantum services –

are anticipated to emerge over the longer term as enabling technologies, particularly quantum repeaters, reach higher levels of maturity.

Results of the quantitative monitoring

The number of *publications* on the topic of quantum communication has risen significantly and continuously over the last twenty years and reached more than 2000 in 2024. The majority of these publications were from China (40% share of publications), closely followed by the EU (30%, 10% from Germany) and the USA (16%). A citation analysis reveals that, on average, publications from the EU are cited 16 times, more frequently than publications from the other regions/countries analyzed, suggesting a high relevance of European publications.

Patenting activities in the field of quantum communication have also increased significantly in the past few years, with more than 250 transnational patent applications in 2023. The majority of recent patent applications have come from the EU (34% share of patents), followed by the USA (30%) and China (13%). Technology enterprises, large telecommunications providers, and research institutions/organizations show the highest levels of patent activity. Even though most patent applications are from industry (approx. 67%), the technology continues to be strongly driven by research organizations (approx. 33%).

An analysis of numerous market studies published between 2019 and 2025 on quantum communication, quantum cryptography and QKD indicates that the market will grow strongly in the coming years. The median of the analyzed market assessments and projections point to a global turnover of around 1.4 billion dollars in 2024, which could increase to 5.4 billion dollars by 2030. Most of the studies forecast annual growth rates of between 15 and 25 percent.

An *analysis of the funding programs* in Germany and Europe identified 83 projects in the field of quantum communication funded by the BMFTR from 2017 to 2025, and 52 projects funded by the EU Framework Programme Horizon Europe (HE) from 2022 to 2025. The majority of these projects focus on QKD, light sources, and quantum networks. In addition, the quantum internet is an important topic under HE is assigned a high strategic priority for the EU.

Analyzing the international R&I strategies reveals that, in addition to Germany and the EU, other countries have recognized the strategic importance of quantum communication in their quantum strategies. Numerous countries have developed and updated their quantum strategies and are making significant investments in quantum communication. In particular, the importance of industrial applications and satellite-related projects has been further highlighted. China, USA, UK, Japan, South Korea, Canada, and India should be mentioned in particular.

To provide an *overview of the existing test infrastructure*, this report includes a map of the so-called *testbeds* for quantum communication in Germany, including a brief description of each one. The construction of (test) infrastructure is hugely important for the industrialization and widespread application of quantum communication. With the update over the course of 2025, our list currently comprises 27 testbeds throughout Germany.

Overall, no fundamental change from the previous reporting period was observed, indicating that the importance of quantum communication technologies has been retained globally. According to our publication and patent analysis, the most active countries (China, the EU, and the USA) remained the major players as of this reporting period. BMFTR and the EU have continued to invest in new R&D projects in the field of quantum communication under their funding programs. Although some countries have seen fluctuations in the amount of annual funding in recent years, in general, the total investment of the countries investigated has increased compared to the 2019 level. Taken together, these results highlight the sustained strategic priority and growing global commitment to advancing quantum communication technologies.

Technology sovereignty considerations

The discussion about the need to ensure technological sovereignty for critical technologies in Germany and Europe has gained momentum in recent years. This is particularly true for secure communication, as this guarantees national security, the protection of secrets and privacy, as well as the integrity of economic and political processes, and is therefore a fundamental component of a nation's critical infrastructure. Within the scope of this study, we analyzed how German quantum communication experts assessed aspects of technological sovereignty. In this context, the goal of leveraging the future economic potential of quantum communication technologies was frequently emphasized, going beyond technology sovereignty.

Requirements in Germany and Europe include the *need* to understand quantum communication technologies at least at a system-level in order to be able to develop and produce them. Importing the required components while avoiding one-sided dependencies is not regarded as problematic, provided that the security of the imported components and systems can be tested.

Challenges to achieving technology sovereignty were identified in the previous report and are further assessed in our survey. The challenges most frequently identified as important include high end-to-end costs, a lack of awareness among potential end users, a lack of potential customers for QKD solutions (in both the private and public sectors), as well as a lack of certified and approved devices and standards in quantum communication.

Measures to achieve technology sovereignty could accordingly include continued public funding, purchase incentives for end users in industry, investments in European infrastructure, as well as public relations and educational programs for stakeholders from the relevant specialist areas. Other measures include promoting technology transfer to industry, cooperation along the value chain, removing barriers to approvals, supporting standardization and certification activities, close cooperation between the authorities of the European member states, and streamlining and reducing bureaucracy.

1 Introduction

Information technology and telecommunications is defined by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) as one of the ten critical infrastructure sectors. Cryptographic methods have been developed and used for centuries to ensure secure communication, as this not only protects the privacy of the communicating individuals but is also required to protect a state's ability to act. With the rise of quantum computing, there is a growing threat to conventional encryption methods. Even before quantum supremacy has been reached, secrecy keeping is at risk due to "harvest now – decrypt later" strategies. This makes it necessary to act now. Quantum communication (QCom) technologies are one potential approach to address this threat and achieve potentially perfect security along the transmission path. Achieving and securing technology sovereignty in quantum communication has therefore been formulated as one goal of the German government.

In this monitoring report, we want to give an overview of the current state of quantum communication research, technology, and economy within Europe and discuss aspects of technology sovereignty. A combination of methods (section 2) was applied to obtain a detailed picture.

This report is an update of the monitoring report published in 2024 [1]. The new version includes updated data for patents, publications, projects and funding; an extension of the trend analysis to account for recent developments; and most importantly the results from a survey conducted among experts from the quantum communication community.

The background of quantum communication is shortly introduced (section 3). In the qualitative analysis (section 4), the state of research in quantum communication is discussed, different software and hardware approaches are introduced, the potential evolution of technology generations is highlighted, and the survey results are presented. Based on these results, this update takes a closer look at several developments and particularly prominent trends that have gained considerable momentum in recent years but were not examined in detail in the previous edition of the monitoring report.

The quantitative analysis (section 5) includes a patent and publication analysis, which identified the players from science and industry and outlined the global dynamics. The player analysis is complemented by a meta-market analysis. Besides analyzing the actors most often mentioned, potential market sizes for QCom technologies were also explored. The funding priorities of research projects in Germany and Europe were identified, providing insights into the strategies of the respective policymakers. Subsequently, the quantum communication strategies of various countries were analyzed and compared.

The concept of technological sovereignty is introduced and applied to quantum communication (section 6). Based on expert interviews and survey results, a discussion of the capabilities in the field of European quantum communication is presented and potential challenges and measures are discussed.

Finally, conclusions are drawn from the results presented (section 7) and an outlook on potential further activities is provided.

2 Methods

Qualitative Analysis and Survey on Quantum Communication

The qualitative analysis is based on desk research, including the analysis of current scientific literature. To complement these findings, a survey was conducted among experts from the quantum communication community. In section 4.4, a detailed introduction to the methodological approach is provided and the survey results are discussed. A complete overview of the survey results is given in appendix A.1. Building on these results, section 4.5 takes a closer look at several developments that have gained considerable momentum in recent years but were not covered in detail in the previous edition of the monitoring report.

Publication Analysis

Peer-reviewed publications for the publication analysis were extracted from "Web of Science" using a keyword-based search. The search was limited to peer-reviewed publications to identify "key publications" that allow a comparison of R&D activities between countries and key organizations. The following search string was used to search in title, abstract, and keywords of the publications:

{"quantum communication" OR "quantum key distribution" OR ("quantum cryptography" NOT "post-quantum cryptography") OR "quantum repeater" OR ("quantum memory" AND communication) OR ("entangled photon" AND communication) OR (entanglement AND communication AND quantum) OR ("entangled state" AND communication) OR (entanglement NEAR distribution) OR ("Bell state" AND communication) OR "quantum teleportation" OR "quantum information transmission" OR "quantum network" OR "quantum internet" OR (QKD AND quantum)}*

Compared to the first monitoring report, the following search terms were added: "quantum teleportation", "quantum information transmission", "quantum network*", "quantum internet", and "QKD and quantum". Some others terms were adjusted to reduce the number of false hits.

Citation analyses were carried out using the QCom-related publications from 2022. We chose this year as it allows sufficient time for citation but is still relatively recent. Compared to the first monitoring report the time for citation is slightly shorter, which results in lower absolute citation numbers. However, the comparison between the numbers of different countries is relevant for this analysis, not the absolute numbers.

Patent Analysis

The total number of patent applications was identified using a search strategy based on both patent classification codes and a keyword-based text search of titles, abstracts, and claims. In order to enable a fair comparison between the patenting activities of different countries, the search was restricted to transnational patent applications, i.e., patent applications to either the European Patent Office (EPO) or the World Intellectual Property Organization (WIPO). Differences in national patenting systems tend to lead to an overestimation of patenting in certain countries when only considering national patent offices. Additionally, transnational patents are typically linked to inventions with a higher expected economic value.

The following search string was used:

"quantum communication" OR "quantum key distribution" OR ("quantum cryptography" NOT "post-quantum cryptography") OR "quantum repeater" OR ("quantum memory" AND communication) OR ("entangled photon" AND communication) OR ((entanglement AND communication AND quantum) OR ("entangled state" AND communication) OR (entanglement(3W)distribution) OR ("bell state" AND

communication) OR ("quantum teleportation" OR "quantum information transmission" OR "quantum network?" OR "quantum internet") OR (H04B0010-70/IPC,CPC OR (H04L0009-0852 OR H04L0009-0855 OR H04L0009-0858)/CPC) OR (QKD AND (H04! OR G02! OR G06! OR G09! OR B82! OR C!!!)/IPC) AND (WO OR EP)/PC

Equivalent to the publication analysis, certain search terms were added and others adjusted.

Meta-Market Report Analysis

For the meta-market report analysis, the search engine Google was used to search for relevant market reports on quantum communication, quantum cryptography and quantum key distribution. This method does not guarantee completeness, but we identified 136 relevant market reports with publishing dates from January 2019 to April 2025. Access to market reports is typically very cost-intensive, so we relied exclusively on the free information that is available on the homepages of the market report providers. This includes global revenue estimates and forecasts, expected growth rates, and relevant players in the field of technology. We collected this information systematically, interpolated missing forecast values under the assumption of uniform growth and analyzed the revenue forecasts and company mentions.

Project Monitoring

The search for BMFTR projects was carried out using the official website of the ministry listing calls and funded projects in the areas of IT security and communication systems [2]. The projects related to quantum communication were identified based on the information provided in the project description page such as objectives and approach. For EU projects, we used the CORDIS project database [3]. The search methodology for the EU database included a first round of filtering applying the aforementioned search string used for publication analysis to the titles and abstracts of projects. In the second round, related projects were selected based on the content of their abstracts. In some cases, further investigation was conducted using the projects' websites or publications.

International Situation and Initiatives

Governments typically do not disclose the total public funding in QCom technologies. Therefore, we focused on the most relevant quantum strategies in the US, UK, and Japan to collect data, namely:

- US: National Quantum Initiative (NQI) [4]
- UK: National Quantum Technology Programme (NQTP) in 2014-2023 and National Quantum Strategy in 2024-2034 [5]
- JP: Quantum Technology and Innovation Strategy [6]

For the EU and Germany, we used the project monitoring data shown in section 5.4. In addition, the EuroQCI initiative was included for the EU, as it plays a significant role in supporting deployment. The programs examined are:

- EU: Horizon 2020/Horizon Europe and the European Quantum Communication Infrastructure (EuroQCI)
- DE: Framework programs "Quantensysteme" and "Digital. Sicher. Souverän"

Despite its importance in the field, official information on China's investment in QCom research is difficult to obtain. Previous research has shown drastically diverging figures from different sources [7]. Therefore, our analysis only provides a rough estimate of China's investment.[1]

In exploring the QCom funding to the total quantum technology R&D, the following references were used: the NQI report for the US [8]; the documents from the Quantum Technology Innovation Committee for Japan [9]; parliamentary document for Germany [10]; the NQTP website for the UK [5]; and the JRC report for the EU [11]. To examine the development of funding over time, data on the annual distribution of estimated funding for Germany and the EU were derived from our project monitoring. This means that the annual distribution was obtained by multiplying the number of projects started in the year by the average project budget. The EuroQCI was excluded from the EU due to missing time series data.

Data for the US were derived from the NQI Annual Budget Report 2025, which provides the actual budget for FY2019-2023, the estimated budget for FY2024, and the proposed budget for FY2025 [8]. In Japan, budget planning is usually based on a single year, and our data mostly reflect the actual annual allocation to projects and programs. When annual budget data was not available (e.g., SIP program), the annual average of the whole project budget was used. The UK was not analyzed in this subsection, due to the lack of available information on the temporal distribution of funding.

The yearly average exchange rate from the European Central Bank (ECB) for 2025 is used in the texts of Section 5.5.1. In Section 5.5.2, the yearly average exchange rate from the ECB of the corresponding year was used for the analysis of the US and JP data for each year.

Technology Sovereignty

The discussion of aspects of technology sovereignty in quantum communication was based on five interviews with experts from science, industry, and politics in 2023 (results presented in the initial monitoring report [1]). The interviewees were introduced to the concept of technological sovereignty as developed by Fraunhofer ISI [12]. The aim of the interview was to obtain the expert's assessment of the status quo of European quantum communication in terms of needs and requirements (what level of sovereignty should Europe strive for in quantum communication?), legitimation and motivation (why do we need technological sovereignty in quantum communication?), challenges (what challenges have to be overcome to achieve technological sovereignty in quantum communication?), and measures (how can these challenges be addressed by science, industry, and politics?). The discussion of the status quo, the challenges and measures was structured by referring to the factors hampering innovation, as discussed in the OECD's Oslo Manual [13].

The analysis has been updated by integrating results from the survey (section 4.4) and based on a workshop from the SQuaD consortium, both held in 2025.

Survey on Trend Analysis in Quantum Communication

The survey included 20 questions on quantum communication, quantum technologies, and quantum networks, organized into four thematic blocks. The first block collected participants' institutional and project affiliations. The second covered quantum communication protocols and technologies, asking respondents to rate their expected maturity over the next ten years, potential impact,

[1] The estimation of Chinas's investment in quantum communication (QCom) is made by multiplying the announced government investment of China in all quantum technologies (QT) (according to OECD 2025) with the averaged ratio of QCom funding to QT funding in other analyzed countries.

and likelihood of commercial availability, as well as to identify key application areas, beneficiary sectors, and obstacles to large-scale deployment.

The third block focused on quantum networks, exploring critical factors, roadblocks to real-world implementation, and the most significant future applications. The final block invited suggestions for additional topics for the monitoring report and general comments.

The survey was conducted online via the open-source platform LamaPoll. Participation was voluntary and unpaid.

The link was emailed to coordinators of BMFTR-funded projects (SQuaD, QR.N, DIVQSec, and QuNET) and to industry-led projects in the quantum communication innovation hub (6G-QuaS, Q-Fiber, DE-QOR, Quant-ID, DemoQuanDT, and QUIET). It was also promoted at the World of Quantum 2025 trade fair in Munich through QR codes on table stands and flyers.

A total of 63 respondents completed the survey, and 46 provided partial responses. Both were included in the analysis where the relevant questions were answered, resulting in 50–63 responses per question. To protect privacy, no personal data (e.g., country of origin, age, or gender) was collected, preventing identification of individual participants.

Respondents' professional background was assessed through questions on institutional and project affiliations (multiple selections possible). Nearly half of participants were from academia (n = 29), followed by non-university research institutions (n = 14) and industry – mainly technology or service providers (n = 12). The remainder came from federal agencies (n = 7), industry users (n = 1), and associations (n = 1).

In terms of project affiliation, most respondents were linked to QR.N (n = 33), SQuaD (n = 28), and QuNET (n = 25). Smaller numbers were affiliated with DIVQSec (n = 8), the quantum communication innovation hub (n = 7), Q-net-Q (n = 2), and MuQuaNet (n = 1). Two respondents reported no affiliation with any listed project.

In the analysis (section 4.4), thematically related questions were grouped and examined together. Drawing on the survey results, the report highlights several developments that have gained considerable momentum in recent years but were not covered in detail in the previous edition (section 4.5).

3 Background

In a digitalized world in which information is transferred from A to B via the internet in a matter of seconds, cryptography plays a crucial role in protecting privacy and IT security. The bottom line is that this means the encryption of digital information to ensure that sensitive data are protected against manipulation and unauthorized access. Cryptography is more than just a tool for secrecy, as it now forms the foundation for the security of critical infrastructures such as government communications, health care, energy and water supply and much more. Not only does it allow information to be encrypted from sender to receiver, it also ensures the secure functioning of applications and is therefore an essential part of today's hyperconnected world, which is also of central importance for banks, authorities, data centers, and companies. In the financial sector, e.g., cryptography is indispensable for protecting online transactions. Banks use complex encryption technologies to ensure that money transfers and other financial operations are protected from fraudulent activity. A prime example of this is blockchain technology, which is based on advanced cryptography and is used in cryptocurrencies such as Bitcoin (BTC). This decentralized, secure transaction processing method has had a lasting impact on the financial industry and continues to demonstrate how cryptography is driving innovations. Without it, our communication, our finances, and our privacy would be massively at risk. It is clear that its use is now ubiquitous in every conceivable area of daily life and continues to gain ground.

In recent years, the fields of quantum computing, quantum sensing, quantum simulation, and quantum communication have emerged as new, important areas of development and investment and are seen as key areas in research and industry. What these four thematic technology pillars have in common is that they make use of the laws of quantum mechanics, i.e., that branch of physics that describes the behavior of particles at the atomic and subatomic levels. The applications of quantum technologies are diverse and range from quantum sensors and quantum computers to cryptographic systems. Quantum cryptography offers a way of making digital communication secure and guaranteeing encryption at the highest level of security. Unlike modern encryption protocols such as RSA (Rivest-Shamir-Adleman) or ECC (Elliptic Curve Cryptography), it is not based on the expected complexity of a mathematical algorithm, but on fundamental physical laws of nature, which can be used to achieve a level of security that is superior in terms of information theory. Quantum technologies are currently in various stages of development, but hold promising potential for Germany as a business and science location and could be used extensively in different areas and sectors of modern society in the future. In the field of quantum communication, research and development face a considerable challenge to develop practicable technologies that meet the security requirements for communication and at the same time satisfy strict criteria such as high communication rates and resilience to side-channel attacks, so-called hacking attacks. The overarching goal is to create systems that are not only secure and scalable, but also cost-effective in order to ensure their widespread availability for society.

In quantum communication, information is transmitted based on fundamental principles of quantum mechanics that go far beyond classical physics. Quantum cryptography is particularly important in this context. This refers to the use of quantum physics to support data encryption. This not only enables the fundamentally tap-proof exchange of keys over long distances, but also points to a promising future in which quantum technology could play a pivotal role in digital communication. Even if the mathematical cryptographic methods currently in use cannot be broken by modern computers at reasonable cost and within a reasonable time and are therefore considered secure, it should not be forgotten that the security of digital information depends not only on vigilance but also on constant research and development. Immensely powerful quantum computers pose the greatest threat in this regard. Back in 1994, the US mathematician and computer scientist Peter

Shor presented his groundbreaking quantum algorithm called "Shor's Algorithm". This algorithm factors large integers into their prime components and highlights the ability of quantum computers to solve problems that require extremely high computational effort on classical computers and therefore form the basis of asymmetric public-key cryptography. Since quantum computers can break cryptographic keys in polynomial rather than exponential time thanks to an efficient algorithm, it can be assumed that they are fundamentally capable of undermining the security of numerous current encryption methods. Furthermore, it is already possible today to intercept conventionally encrypted data and decrypt it at a later point in time ("harvest now, decrypt later"). This means that a hacker could use a quantum computer to gain access to information that was encrypted in the past. The long-term storage of data and subsequent access to it raises massive security concerns that need to be carefully considered today to ensure the integrity and confidentiality of digital information in the age of quantum computers. In short, quantum computers have the potential to break some of the encryption algorithms currently in use and to make communication insecure. To ensure IT security in a quantum computing world, encryption techniques must be developed that are robust against quantum attacks, and the related tap-proof communication networks must be built.

Although no quantum computer currently exists that could circumvent the public key cryptography methods used today, the US National Security Agency (NSA) warned of this potential danger back in 2015. In the working hypothesis of its 2017-2020 study "Entwicklungsstand Quantencomputer (Development status of quantum computers)" [14], the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) assumes that the first cryptographically relevant quantum computers will be available until 2040. Based on this, it initiated the paradigm shift to quantum-resistant cryptography in the field of post-quantum cryptography (PQC) together with the framework program "Quantentechnologien – von den Grundlagen zum Markt (Quantum technologies – from basic research to market)" [15], which was launched by the German Federal Ministry of Research, Technology and Space (Bundesministerium für Forschung, Technologie und Raumfahrt, BMFTR) in September 2018.

Two solution strategies are currently being pursued to accomplish the transition to quantum-secure encryption: quantum key distribution (QKD) and the aforementioned post-quantum cryptography (PQC). The latter is a further development of classical public key cryptography. In this context, new cryptographic methods based on classical information theory are being developed, which cannot be broken even using powerful future quantum computers and which are more complex than the known prime factorization. Among these methods are algorithms based on lattice-based protocols [16].

Though this does not require any special hardware, it relies on conjectures about hardness of solving certain mathematical problems and therefore cannot provide “information-theoretic” security guarantees [17], which leaves the possibility that mathematical breakthroughs could introduce new vulnerabilities in the long term. One prominent example to promote the development of PQC is led by the US National Institute of Standards and Technology (NIST): The NIST has been organizing a public standardization process to investigate the vulnerability of numerous proposed methods in a multi-stage process since 2017, drawing on the expertise of the entire cryptographic community. Only one algorithm for public-key encryption/key encapsulation mechanisms and three algorithms for digital signatures were identified for standardization in 2022: the CRYSTALS-Kyber key-establishment method and the CRYSTALS-Dilithium, Falcon and SPHINCS+ signature methods [18]. In addition, the three code-based key agreement methods Classic McEliece, BIKE and HQC as well as other signature methods were selected as the candidates to advance to the fourth round. In 2025, NIST has selected HQC for standardization. HQC will serve as a backup for ML-KEM, the main algorithm for general encryption [19].

Today, quantum cryptography is considered one of the pillars for the security of digital infrastructures in our society—see for example the Hightech Agenda Deutschland including quantum communication as a key technology [20]. By harnessing quantum physical effects, it promises secure key exchange between two parties even in the age of quantum computing. Research in this field strives to develop protocols for the secure exchange of cryptographic keys, which can be used to reliably detect eavesdropping attempts from the result of unintended modifications caused by measurements being part of the protocols. Instead of transmitting the messages themselves, symmetric keys are generated which can be used to encode the message to be transmitted. The encryption allows the transmission to take place via a classical, possibly insecure channel. For this reason, quantum cryptography is regarded as groundbreaking for tap-proof key distribution within communication and information networks and is currently the subject of a wide range of research and development efforts. One example of such a cryptographic method is QKD, which is described in more detail in the following section.

4 Qualitative Analyses: Theoretical Foundations and Research on Quantum Communication

In order to show the current state of research and the latest developments in the field of quantum communication, an overview of the theoretical foundations and current national and international activities is provided below. A systematic, sequential structure is used, with the different generations reflecting the development status of the technology discussed, from advanced to elementary. Each generation represents a stage in the realization, implementation, and integration into the existing infrastructure. The generations are divided into: 1. Quantum Key Distribution following the prepare-and-measure principle, 2. Quantum Key Distribution with photonic entanglement sources, and 3. Quantum repeaters with entanglement distribution.

4.1 First Generation: Quantum Key Distribution (Prepare-and-Measure)

4.1.1 Theoretical Foundations

Quantum cryptography offers the possibility to make digital communication tap-proof using single photons and ensuring encryption at the highest level of security. As mentioned above, this provides security based on physical principles rather than on algorithms. The main purpose of Quantum Key Distribution (QKD) is to guarantee the security of the keys generated jointly by the sender and receiver. The physical foundations of the first generation, quantum superposition and the no-cloning theorem, are outlined below.

- **Quantum superposition**: Quantum superposition is a fundamental principle of quantum mechanics that states that a quantum particle can exist not only in one state, but at the same time in a superposition of any number of states. In quantum cryptography, this is used to generate secure keys based on quantum mechanical principles with which messages can be encoded and decoded. In this sense, quantum bits (qubits), the smallest logical units in quantum information, can assume different key values simultaneously. An attacker attempting to intercept the key would not know what state the qubit is in due to the superposition principle until he measures it—because the decision for a final state is only forced by the measurement itself. After the measurement, the quantum system is no longer in the superposition state, but in a certain eigenstate, which is determined by the measurement result—the superposition is destroyed by the measurement. In a transmission protocol of the legitimate communication partners (see below), the measurement carried out by the attacker generates errors that the communication partners can detect and thus prove the attack. One challenge in key generation is the decoherence of qubits, where superposition can be disturbed by external influences—especially over long transmission distances—due to the inherently fragile nature of qubits. However, if qubits are encoded on the states of photons, it is possible to benefit from the comparatively low decoherence of the light particles.
- **No-cloning theorem**: According to the quantum mechanical no-cloning theorem by William Wootters and Wojciech Zurek (1982) [21], it is not possible to produce an exact copy of an unknown quantum state without changing the state of the original system. Whenever the state of a quantum object (e.g., a photon) is copied, the state of the original

object is inevitably modified. This principle has a significant impact on IT security, as it ensures that an attacker cannot copy a quantum key undetected without necessarily changing its state.

As part of QKD, identical keys in the form of random bit sequences are generated simultaneously at the sender and receiver. The subsequent encryption and decryption using the identical keys means that communication can also take place via an insecure channel without either party having to worry about the integrity of the data.

How QKD functions can be described as follows: QKD uses qubits that can be represented in different ways. One option is to employ attenuated coherent light pulses or single photons prepared in complementary quantum states with non-orthogonal bases, such as horizontal/vertical and diagonal/antidiagonal polarization. In the first step, the transmitter generates qubits (e.g., as single photons), which are encoded in a random sequence of 0 and 1 and in random bases and then transmitted to the receiver via a communication channel such as a fiber optic cable (*Prepare*). This is done individually for each photon and without prior agreement between the two parties. The legal receiver in turn measures the individual qubits in randomly selected measurement bases (*Measure*). The sender and receiver exchange information about the selected preparation and measurement bases via a public channel and only use those measurement results where the bases match (because only then does a measurement provide a deterministic result). If an attacker attempts to eavesdrop or copy the qubits during transmission, he must select a random measurement base and carry out a measurement. This inevitably changes the qubit state in line with the no-cloning theorem. This change of state does not go unnoticed, as the transmitter and receiver compare the states of a subset of the transmitted and received particles. A high error rate in this comparison—in relation to the channel losses—indicates an attack. Accordingly, an attacker can intercept information about the key, but cannot do so without being detected by the sender and receiver. In this case, the protocol aborts before sensitive data are encrypted and transmitted, which highlights the security of QKD as a fundamentally tap-proof procedure. To increase security, several key bits can be combined using logical operations ("privacy amplification") to obtain the so-called sifted key, with which the information to be transmitted can be encrypted and decrypted. If a key is at least as long as the message, is randomly generated, kept secret and never recycled, i.e., is used as a one-time pad (OTP), it is demonstrably impossible for the encrypted message to be broken by an unauthorized party during transmission [22]. The practical benefit of QKD is therefore to ensure that the keys agreed by the sender and recipient remain secret and unchanged in order to transmit messages that are tap-proof based on information theory.

In its position paper published in 2024, the BSI and its international partners point out the limitations of QKD. One of these is, e.g., that, unlike the PQC already available today, QKD cannot be implemented using current technology, but requires specialized hardware, which in turn is expensive. In addition, signal losses in fiber-optic cables limit the distance and therefore the field of application. Eventually, the security of specific implementations of QKD has not yet been proven. The commercial use of QKD is now being tested in many field trials, but is currently still limited to a few niche applications [23].

4.1.2 Encoding Variants

In the following, the term *variable* refers to the quantum properties or degrees of freedom (DOF) used to encode information. Fundamentally, QKD can be implemented in different ways or in different quantum states, namely in discrete or continuous states. These two also represent two classes of quantum key exchange methods. The variant of QKD described in the previous section is based on discrete variables (DV), which is why they are called "DV-QKD" protocols. This means that the states of the qubits are discrete in nature. These protocols are based on the uncertainty principle

(superposition and no-cloning theorem). Correspondingly, CV-QKD protocols refer to encoding principles in which qubit states are continuously distributed [23]. In contrast to DV-QKD protocols, CV-QKD protocols work with infinite-dimensional quantum states.

The encoding of qubits can take place in different degrees of freedom of a physical system. An example already mentioned is the polarization of a photon or a light pulse in non-orthogonal bases (horizontal/vertical, diagonal/antidiagonal, left/right circular). Light states can also be encoded using their arrival time (time-bin) or spatial modes. In CV-QKD protocols, states are defined by their amplitude and phase angle relative to a reference wave. The two classes (DV and CV) of quantum key exchange methods are explained below.

DV encoding

DV encoding uses discretely distributed degrees of freedom of a physical system for encoding, e.g., the binary distribution "horizontal polarization" or "vertical polarization" of a light particle for the states 0 and 1 or two defined energy states of an electron.

The oldest and best-known method for QKD is the BB84 protocol introduced by Gilles Brassard and Charles Bennett in 1984, which has been used as a standard since the first implementations in the early 1990s. This is a DV-QKD protocol that uses the prepare-and-measure method described above. In the original version, it uses the polarization degrees of freedom of single photons for transmission. The advantage of a DV-QKD protocol such as the BB84 protocol, in addition to its robustness and long range of approx. 100 km, is the simplicity of its modulation, as the techniques used are easy to implement and control. Its disadvantage, however, is that the photon detection methods required are expensive and complex [24].

The BB84 protocol was originally formulated for single photons, which entails a great deal of effort for the generation and detection of single photons. Sending very weak laser pulses is technically much simpler, but there is always a certain probability that there will be light pulses in which more than one photon could be detected. One eavesdropping strategy would be to split off a part of the light pulse, wait until the correct base is known from the communication between transmitter and receiver, and only then measure it. In this way one could obtain complete information from these tapped signals. However, by cleverly using weak light pulses with different intensities (so-called "decoy states"), these weak light pulses can still be used for quantum key exchange, which makes their practical application much simpler. In this method, the communication partners test whether an attacker splits off larger portions of more intense light pulses than of weaker ones, which is an attack strategy that minimizes the chance of detection. The decoy state variant of the BB84 protocol is used today in almost all DV-QKD applications.

CV encoding

Quantum cryptography includes not only discrete methods for quantum key exchange, but also those based on continuous variables. While DV-QKD protocols, as just described, encode information in discrete states of single photons, CV-QKD protocols use continuous parameters such as the amplitude and phase of light for encoding and measurement.

CV-QKD was first proposed by Timothy C. Ralph in 1999 [25] and converted into a practicable protocol [26] by Frédéric Grosshans and Philippe Grangier. Phase coding is typical for CV-QKD, i.e., the transmitter selects a fixed amplitude of a light field (laser) and random phases that are imposed on the light field by phase modulators. Ideally, these phases follow a Gaussian distribution in phase space; in principle, they can assume an infinite number of values, whereby the probabilities for these values are Gaussian-distributed. In practice, this is difficult to realize, so the Gaussian distribution is

approximated by discrete distributions with a finite number of phase settings. These discrete modulation schemes use M different phase values and correspondingly M equidistantly distributed coherent states in the phase space ("M symbol quadrature modulation").

A typical key generation protocol runs as follows: The transmitter prepares one of M different coherent states and sends it via a channel to the receiver, which measures the state using a homodyne method (determination of amplitude and phase relative to a reference wave). During homodyning, the optical signal is interfered with a reference light field, the so-called local oscillator (LO), which aids in the phase alignment of the transmitter and receiver and the intensity of which is much higher than that of the quantum signal (the quantum signal in CV-QKD protocols basically contains only a few photons to ensure the non-orthogonality of the quantum states). The receiver still has to assign the measured phase values to a discrete distribution of the M possible phases ("reverse reconciliation"). Finally, the key is generated using error correction and privacy amplification methods. Analogous to DV-QKD protocols, again, attacks on the channel are detected, as measurements change the quantum state.

One advantage of CV-QKD protocols is that they do not require special light sources such as single photons or associated single photon detectors, but use a similar method to phase-coded classical communication, known as phase shift keying, which is used for very high data rates. As both methods are very similar, CV-QKD is easier to integrate with existing classical communication systems and is therefore the preferred variant to DV-QKD, particularly in coherent optical communication methods [27]. In addition to compatibility with existing infrastructure and the associated cost efficiency, CV-QKD protocols also benefit from practicability in the detection process. However, the disadvantages include the more limited range of less than 100 km on average [28] and the more complicated theoretical security analysis [24]. Another disadvantage is the often complex implementation, the need for precise control over the continuous variables of the light and the complex deconvolution and alignment procedures.

4.1.3 Network Architectures

QKD can be used in various topological arrangements to securely exchange keys between two or more parties over different distances. The most common network architectures are outlined below:

- **Point-to-point connection**: The point-to-point connection represents the simplest architecture for tap-proof communication between two parties. The theoretical basis for this is the simple sender-receiver model for communication, which was developed by Claude E. Shannon and Warren Weaver in the 1940s. According to this model, keys are exchanged between a sender and a receiver via a direct communication channel. Point-to-point connections have therefore already been implemented and are widely used. One example are direct connections that bridge a distance of 1000 km via fiber optics.
- **Quantum communication network**: A quantum communication network extends the basic idea of a point-to-point connection to larger, meshed quantum networks with a large number of nodes. Here, not just two, but multiple communication partners can interact with each other via communication channels, which can be arranged in different topologies (e.g., star, ring, tree or mesh structures). These networks therefore offer the advantage of integrating a larger number of participants into the communication, which is particularly advantageous in complex scenarios. Each participant can exchange encrypted messages with every other network participant without unauthorized persons being able to intercept, change, or copy the message unnoticed. Depending on the application scenario, such networks can contain so-called trusted nodes at the intermediate nodes. "Measure and forward" procedures are used at these nodes to ensure point-to-point security. As the key is available at these points as a classical bitstring and is easy to attack, the connection nodes

must be highly secured against unauthorized access. This architecture allows multi-party networks to be set up in urban areas, for example. However, the real advantage of multi-party networks only emerges when using distributed entangled states, which enable special protocols such as secure voting and group decisions.

The choice of network architecture depends on the specific requirements of the respective application, the available resources and the desired level of security. While point-to-point connections may be sufficient in some scenarios (e.g., if there is a direct physical connection between two communication partners and the key exchange is limited to these two), more complex architectures are required for more extensive networks or transmissions over long distances. These must meet correspondingly higher requirements in terms of reliability, scalability, and security. In addition, such network architectures must be able to cope with challenges such as interference, optical attenuation and other environmental influences that could adversely affect quantum information.

Network integration

Point-to-point connections can be implemented in various ways. In addition to conventional fiber optics, there is also the option of implementation via free space links or satellites. For reasons of practicability, there are also hybrid approaches in which QKD is integrated into existing communication networks. In this case, quantum cryptography is used to enable secure key exchange in a higher-level network that also includes conventional communication channels. Here, QKD is used to generate keys at a relatively low rate, which are then handed over to a classical encryption process (often the two symmetric encryption algorithms or block ciphers Data Encryption Standard, DES, or Advanced Encryption Standard, AES) and regularly refreshed. The integration of QKD not only promises increased security and flexibility in different communication scenarios, but also makes it possible to use existing communication networks in a hybrid function without having to set up a new infrastructure.

4.1.4 State of Research and Technology

QKD demonstrations and testbeds

Although comparatively new, QKD that is based on the prepare-and-measure principle has established itself as a market-ready technology for enabling secure communication as of 2024. It is being explored on many testbeds around the world and integrated into existing infrastructures such as fiber optic networks. The transition from research to commercial application has already been successful in some niche markets.

The world's first network for the distribution of quantum keys, which began operating in Massachusetts in 2004, was the DARPA (Defense Advanced Research Projects Agency) QKD network. This operated ten optical nodes and demonstrated the feasibility of QKD in a realistic test environment for the first time [29]. This was followed in 2004 by SECOQC (SEcure COmmunication based on Quantum Cryptograph) in Vienna, the first functional EU-funded QKD network, which comprised six nodes and eight connections and linked six locations in Vienna and the city of St. Pölten, around 70 km to the west, via 200 km of optical fiber [30]. As part of the "Swiss Quantum Initiative (SQI)", a further QKD network was installed in 2009, which was in operation for almost two years. Its aim was to demonstrate the reliability and robustness of QKD in continuous operation in a field environment [31]. Similar developments can also be found in Asia. China presented a hierarchical quantum network in Wuhu in 2009, which consisted of a backbone network with four nodes and a series of subnets [32]. Another network was set up in Tokyo in 2010, enabling the first quantum-secured video conference to be held, which is considered a milestone on the way to tap-proof communication [33]. In the USA, the hub-and-spoke network installed by the Los Alamos National Laboratory

in 2011 was used to test the possibility of quantum-secured internet [34]. In addition, at European level, a video call secured by quantum cryptography was successfully made from Vienna to Beijing for the first time in 2017 using Chinese satellites [24]. A similar event took place in 2021 as part of the "QuNET" project, when the first quantum-secured video conference took place between two federal authorities in Bonn [35].

The Beijing-Shanghai Backbone Network (BSBN), which began operations in August 2017, was the world's first quantum-secure long-range communication link, developed under the leadership of the University of Science and Technology of China (USTC), and is already being used by banks and other financial enterprises for data transmission. The Trusted Node network is located in China and connects the cities of Beijing, Jinan, Hefei, and Shanghai. It consists of more than 700 fiber links and two high-speed free-space links between the Micius quantum communication satellite, which has been orbiting the earth at a distance of approx. 500 km since 2016, and the ground stations that support QKD transmission. The network includes a total of around 2000 km of fiber optic cable linking the four cities and a 2600 km satellite link between two observatories east of Beijing and near the Chinese border with Kazakhstan. The fiber optic links are supported by 32 trusted nodes that relay the quantum information. The nodes of the network each branch out in different directions to the user, creating a comprehensive and secure quantum communication infrastructure [36]. Building on BSBN, China has recently deployed the China Quantum Communication Network (CN-QCN), a carrier-grade, trusted-relay QKD network spanning more than 10,000 km of optical fiber and interconnected with BSBN [37]. CN-QCN comprises 145 backbone fiber nodes (average spacing ~70 km, average link attenuation ~18.6 dB), 20 metropolitan networks and an operations and maintenance center, providing long-range key distribution across 17 provinces and 80 cities. Several backbone nodes are equipped with satellite ground stations linked to the Jinan-1 quantum microsatellite, enabling integrated satellite–fiber QKD. The network uses multiple high-speed decoy-state BB84 systems in the backbone and both DV-QKD and CV-QKD systems in metropolitan networks, and has demonstrated stable long-term operation with end-to-end secure key rates on the order of 10–20 kb/s over multi-hundred-kilometer segments. CN-QCN currently represents the largest operational quantum communication network worldwide.

In the USA, the start-up Quantum Xchange is planning an extensive QKD network along the east coast. The first stage is to connect the metropolis of Manhattan with its neighboring city of New Jersey, where the data centers of many banks are located [38]. Other important examples of existing research networks in this field include the Chicago Quantum Exchange (CQE) and the Brookhaven National Laboratory Quantum Network Facility (BNL): While the six (mainly university) members of the CQE focus on developing new ways of understanding and using the laws of quantum mechanics [39], the BNL is a government experimental facility that provides infrastructure and capabilities to help develop the quantum ecosystem [40]. On the academic side, the NSF Engineering Research Center for Quantum Networks (CQN), which has been based at the University of Arizona since September 2020, is attempting to create the technical and social foundations for quantum networks [41]. In June 2022, Amazon announced the AWS Center for Quantum Networking, an industrial initiative intended to develop new hardware, software, and applications for quantum networks. The initiative was part of Amazon's broader quantum technology efforts at the time [42].

One of major quantum communication centers within the EU is the Dutch "QuTech" initiative. Extensive activities are taking place here, especially on a theoretical level, such as protocol development, layer structures and embedding in existing infrastructure [43]. QuTech also acts as the technical coordinator of the Quantum Internet Alliance (QIA). This alliance brings together 40 leading European academic, industrial and research-oriented technology organizations whose goal is to build the world's first complete prototype of a quantum network. The "London Quantum-Secured

Metro Network" is one example for the hybrid integration of QKD into existing conventional networks. This has three nodes connected by fiber optics and is now also being used commercially [44, 45]. In addition, Toshiba UK and British Telecom implemented the UK's first quantum-secure network in Bristol in 2021. It transmits data and quantum keys between three institutes in Bristol via a 7-km fiber optic cable [46]. Other efforts include the transnational initiatives "Europäische Quantenkommunikationsinfrastruktur (European Quantum Communication, EuroQCI)" and the "PETRUS" coordination project led by Deutsche Telekom. Both of these aim to establish a highly secure EU-wide fiber optic backbone for QKD applications. EuroQCI will deploy a fiber-based terrestrial segment and a satellite-based space segment, which will also be part of IRIS, the EU's space-based secure communications system [47].

QKD performance parameters

A major problem that QKD still faces is its limited range, as the photons used are generally transmitted either via optical fibers or in free space (free-space optical communication, FSO). Long distances are problematic in both cases: There are transmission losses due to the strong absorption of the optical fiber material, while in free-space optical transmission the beam expands. This limits transmission to a few hundred kilometers and is therefore not sufficient for large-scale, secure communication networks. With the aim of keeping absorption as low as possible, transmission usually takes place in wavelength ranges with particularly low absorption, the so-called telecom windows in the infrared region at 1310 or 1550 nm. In contrast, the losses in free space are significantly lower, such that satellite-based communication over several thousand kilometers can be made possible using FSO in near-infrared (approx. 800 to 850 nm) [22].

Direct QKD connections can typically bridge distances of 100 to a maximum of 400 or 500 km. These distances are limited by losses in the optical fibers (usually 1% transmission after 100 km) and the dark noise of the detectors used. Therefore, field-deployed P&M-QKD often relies either on trusted nodes or advanced protocols requiring phase coherence (e.g., TF-QKD variants, see Sec. 4.5.1). The maximum fiber distance that has been achieved to date without quantum repeaters is at the ~1000 km level using Twin-Field QKD and spooled fibers in a lab environment [48]. For field-deployed links, the current distance record for a direct QKD connection without trusted nodes is a 511 km Twin-Field QKD link between two metropolitan areas [49]. In addition to distance, the transmission clock rate also plays an important role in the implementation. The highest key generation rate achieved to date for DV-QKD was 110 Mbps over 10 km of optical fiber [48, 50, 51].

Recent CV-QKD demonstrations have pushed secret-key rates into the hundreds of Mb/s to Gb/s regime at metropolitan distances. For example, a 10-GBaud integrated-receiver system reported SKRs of ~0.7 Gb/s at 5 km and ~0.3 Gb/s at 10 km [52], and multi-carrier CV-QKD experiments in 2025 reported Gbps SKR within 10 km and Mbps SKR at 100 km [53].

Hybrid Integration

QKD is often integrated in a hybrid form by combining it with conventional encryption methods. The reason for this is the rather low key generation rates of QKD—compared to data communication rates—such that the quantum keys are used as an input to conventional encryption methods at a low refresh rate. Implementing QKD and integrating it into existing communication infrastructures generally requires special hardware components such as photon sources with polarization filters, quantum channels and detectors. For example, in the case of the controlled generation of individual photons, complex sources and sensitive detectors are required to detect them. For this reason, there are numerous research efforts aimed at making this hardware more efficient and less expensive in order to further advance the spread of the technology. Examples for the hybrid integration of QKD include the metro network in London mentioned above, as well as the Cambridge

Quantum Network [44, 45]. The latter comprises three nodes that are separated by a 5- to 10-km-long fiber optic line.

QKD research projects

The trials on testbeds and the attempts to integrate the technology into existing infrastructure have sparked numerous national and international research projects aimed at developing systems and components. One of the key players in this field in Germany is the BMFTR-funded "QuNET" initiative. This initiative is investigating implementations of QKD to establish a quantum-secure IT infrastructure and developing innovative technologies for quantum communication, e.g., in fiber and free-space links and the development of single photon sources and detectors. The aim of the project is to implement highly secure communication systems based on quantum technology that are safe from cyberattacks. This is intended to ensure secure communication between authorities and (high) security areas as well as within banking networks and critical infrastructure. In addition, the "QuNET+" projects that are led by industrial partners expand the range of topics covered to include technological aspects of QKD [54].

Cooperation with “QuNET” and many other academic, institutional and industry-led projects is also taking place as part of the “Schirmprojekt Quantenkommunikation Deutschland, SQuaD (Umbrella Project for Quantum Communication in Germany)", which is also funded by the BMFTR. The project focuses on the sustainable transfer of technology from science to industry, on networking with the German quantum communication community, on the implementation of QKD on testbeds, and on its integration into conventional communication infrastructures [55].

There were also individual BMFTR-funded projects carrying out research and development in the field of QKD. These include, e.g., the projects "Integration von QKD in IKT-Netze, Q-net-Q (Integration of QKD into ICT networks)” and "Quantum Physical Layer Service Integration (QuaPhySI)" to integrate QKD into existing information and communication technology systems [56, 57].

The recent "OpenQKD" project funded by the European Commission had a similar focus and aimed to demonstrate the transparent integration of quantum-secure solutions for potential end users and relevant stakeholders on a broad scale. This project was intended to lay the foundation needed to introduce a pan-European quantum-secure digital infrastructure and should strengthen Europe's global position at the forefront of quantum communication capabilities [58].

Another project worth mentioning is "Anwendungsorientierte Demonstration von Quantenkommunikation in Deutschland, DemoQuanDT (Application-oriented demonstration of quantum communication in Germany)”, which focused on the research, development, and demonstration of a secure, cross-network and manufacturer-independent QKD network management system in Germany. As part of this project, a QKD-secured demonstration link was demonstrated on a real-world backbone link between Berlin and Bonn. In November 2024, QKD interoperability and operation were successfully tested over ~923 km using existing Deutsche Telekom fiber and regular operating sites, establishing the largest carrier-grade QKD demonstrator in Germany to date [59].

In addition, the BMFTR-funded "6G-Quantum Security (6G-QuaS)" project targeted the development of a hybrid wired industrial network. Here, the quantum information was stored continuously in the phase and amplitude of the light. This aimed to result in significantly lower latency times and greater resilience to attacks while maintaining the same level of security [60].

The BMFTR-funded project "Entwicklung hochperformanter Übertragungskomponenten für quantensichere Kommunikation über Glasfaserleitungen in Metro- und Weitverkehrsnetzen (Development of high-performance transmission components for quantum-secure communication via fiber optic cables in metro and wide area networks, DE-QOR)” aimed to further develop existing CV-QKD approaches based on coherent optical transmission technology. In this context, the objectives were

to develop core components on the transmitter and receiver side, integrate them into compact systems and target transmission links in urban areas with a length of more than 80 km [61].

Also worth mentioning is the joint project "Quantum Internet of Things (QUIET)", which focused on the development of a communication network and the connection of quantum sensors using distributed quantum states and conventional transmission. This was expected to significantly increase the performance and security of the network [62].

As it is based on quantum mechanical principles, QKD is considered to be highly resilient to side-channel attacks. As a result, it is seen as the foundation for secure communication in the age of quantum computing. This resilience has led to QKD being seen not only as a means to safeguard conventional communications, but also as a key technology for future applications. Ongoing research projects and developments show that it is continuously being improved to meet the challenges of the ever-evolving technology landscape. Its potential extends beyond tap-proof communication and is also used in emerging technology fields such as the Internet of Things (IoT) and secure cloud communication platforms. In this context, QKD has become much more important in recent years and is being intensively promoted in research and industry in order to uphold communications even in an age when the world is shaped by quantum computers.

4.2 Second Generation: Quantum Key Distribution (Photonic Entanglement Sources)

4.2.1 Theoretical Foundations

Entanglement-based QKD, which is based on entangled photons, extends the spectrum of point-to-point connections in which the exchange of information takes place directly between a transmitter and a receiver. Unlike the prepare-and-measure method described in 4.1.1, which is based on the preparation, transmission and measurement of individual particles and needs a trustworthy source or detectors, this approach assumes a high degree of correlation between entangled particles. As a result, this protocol does not require trustworthy sources or detectors. It is based on the principle of quantum entanglement. This refers to a special form of linking between two or more quantum mechanical particles, regardless of the spatial distance between them. The common properties of all particles together are fixed, but the states of the individual qubits are undetermined. These are only clearly determined when measured. By measuring the state of one qubit, however, the state of the others is also known without having to measure them directly. Any interference or interception of the transmitted information leads to an unavoidable change of state in one of the qubits. As the particles are entangled, this change is immediately registered in the correlated qubit, meaning the interference or side-channel attack can be detected.

How the protocol functions (according to the basic principles of the protocols described by Artur Ekert 1991, E91 [63], and Charles H. Bennett, Gilles Brassard and N. David Mermin 1992, BBM92, [64]) can be outlined as follows: The central resource is a source of entangled quantum mechanical particles, e.g., photons. In the first step, a pair of entangled photons is split between the two communication partners. Similar to the BB84 protocol, the two partners each measure their photon in a randomly selected base. For E91, the difference to the BB84 protocol is that not only two nonorthogonal bases are selected here, but three. Depending on the combination of the chosen measurement bases, the communication partners can generate a common key bit or prove that the measured photons are actually entangled. The increased security of this technology is therefore guaranteed by entanglement detection, which can be used to prove that the particles faithfully originate from the entanglement source and have not been modified. In practice, various methods are used for the entanglement test. For example, in addition to the Bell test proposed by

John Steward Bell in 1964, the CHSH inequality developed by John Clauser, Michael Horne, Abner Shimony and Richard Holt in 1969 is also used. Entanglement-based QKD can be advantageous in special application scenarios, especially those that require communication between several participants (multi-party QKD). It ensures secure transmissions over long distances and could therefore also play a role in complex networks or applications such as the IoT. Although this technology is being widely explored on testbeds, it is not yet as mature as the previous generation.

4.2.2 Encoding Variants

DV encoding

The implementation of entanglement-based DV-QKD protocols requires entangled photon pair sources, for which parametric fluorescence (Spontaneous Parametric Down-Conversion, SPDC) is often used. In this physical process, a high-energy (e.g., ultraviolet) photon is converted in a non-linear crystal into two entangled low-energy (e.g., infrared) photons, the so-called signal and idler photons. The entanglement usually exists in the degree of freedom of polarization (e.g., one photon is horizontally polarized, the other vertically, whereby it is undetermined which photon has which polarization until measured). These two photons leave the crystal at different angles, making spatial separation possible. In this way, parametric fluorescence can be used to generate entangled, spatially separated photon pairs and distribute them to the communication partners such that they can be used for the implementation of DV-QKD protocols. A more complex way to generate entangled photons is to use semiconductor quantum dots, i.e., artificial atoms made of semiconductor materials. Here, a radiative cascade (almost simultaneous emission of two photons from successive optical transitions) is used to generate photons that are usually polarization-entangled. The high technical complexity (operation at cryogenic temperatures) is offset by deterministic emission at a high rate with high purity of the generated entangled state [65].

CV encoding

Currently, most CV-QKD implementations are based on a one-way method where, as described in section 4.1.2, the quantum keys are generated using continuous parameters such as the amplitude and phase of light pulses sent from transmitter to receiver. Placing an entanglement source in the middle between two users offers an alternative option for secure communication with efficient use of quantum resources, similar to the E91 protocol with discrete variables. Here, the entanglement source produces states whose entanglement is encoded in continuously distributed variables (Einstein-Podolsky-Rosen or EPR states), e.g., "squeezed states", in which the quantum mechanical uncertainty of a variable (e.g., phase) is reduced below the limit of Heisenberg's uncertainty principle (at the expense of the fluctuations of the complementary variable, e.g., amplitude). The two communication partners then use homodyne measurements, like the first-generation of CV-QKD, to randomly measure the amplitude or phase of the states. Here, the comparison of the measurement bases and the post-processing procedures of the CV-QKD also lead to key generation and verification of the entanglement properties. Entanglement-based CV-QKD methods have been theoretically proposed for about ten years [66], but have so far only been implemented in a few demonstration experiments [67].

4.2.3 Network Architectures

Like the previous generation, entanglement-based QKD also offers point-to-point quantum security. The main difference between the two technologies is that second-generation QKD does not require a trusted source or detector due to the possibility of entanglement verification. Since the security of quantum key exchange is guaranteed by the intrinsic nature of quantum entanglement

and there is a high degree of correlation between states of the individual particles, no prior state preparation is required to ensure efficient key generation.

In the field of entanglement-based QKD, multi-party quantum encryption is of great interest, in which entangled photon pairs are generated by the service provider and distributed to several users at different locations [68, 69]. This can be implemented technically using a spectrally broadband source of photon pairs, which are divided into different frequency channels using wavelength demultiplexing [70]. In such multi-party networks with multipartite entanglement distribution, more extensive protocols are possible than is the case with point-to-point connections: When communicating with multiple users, it is often desirable for all participants to share a single secret key such that each member can decrypt messages sent by another member of the group. The process by which the users of such a network share a key is called a conference key agreement. This type of key distribution can provide strong encryption for multiple users, e.g., for video conferences. Sharing information among multiple users in such networks also enables quantum secret sharing (QSS). QSS can protect secret messages from eavesdroppers and dishonest players and has important applications in areas such as key management, identity authentication, remote partner coordination, and so-called "quantum auctions".

4.2.4 State of Research and Technology

QKD demonstrations and testbeds

As described above, QKD is now considered a market-ready technology and is being explored on numerous testbeds and integrated into existing communication infrastructures. Although entanglement-based QKD is not yet as mature as the previous generation, experimental studies have already been carried out. These have demonstrated entanglement-based communication via fiber links and up to satellite links of more than 1100 km [71]. While SPDC-based probabilistic sources still dominate most entanglement-based demonstrations, semiconductor quantum dot sources have progressed rapidly and are increasingly engineered for telecom-band quantum networking [72]. However, their use in field-deployed entanglement-based QKD is vastly reported at shorter distance [73, 74].

An implementation of the BBM92 protocol was tested recently over a regional link using the deployed optical fiber Niedersachen Quantum Link between Braunschweig and Hannover, with a special focus on fiber noise and metrological aspects [75]. Furthermore, a collaboration between the telecommunications operator Deutsche Telekom and the quantum networking company Qunnect demonstrated metropolitan-scale entanglement distribution over deployed fiber infrastructure in Berlin under realistic operating conditions, including the co-propagation of classical data traffic [76].

In context of the second QKD generation, the "Quantum Communications Hub" in the UK (Phase 2 of the national programme, 2019–2024) developed secure quantum communication over all distance scales and to integrate QKD into existing networks for secure communication. The hub's fiber link extended from Bristol via London to Cambridge/Ipswich and has metro networks at the endpoints. Among other goals, the project investigated entanglement distribution to a large number of users, architectures for the physical and higher layers and the integration of quantum communication with conventional data traffic [77].

QKD performance parameters

Currently, entanglement-based QKD via optical fibers has been demonstrated from deployed links up to 248 km [78], and in laboratory/ULLF spools to beyond 300 km, with proof-of-principle secure-

key generation reported at 201 km, 301 km, and 404 km distance (however, very low rates at the longest distance) [79].

Despite the limited range of individual links, a communication network of trusted nodes can be created by concatenating several short segments. As mentioned above, in addition to range, the clock rate also plays a major role in the implementation. Key rate have improved substantially over the past years. A recent demonstration achieved 440 secure key bits per second over 201 km [79].

QKD research projects

Several national and international research projects emerged that built on the advances described above. For example, the projects "IT-Sicherheit durch verschränkungsbasierten Quantenschlüsselaustausch (Quantum-based Security Promise, Q-Sec-Pro)" and, to some extent, "Integration von QKD in IKT-Netze (Q-net-Q)" aimed to ensure a new level of security, particularly for critical infrastructures, through developments in the field of quantum cryptography based on a source of entangled photon pairs in the wavelength range used for telecommunication. To realize this, the objective was to investigate and implement a QKD protocol and suitable hardware and software. This was expected to make an important contribution to the development of a German quantum communication industry and to strengthen Germany's technological sovereignty [80]. Similar efforts were made in the BMFTR-funded "Q-Fiber" project that aimed to demonstrate entanglement-based QKD with four communication participants, with potential future applications in the medical sector. In this context, e.g., sensitive health data could be encrypted and exchanged using entangled light quanta. The aim was to implement and research novel light conducting cables for the transmission and low-cost detection of light quanta within existing IT infrastructure [81].

A current research focus is on Device-Independent Quantum Key Distribution (DI-QKD). This is also based on quantum mechanical principles, but was developed with the aim of guaranteeing the security of the key exchange regardless of the exact implementation of the quantum devices. Conventional quantum key exchange protocols, such as the BB84 protocol, rely on the quantum devices used fulfilling certain properties and that the measurement results can be reliably attributed to quantum entanglement and measurements. DI-QKD, on the other hand, attempts to dispense with these assumptions and guarantee the security of the protocol even if the devices could be manipulated by an attacker. The basic idea is to design the key exchange in such a way that it is robust against general quantum attacks, even if the attacker knows the exact nature of the quantum devices used or influences them. Currently, there are various approaches and protocols in the field of DI-QKD. Some of these approaches rely on the nonlocal correlation of quantum-entangled states and the loophole-free violation of a Bell inequality to rule out possible interference and tampering. Although DI-QKD is challenging in practice, recent theoretical and experimental efforts have led to proof-of-principle DI-QKD implementations [82]. The technological basis for these protocols is the distribution of entanglement (in the form of photon pairs or entangled quantum memories) with high quality and near-perfect quantum measurements—this is very difficult to achieve in practice. Initial demonstration applications in laboratory environments show DI-QKD with entangled photon pairs in the telecom wavelength range over a fiber distance of 220 m [83]. Another option is the generation of entangled states of stationary quantum memories that are spatially separated (see also section on third generation and entanglement distribution). Here, initial experiments used trapped strontium ions [84] and rubidium atoms [85] that were spatially separated by 2 m and 440 m. The key generation rates in all these experiments are currently still far too low for technologically relevant applications and are essentially limited by the detection efficiencies of single-photon detectors and insufficient repetition rates. On the other hand, the DI-QKD approach guarantees the highest possible level of security of the QKD methods.

Motivated by similar concerns regarding device imperfections, Measurement-Device-Independent QKD (MDI-QKD) removes all trust assumptions on the measurement devices and thereby closes the most relevant practical side-channel attacks. An important extension of this concept is Twin-Field QKD, which is based on the MDI-QKD security model and enables secure key distribution beyond the fundamental rate-distance limit of point-to-point QKD. This approach is discussed in more detail in a later section.

4.3 Third Generation: Quantum Repeater (Entanglement Distribution)

4.3.1 Theoretical Foundations

As already mentioned, a current major challenge for QKD is to achieve the longest possible transmission distance. While the transmission of information over shorter distances is generally not a problem, it is much more difficult over longer distances of several hundred kilometers. Over such distances, optical signals such as single or entangled photons or weak laser pulses of the first and second generation QKD are greatly diminished due to losses and attenuation of the optical fibers. If the losses become too high, it is no longer possible to distinguish between an eavesdropping attack and the technical attenuation of the channel and the security of the key exchange is compromised. The achievable key rate also drops massively. One option, which has already been mentioned, is the serial concatenation of individual short segments in so-called trusted node networks. These networks have the disadvantages that the information is available as classical information at each intermediate node, is thus easier to attack and end-to-end quantum mechanical security cannot be guaranteed. In order to eliminate the problem of information loss and to enable transmission over longer distances, research is focusing on the development of quantum repeaters.

Quantum repeaters were first introduced in 1998 by Hans Briegel et al. [86], and have been regarded as a pioneering technological building block ever since. The term *quantum repeater* is slightly misleading and can result in misunderstandings. In contrast to the widely known repeaters (repeating amplifiers) in communication links, the incoming signals are not measured and retransmitted or amplified. As is known from the measurement problem in quantum mechanics, this would lead to undesirable errors. Instead, quantum repeaters divide a longer transmission link along a communication channel into shorter sections, within which entanglement is distributed with only minor losses, without quantum states being measured or copied. Distribution of entanglement is achieved by sending entangled photon pairs or by entanglement swapping (see below). At the ends of these segments, the received or generated entangled states are stored using quantum memories. By storing the quantum information, the entanglement distribution does not have to be synchronous for all segments, which offers a decisive advantage if the protocol has a finite probability of success. The second decisive component of quantum repeaters is the principle of entanglement swapping. This allows two sections of the transmission path to be linked together, which successively increases the range of quantum entanglement in communication networks. To explain this principle, consider a simple chain of nodes A - B - C - D. In a first step, nodes A and B each generate a local entanglement between a quantum memory and a photon (e.g., through special protocols that exploit selection rules in the emission of photons). The two photons from A and B are sent to a measurement station between A and B, where a measurement of their common properties ("Bell state measurement") is performed. The state of the individual particles remains unknown. Given a specific outcome, this measurement ensures that the quantum memories at A and B are projected into an entangled state (among all possible options for the common state of the quantum memories, the entangled state is selected by the measurement outcome). This distributes entanglement over the segment A - B; the nodes C - D can proceed analogously. In a further entanglement swapping, a

Bell measurement can now be carried out on quantum memories B and C. Again, if a selected measurement result occurs, the quantum memories A and D become entangled. In this way, entanglement has now been created between the ends of the chain. For larger distances and several segments, this process is repeated until the ends of the entire chain are entangled.

Eventually, the distributed entangled states can be used as a resource: on the one hand for entanglement-based QKD, in which the principle of key generation is identical to the second-generation schemes introduced above. The difference between the second and third QKD generation is that quantum repeaters can bridge greater distances without having to rely on trusted nodes. However, the real advantage of quantum repeaters is the option of using the distributed entanglement resource to transmit quantum states without destroying them. Quantum teleportation is used for this, in which the quantum state to be transported is measured together with one part of the entangled state (Bell measurement) and, based on the result, a specific operation on the second part of the entangled state restores the original initial state. By distributing entangled states over long distances using quantum repeaters, teleportation can also be carried out over long distances. The distribution of quantum states also makes distributed quantum computing possible. This involves using quantum links to connect several quantum computers at different physical locations with the aim of increasing computing power and jointly solving complex tasks. In this way, quantum computers can also be integrated with conventional systems, which also offers more application options and greater flexibility. The advantage of distributed quantum computing stems from an exponential increase in the available computing space and performance which enables complex problems to be solved at previously unattainable speeds. The possibility of connecting several quantum computers with each other is an enormously important step for future quantum networks.

In the context of quantum communication in a hyperconnected world, the entanglement resources generated by quantum repeaters not only ensure increased IT security through end-to-end encryption protected by quantum mechanical principles, but can also be used in entanglement-assisted classical communication and increase the security and resilience of communication networks. The advantages of entanglement-assisted encoding are lower latency times, higher transmission capacity and greater resilience as well as the prevention of DoS (denial of service) attacks. This shows that quantum repeaters can make an important contribution to research on 6G networks, as stated in the BMFTR's 2021 research program for "Kommunikationssysteme: Souverän. Digital. Vernetzt (Communication Systems: Sovereign. Digital. Connected.)" [87]. The different application prospects opened up by quantum repeaters are highly relevant for society in the context of IT security and the protection of critical infrastructures. However, their development and widespread implementation are extremely complex. Although there is still no serious commercial market and no direct economic competition at present, it can be assumed that both will be strongly promoted in the coming years. This is because quantum repeaters are a necessary prerequisite for the construction of long-range quantum communication networks that cover distances of several hundred kilometers and therefore offer enormous benefits for the communication systems of the future.

4.3.2 Encoding Variants

Similar to the DV protocols of the first and second QKD generation, quantum repeaters are also predominantly based on discrete variables, i.e., DV-QKD protocols in which information is encoded in discrete states of individual or entangled quantum systems and projective measurements are made. CV-QKD protocols, which are attractive because they are technically related to current classical communication systems, have not yet been used in the realization of quantum repeaters. CV concepts are hardly considered even in theoretical studies that currently far outweigh experimental studies and dominate the research field of quantum repeaters [88–90]. The reasons for this are the complexity of the required operations, the error correction for CV states, and the lack of quantum

memories. CV systems require advanced error correction techniques to protect the transmitted quantum states from noise and losses in the transmission channels and to maintain entanglement. While quantum error correction is well established for DV systems, expanding this technique to CV is still an active field of research. The implementation of quantum memories for CV systems that can efficiently store and recover states with continuous variables remains a technical challenge.

4.3.3 Network Architectures

Quantum repeater networks form the basis of this technology. Their aim is to increase the transmission range of quantum information using repeater stations. The stations are placed at regular intervals along the transmission path. They generate entanglement locally, store it using quantum memories and pass it on to the next station via entanglement swapping. This entanglement swapping is used to link the ends of the individual sections so that, eventually, entangled quantum states are available between the endpoints of the transmission path. Quantum repeaters offer security in communication links across multiple nodes and long distances through end-to-end entanglement. They also enable the secure connection of quantum computers in quantum networks. As is the case with QKD, the implementation of quantum repeaters focuses primarily on the characteristics of distance and key rate. As this technology is still under development, there are currently no meaningful figures available for distances or key rates.

4.3.4 State of Research and Technology

QKD demonstrations and testbeds

Quantum repeaters are considered to be the fundamental cornerstone for secure communications and the distribution of quantum states in future quantum networks. Their fields of application in secure communication are in principle identical to those of QKD, however, with the difference that quantum repeaters can theoretically bridge greater distances without having to rely on chains of trusted nodes. This is why they can make an important contribution to implementing the strategic goals of IT security research within the BMFTR-funded program "Digital. Sicher. Souverän. (Digital. Secure. Sovereign.)" and ensure technological sovereignty in tap-proof communication over long distances. Against this background, the "Quantenrepeater.Link (QR.X)" project aimed to explore the distribution and storage of entanglement as a resource for quantum communication and quantum networks. For this purpose, optimized components and modularized devices were developed, fiber testbeds outside the laboratory environment were deployed, and an elementary quantum repeater link was demonstrated under realistic field conditions [91]. Building on the results of QR.X, the research network "Quantenrepeater.Net (QR.N)", established in January 2025, now addresses further developments in the field of quantum repeaters [92].

Although the transition from research to commercial application of QKD has already been successful in some niche markets, its widespread availability for society is still a long way off. There is still a high demand for research on implementing the quantum physical principles in practical, field-deployable applications. Despite innovative approaches (e.g., Twin-Field QKD), it is only possible to cover fiber-based distances of more than 1000 km using chains of trusted nodes, whose end-to-end security is limited due to the necessary conversion of quantum information into classical information at each node. Quantum repeaters are necessary for realizing quantum-secured communication in networks beyond point-to-point connections.

QKD performance parameters

Research has made significant progress in recent years with demonstrations of basic elements of quantum repeaters. However, the major technological challenges involved limit repeater-grade demonstrations to short distances and a small number of nodes. For example, it was possible to demonstrate the distribution of entanglement between two quantum memories via optical fiber links over distances between approx. 500 m and 35 km [93–97]. A notable 2024 milestone is the demonstration of a two-node network of nanophotonic diamond quantum memories with bidirectional quantum frequency conversion to telecom wavelengths, achieving memory–memory entanglement through 40 km fiber spools and a 35 km deployed urban fiber loop, together with second-long entanglement storage and integrated error detection, representing a decisive step toward practical repeaters. In addition, the distribution of qubit-telecom-photon entanglement over longer fiber distances has been demonstrated, including a distance of 101 km via fiber coil (rubidium atom quantum memory) and 50 km over deployed fiber in a metropolitan area (rare earth-based quantum memory) [98, 99]. The teleportation of quantum mechanical states over longer fiber distances between photons (approx. 64 km) as well as between quantum memories and photons (approx. 5 km) and ions (approx. 14 km) was also successfully carried out [100–102]. More recent field-oriented demonstrations include teleportation that coexists with high-capacity classical data traffic in the same fiber, addressing a key systems-integration requirement [103].

As part of the "QR.X" project, a quantum repeater cell was successfully demonstrated as the central element of a quantum repeater for photonic entanglement distribution as well as quantum gate operations on two quantum memories [104, 105]. Also in QR.X quantum teleportation over an urban 14.4 km dark-fiber link was demonstrated [102]. Looking at more complex quantum network demonstrations consisting of three nodes a landmark implementation using NV centers in diamond, showed entanglement distribution between the outer nodes and entanglement swapping via the middle node. Furthermore, teleportation of a quantum state between the outer nodes was performed [106]. Building on this work, a 2024 experiment reported further advances in NV-center-based quantum networking, including enhanced multi-node teleportation capabilities in a diamond quantum network [107]. More recently, a metropolitan multi-node quantum-memory network has been demonstrated, distributing entanglement between three memory nodes in the city of Hefei, China [108]. In the field of modeling of quantum repeaters, the "QR.X" consortium has developed analytical models and simulations of quantum repeater links that use realistic parameters of existing hardware components [109–111]. Similar research directions are also pursued internationally, e.g. in a study of TU Delft based on modular simulation environments that models a prospective quantum repeater along the DemoQuanDT route between Berlin and Bonn [111, 112]. The use of new entanglement-assisted protocols for classical communication can improve communication performance and prevent attacks on IT infrastructures [113]. Please refer to Azuma et al. [114] for a comprehensive overview of current theoretical concepts and experimental progress.

QKD research projects

Despite the steady progress made, developing quantum repeaters and future end-to-end quantum networks is an enormous technical challenge. For example, quantum states must be generated, buffered, and transmitted with high quality, and gate operations between the states are required for error correction and fidelity improvement. Furthermore, not only is research into system components required, but also the development of adapted protocols. Eventually, as the level of development of quantum repeaters increases, prospective application and examples need to be considered in collaboration with industry.

As part of the "Quantenrepeater.Link (QR.X)" research network, important elements of a quantum repeater have already been demonstrated on fiber links. These included qubit-photon entanglement over long distances [99] and the generation of entanglement between spatially separated qubits [95]. Building on the findings of QR.X, the research network Quantenrepeater.Net (QR.N) is now pursuing further advances in quantum repeaters, which enable secure long-distance transmission of information and are essential for future quantum-secured IT infrastructures. A central goal of QR.N is to demonstrate quantum repeater functionalities in real-world testbeds, including multi-node repeater chains and parallel quantum channels using multiplexing technologies [92]. Research activities on quantum communication are currently being strongly promoted in an international context as well. One example of this is the US "National Quantum Initiative", which has set the goal of accelerating quantum research and development to boost the economic and national security of the USA [115]. In addition, a number of research networks already exist. In academia, the "Chicago Quantum Exchange" [39], the "Brookhaven National Laboratory Quantum Network Facility (BNL)" [40] and the Center for Quantum Networks [41] should be mentioned here. In industry, cloud and hardware providers support quantum networking research and companies such as IonQ are strengthening their capabilities in quantum communications through strategic acquisitions like ID Quantique and Lightsynq, which specializes in quantum communication and related technologies. The potential of quantum technologies has also long been recognized in Asia and is being promoted, e.g., by the Japanese "Moonshot Research and Development Program" [116], which supports a research network on quantum repeaters. With the launch of the Beijing-Shanghai Backbone Network (BSBN), China is also expanding its support for quantum communication with the aim of researching a global quantum network. In Europe, the research on quantum networks is strongly driven by the Quantum Internet Alliance (QIA), which aims to demonstrate a prototype quantum internet integrating all network levels [117].

These global efforts underscore that quantum repeaters are a major worldwide research focus and rapid progress has been made on essential building blocks including spin-photon interfaces and multi-qubit node operations [96, 108, 118]. As quantum repeaters are essentially "small quantum computers with an optical interface", the technical complexity is extraordinary. However, because this method is the only way to distribute quantum states in a network, its benefits are enormous.

4.4 Survey on Trend Analysis in Quantum Communication

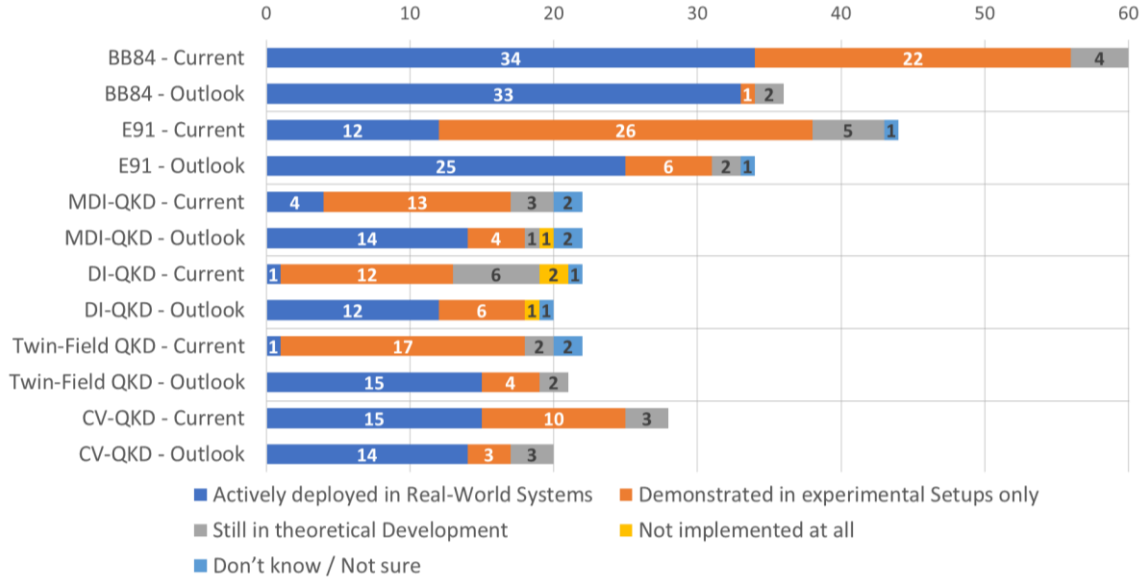
Between June 4 and July 16, 2025, we conducted an online survey on quantum communication to identify current trends and gather insights from the research and industry community. We also asked the participants to highlight key research areas that should receive particular attention in the present revision of this monitoring report. Methods including the survey design and overview over participants are presented in section 2.

In the following sections, we analyze the responses to the survey questions. Rather than discussing each question individually, thematically related questions are grouped together and examined jointly. Graphical representations of all questions and corresponding responses are provided in Appendix A. The part of the survey that asked major challenges regarding widespread implementation of quantum communication is analyzed in section 6.3.

4.4.1 Assessment of Quantum Communication Protocols

To better understand participants' perspectives on key quantum communication protocols – including BB84, E91, MDI-QKD, DI-QKD, Twin-Field QKD, and CV-QKD – the survey asked about their familiarity with each protocol, perceived readiness for real-world implementation, and expectations for future deployment. Figure 1 provides an overview of the results for all quantum communication protocols.

Figure 1: Assessment of the development and deployment of the quantum communication protocols over the next ten years



Source: Survey by UDS/Fh ISI

The following section summarizes the assessments for each protocol.

BB84

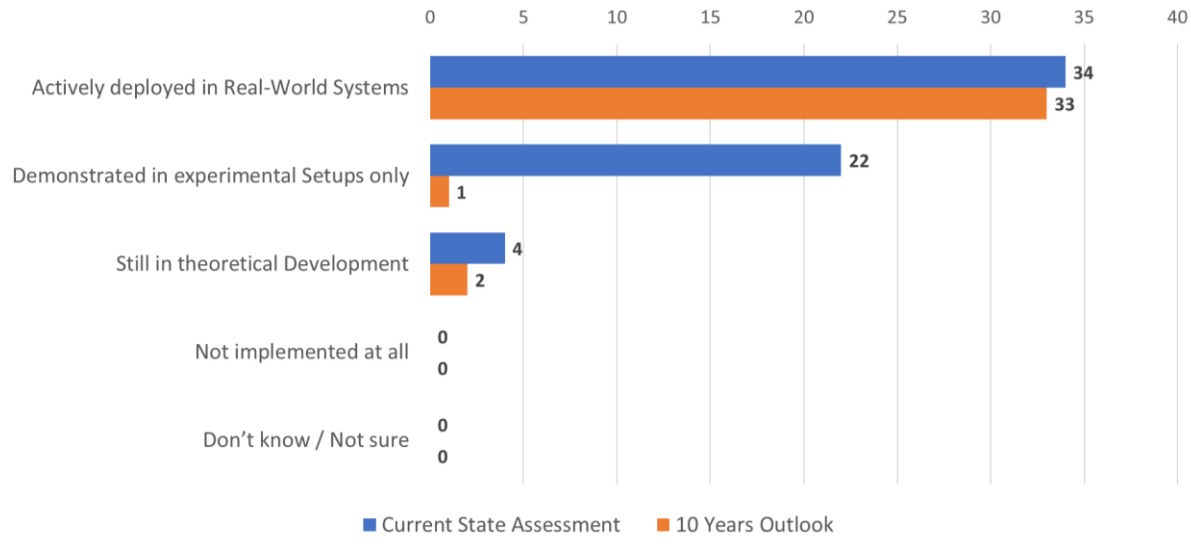
Developed by Charles Bennett and Gilles Brassard in 1984, BB84 is considered the foundational quantum key Distribution (QKD) protocol and serves as a benchmark for subsequent schemes.

Out of 61 respondents, 53 reported a good or expert understanding of BB84, six had a rough idea of how the protocol works, and only two were unfamiliar with its details – making it the most widely recognized protocol in the survey.

Many respondents perceive BB84 as already being actively deployed in real-world systems. Specifically, 34 respondents stated that BB84 is currently in active use, while 33 expect it to remain so over the next ten years. In contrast, 22 participants view it as primarily demonstrated in experimental setups today, with just one respondent expecting this status to persist over the next decade. Only a small minority – four participants today and two in the future – see BB84 as still in theoretical development. These values are shown in Figure 2.

The findings highlight that BB84 remains the reference point for practical quantum communication, combining conceptual clarity with high confidence in its continued deployment.

Figure 2: Current state assessment and implementation outlook on the development and deployment of BB84 over the next ten years



Source: Survey by UDS/Fh ISI

E91

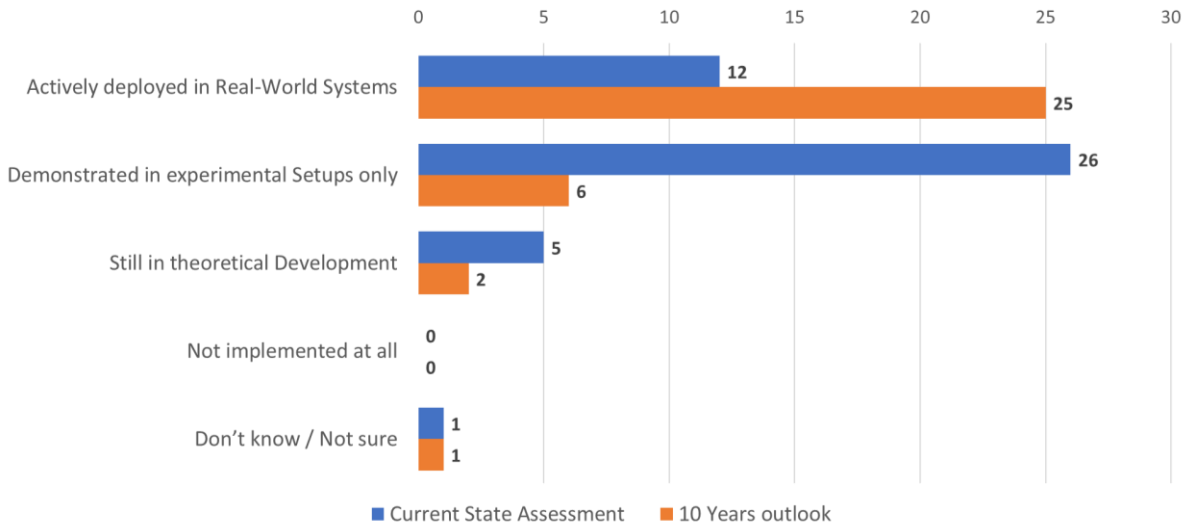
Introduced by Artur Ekert in 1991, E91 uses entanglement and Bell's theorem to ensure security, offering a conceptually distinct approach from BB84.

Among respondents, 39 reported a good or expert understanding of the protocol, twelve a rough idea, and ten limited or no familiarity.

Deployment is perceived as less advanced but shows strong growth expectations. While only twelve participants consider E91 to be actively deployed in real-world systems today, 25 expect it to reach that stage within the next ten years. 26 respondents currently see it as demonstrated in experimental setups only, with just six expecting this status to persist into the next decade. A small number of participants view the protocol as still theoretical – five today and two in the future.

E91 is thus viewed as emerging, with confidence in its future driven by its entanglement-based and potentially device-independent security model. Figure 3 summarizes these values.

Figure 3: Current state assessment and implementation outlook on the development and deployment of E91 over the next ten years



Source: Survey by UDS/Fh ISI

MDI-QKD

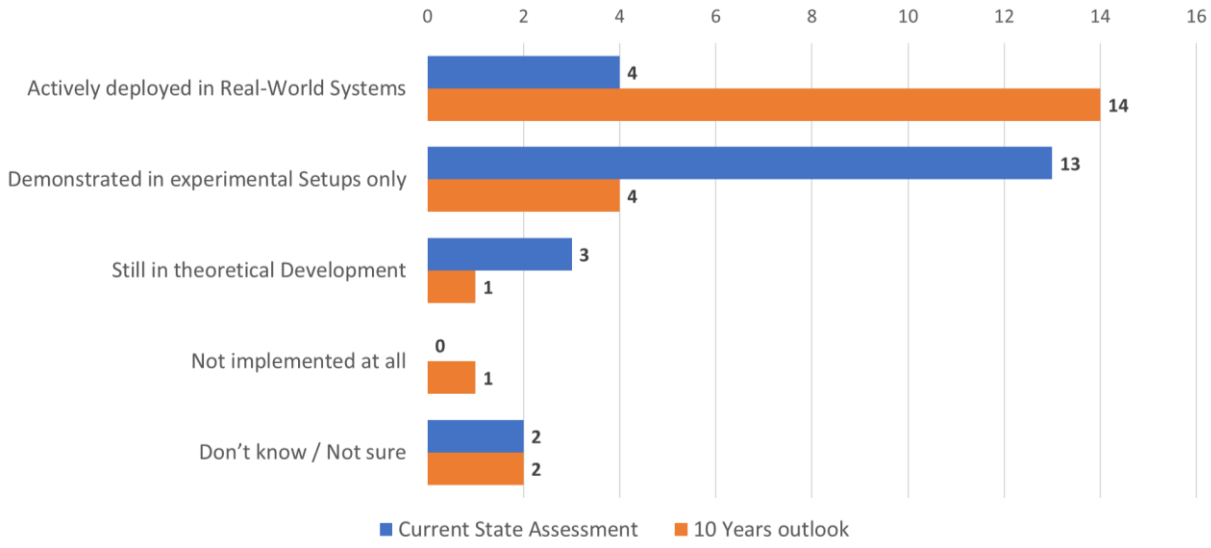
Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) mitigates vulnerabilities in imperfect detectors by ensuring security even with untrusted measurement devices.

Among respondents, 23 reported good or expert understanding of the MDI-QKD protocol, 25 a rough idea, and the remaining twelve participants indicated that they have a limited understanding.

The reported deployment outlook for MDI-QKD reflects its status as a relatively recent and limited protocol. Only four participants consider it to be actively deployed in real-world systems today, while 14 expect it to reach that stage within ten years. Currently, 13 respondents view MDI-QKD as demonstrated only in experimental setups, with four expecting this status to persist into the next decade. A small number of participants – three today and one in the future – view the protocol as still in theoretical development. In addition, one respondent indicated that MDI-QKD is neither implemented today nor expected to be implemented in the next ten years.

These results suggest that most respondents classify MDI-QKD as experimentally demonstrated rather than fully implemented, but there seems to be growing recognition of MDI-QKD's potential, especially for improving practical system security. An overview of the values is given in Figure 4.

Figure 4: Current state assessment and implementation outlook on the development and deployment of MDI-QKD over the next ten years



Source: Survey by UDS/Fh ISI

DI-QKD

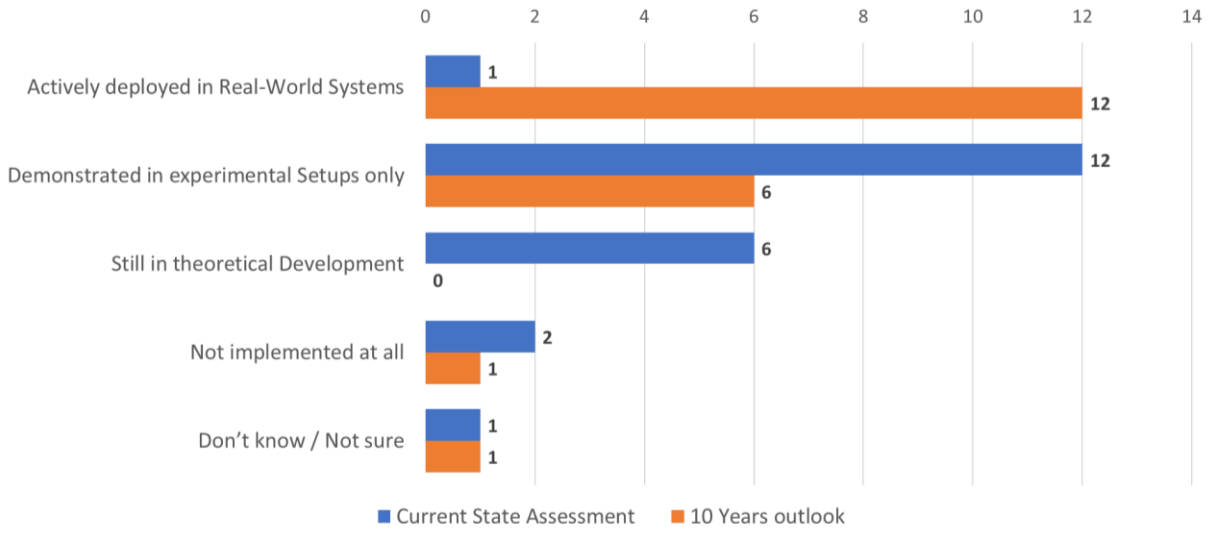
Device-Independent Quantum Key Distribution (DI-QKD) removes trust assumptions about the devices themselves, ensuring security based solely on Bell inequality violations.

In the survey, a total of 21 respondents reported good or expert understanding, 22 a rough idea of how the protocol works, and 17 limited or no familiarity.

The reported deployment outlook for DI-QKD reflects its status as a theoretically robust but technically challenging protocol. Only one participant sees DI-QKD as actively deployed today, while twelve expect that within ten years. Twelve respondents view DI-QKD as demonstrated in experimental setups only, with six expecting this status to persist into the next decade. Six participants view the protocol as still in theoretical development today, while two consider it not implemented at all. One respondent expects this lack of implementation to continue over the next ten years.

The results suggest that DI-QKD is still in the early stages of practical realization, suggesting cautious optimism about long-term applicability. Figure 5 illustrates these values.

Figure 5: Current state assessment and implementation outlook on the development and deployment of DI-QKD over the next ten years



Source: Survey by UDS/Fh ISI

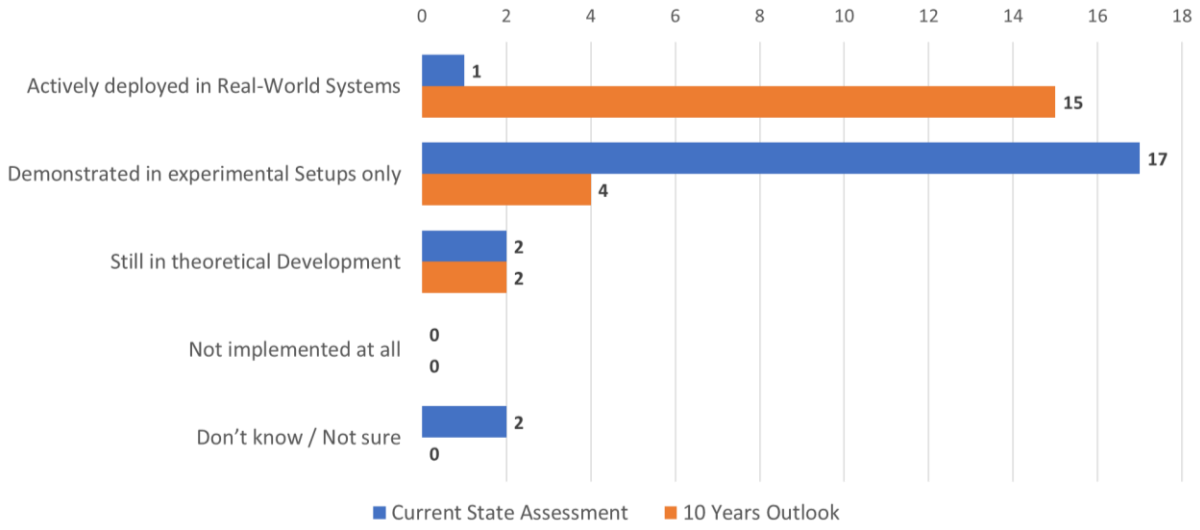
Twin-Field QKD

Twin-Field Quantum Key Distribution (TF-QKD) is a newer protocol designed to overcome the rate-distance limit of conventional QKD, enabling long-distance secure communication without quantum repeaters.

Among respondents, 22 reported good or expert understanding of the TF-QKD protocol. Another 19 respondents indicated that they have a rough idea of how the protocol works. Eleven participants stated that they had heard of TF-QKD but were not familiar with its details, while eight respondents had never encountered the protocol before.

The reported deployment outlook for TF-QKD reflects its status as a promising but still emerging protocol. Only one participant considers TF-QKD to be actively deployed today, while 15 expect it to reach that stage within ten years. 17 respondents view TF-QKD as demonstrated in experimental setups, with four expecting this status to persist into the next decade. Two participants believe the protocol remains in theoretical development today, and two expect this to continue over the next ten years. Although still emerging, TF-QKD enjoys increasing recognition for its potential to extend secure key distribution over long distances. These values are presented in Figure 6.

Figure 6: Current state assessment and implementation outlook on the development and deployment of Twin-Field QKD over the next ten years



Source: Survey by UDS/Fh ISI

CV-QKD

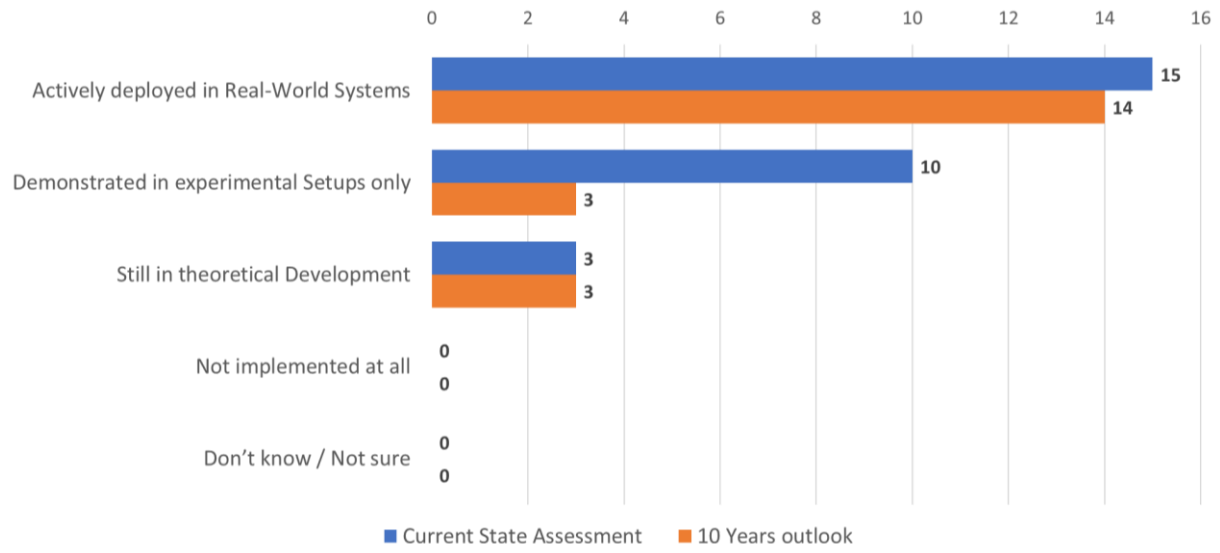
Continuous-Variable Quantum Key Distribution (CV-QKD) encodes quantum information in the quadratures of the electromagnetic field, allowing use of standard telecom components and straightforward integration into existing infrastructure.

Of the respondents, 25 reported a good or expert understanding of the CV-QKD protocol, 19 a rough idea of how it works, and 16 limited familiarity.

The deployment outlook for CV-QKD reflects its relatively advanced stage of development and practical relevance. 15 participants consider CV-QKD to be actively deployed in real-world systems today, while 14 expect it to reach that stage within ten years. Ten respondents view the protocol as demonstrated only in experimental setups, with an equal number expecting this status to persist into the next decade. Three participants believe the protocol remains in theoretical development today, and another three expect this to continue over the next ten years.

These results suggest that CV-QKD is among the more mature quantum communication protocols, with a solid foundation for future deployment and integration into existing infrastructure. An overview of the values is given in Figure 7.

Figure 7: Current state assessment and implementation outlook on the development and deployment of CV-QKD over the next ten years



Source: Survey by UDS/Fh ISI

Summary and Outlook for Quantum Communication Protocols

The survey results reveal a diverse yet coherent landscape of familiarity and expectations regarding current quantum communication protocols. BB84 remains the most widely recognized and mature protocol, serving as a benchmark for other schemes and maintaining strong confidence in its continued deployment. E91 and CV-QKD are also widely known among the participants, and there is growing optimism about their future implementation, driven by their entanglement-based and telecom-compatible characteristics, respectively. MDI-QKD and DI-QKD are perceived as more technically demanding and less mature, but both are considered promising candidates for enhancing system security by mitigating device-related vulnerabilities. Twin-Field QKD, although relatively

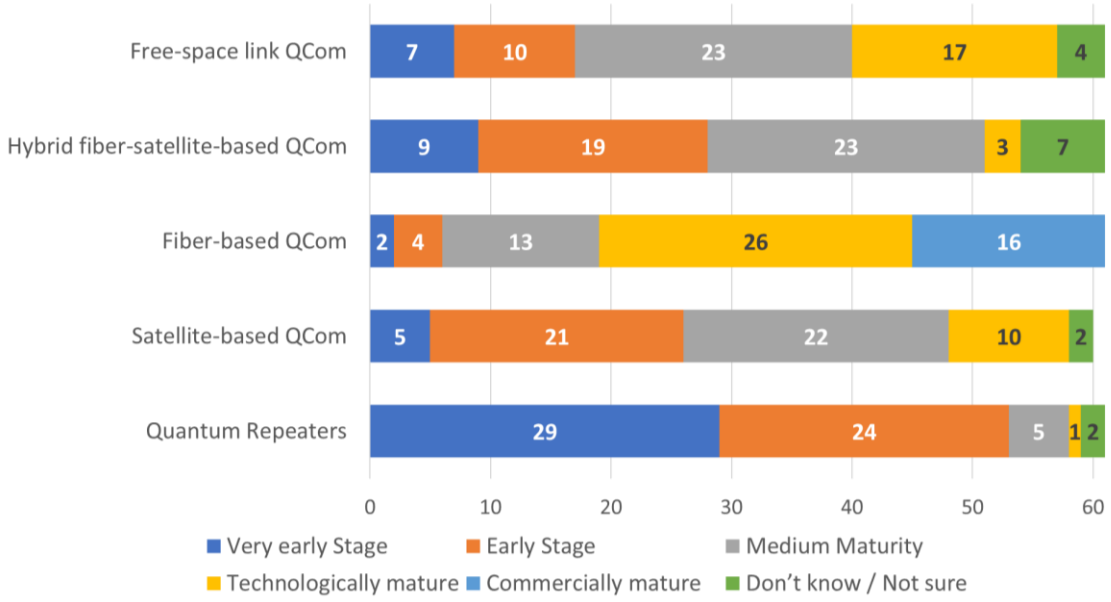
new, is increasingly acknowledged for its long-distance potential, distinguishing it from other emerging protocols.

Overall, the survey indicates that while some protocols are already in active use, others are transitioning from experimental demonstrations toward practical deployment, and the next decade is expected to bring significant progress in their adoption and integration into existing communication infrastructures.

4.4.2 Fiber-based Quantum Communication and the Role of Quantum Repeaters

Considering recent research trends and their potential impact, the survey results indicate a strong consensus among participants regarding the strategic importance of fiber-based quantum communication over the next decade. This approach is viewed as the primary enabler for near-term deployment, with 38 respondents expecting it to become commercially available outside controlled laboratory environments. Moreover, 55 out of 59 participants rated its impact over the next ten years as highly significant (multiple answers were possible). Its compatibility with existing telecom infrastructure and potential for scalable implementation make it a cornerstone of future quantum communication systems. The values of the assessments are illustrated in Figure 8.

Figure 8: Assessment of the maturity of quantum communication technologies

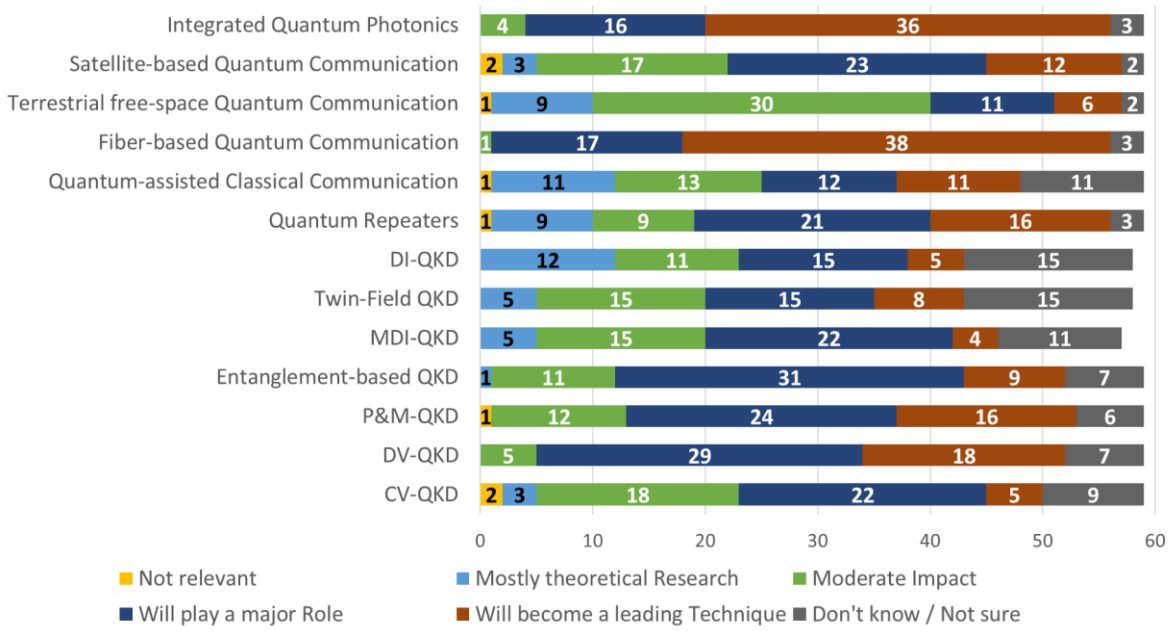


Source: Survey by UDS/Fh ISI

However, the realization of long-distance fiber-based quantum communication faces a fundamental limitation: the exponential loss of quantum signals over optical fibers. Overcoming this challenge requires the development of quantum repeaters, which enable entanglement swapping and quantum memory storage, thereby allowing reliable transmission of quantum information across extended distances.

This technological dependency is reflected in the survey's timeline assessments. Only five out of 61 respondents anticipate that quantum repeaters will be commercially available outside laboratory settings within the next five years, whereas the majority predict availability within the next 20 years (n = 48) or beyond (n = 7). A graphical representation of these values is provided in Figure 9.

Figure 9: Assessment of the potential Impact of quantum communication areas in the next ten years



Source: Survey by UDS/Fh ISI

The importance of quantum repeaters is further underscored by their role in long-term application areas: secure communication was identified as the most critical use case for quantum communication technologies, given its relevance to national security, financial systems, and critical infrastructure. Without quantum repeaters, secure quantum links over continental or global scales would remain infeasible.

Summary and Implications of Fiber-Based Quantum Communication and Quantum Repeaters

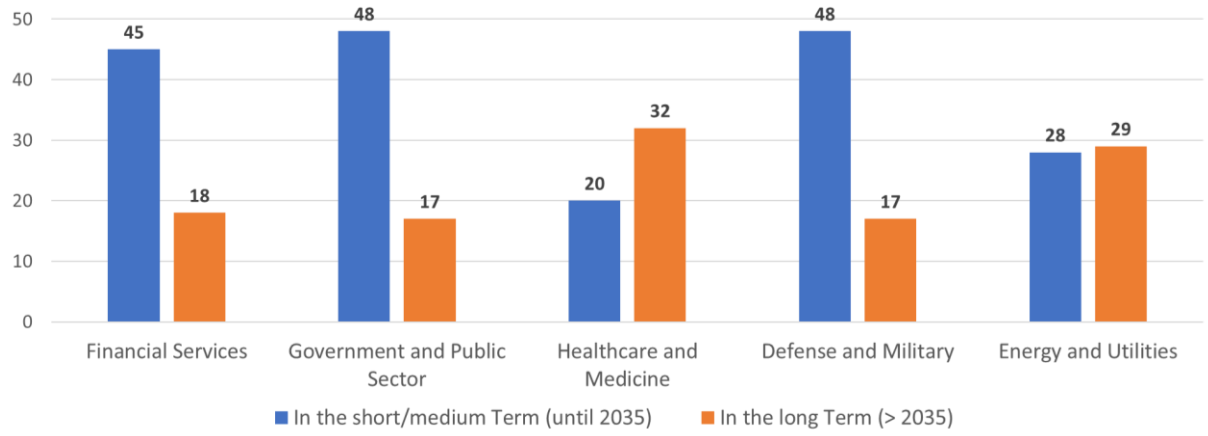
Overall, the survey indicates that fiber-based quantum communication is expected to drive early adoption efforts. Its commercial relevance is closely tied to the advancement in quantum repeater technologies, which are essential for overcoming distance limitations and enabling scalable quantum networks. The full potential of fiber-based quantum systems – particularly for secure communication across large-scale networks – depends on the successful development and deployment of quantum repeaters. This interdependency highlights the need for coordinated research, technological innovation, and infrastructure planning to ensure the scalability and resilience of future quantum networks.

4.4.3 Market Potential of Quantum Communication across Sectors

The survey evaluated the market potential of quantum communication through several questions. One key question asked respondents to assess the potential of quantum communication technologies across five predefined sectors: a) Financial Services, b) Government and Public Sector, c) Healthcare and Medicine, d) Defense and Military, and e) Energy and Utilities. Participants were asked to assess each sector's potential both in the short / medium term (up to 2035) and in the long term (from 2035 onward). A total of 61 respondents answered these questions, with multiple selections possible. The results reveal a clear shift in perceived market potential over time. They are

presented separately for the two time horizons, followed by implications for use cases and value creation. Figure 10 shows the values of the assessment.

Figure 10: Expected highest market potential sectors



Source: Survey by UDS/Fh ISI

Short / Medium Term (up to 2035):

In the short to medium term, Government / Public and Defense / Military lead with 48 responses each, reflecting strong demand for secure communication infrastructures in diplomacy, law enforcement, and mission-critical operations. Financial Services follows closely with 45 responses, emphasizing the need for ultra-secure transactions and fraud-resistant systems. Energy / Utilities received 28 responses, while Healthcare / Medicine had 20, indicating a slower adoption pace in these sectors in the near term.

Long Term (from 2035 onward):

Over the long term, the perceived market potential shifts toward Healthcare and Medicine, which becomes the leading sector with 32 responses, followed by Energy and Utilities with 29 responses. This reflects growing concerns about data protection, secure research collaboration, and infrastructure resilience. Financial Services remains relevant with 18 responses, but its relative priority declines compared to earlier expectations. Government / Public and Defense / Military drop to 17 responses each, indicating that their strategic advantages will be realized earlier and then plateau at a lower level.

Implications for Use Cases and Value Creation

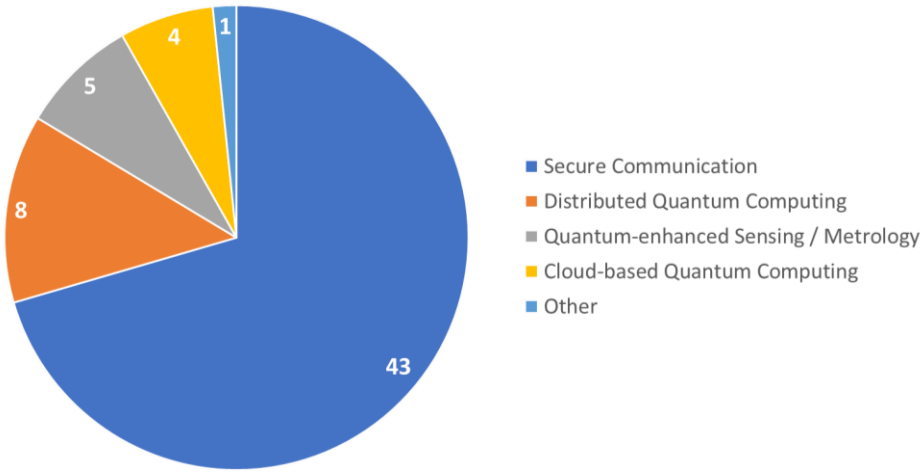
These trends suggest that quantum communication will initially create the most value in sectors where security and confidentiality are mission-critical, such as Government / Public, Defense / Military, and Financial Services. Over time, the focus is expected to shift toward Healthcare / Medicine and Energy / Utilities, driven by increasing digitalization, stricter data protection requirements, and the need to secure critical infrastructures. Healthcare emerges as the strongest long-term growth area, highlighting the importance of safeguarding patient data and enabling secure collaboration in research. Energy / Utilities also gains prominence, reflecting sustained demand for resilient communication in smart grids and energy systems. In contrast, Government / Public and Defense / Military are expected to plateau after early adoption, as their initial strategic advantages are realized and the market matures.

4.4.4 Long-Term Application Areas for Quantum Communication Technologies

QKD

To assess long-term expectations, the survey included a question on which application area is expected to benefit most from quantum communication technologies in the future. Respondents could choose from four predefined options: a) Secure Communications, b) Distributed Quantum Computing, c) Quantum-enhanced Sensing / Metrology, or d) Cloud-based Quantum Computing Access – and could also provide additional suggestions. This question aimed to identify strategic priorities and anticipated value creation across different technological domains. The values are summarized in Figure 11.

Figure 11: Expected long-term application areas of quantum communication



Source: Survey by UDS/Fh ISI

As shown in Figure 11 the results reveal a clear consensus regarding the dominant long-term application: Secure Communications (e.g., quantum key distribution) received 43 out of 61 responses. This strong preference underscores the strategic importance of secure communication channels that remain resilient against future quantum computing threats. The emphasis on security reflects rising awareness of data confidentiality and integrity in an increasingly digitized environment.

The second most frequently mentioned application was Distributed Quantum Computing, with eight responses, indicating that while security remains the top priority, there is also recognition of quantum communication's potential to enable collaborative computing architectures and enhance overall computational efficiency.

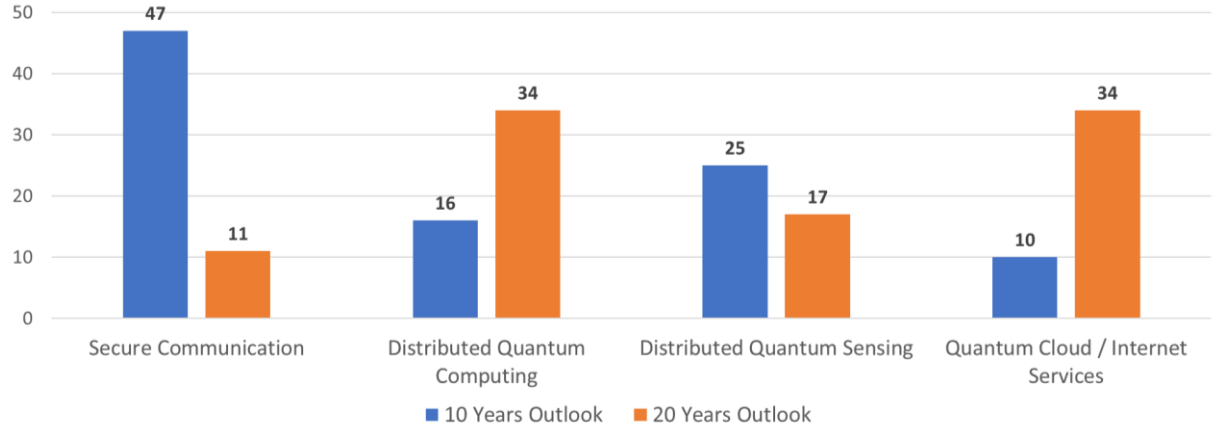
Other application areas – such as Cloud-based Quantum Computing Access (n = 5), Quantum-enhanced Sensing and Metrology (n = 4), and the concept of a so-called Quantum Internet (n = 1) – received comparatively limited attention. These findings suggest that, although such domains hold promise for specialized use cases, they are not yet perceived as primary drivers of long-term value creation.

Quantum Networks

To explore future use cases, the survey included a question on quantum networks, introduced with a brief explanation of their capabilities. Respondents were asked to identify what they believe will

be the most significant applications of quantum networks over two time horizons: in 10 years and in 20 years. The main options were: a) Secure Communication, b) Distributed Quantum Computing, c) Distributed Quantum Sensing, and d) Quantum Cloud / Internet Services, with the possibility of additional suggestions in a free-text field. This question aimed to capture expectations regarding the evolution of quantum network capabilities and their potential to enable transformative applications across various domains. A total of 61 participants answered, with multiple selections possible. The responses were evaluated separately for each time horizon. Figure 12 provides an overview of the values.

Figure 12: Applications of quantum networks by their assessed significance



Source: Survey by UDS/Fh ISI

In 10 Years:

Secure communication clearly dominates in the short-term outlook, with 47 out of 61 responses, reflecting the expectation that quantum networks will primarily serve as a foundation for ultra-secure data transmission using quantum encryption and communication protocols. This focus highlights the continued prioritization of confidentiality and resilience against emerging cyber threats in the near future.

The second most cited application is Distributed Quantum Sensing, with 25 responses, suggesting growing interest in using entanglement-based networks to enhance precision in scientific and industrial measurements across distances. Other potential applications were chosen less frequently: Distributed Quantum Computing received 16 responses and Quantum Cloud and Internet Services ten responses, indicating that computational and cloud-based applications are expected to remain niche over the next decade.

In 20 Years:

In the long term, expectations shift markedly toward computational and cloud-based applications. Both Distributed Quantum Computing and Quantum Cloud or Internet Services receive 34 responses, signaling a strong belief that interconnected quantum processors and remote access to quantum resources will become central capabilities. These developments are anticipated to enable collaborative problem-solving and form the backbone of future digital infrastructure.

Distributed Quantum Sensing remains relevant, with 17 responses, indicating that precision measurement across distances continues to be valued, albeit as a secondary application. Secure Communication, which dominated the ten-year outlook, drops to eleven responses, suggesting that

while security will remain important, it is no longer viewed as the primary driver of quantum network development in the long term.

Summary and Outlook on Long-Term Application Areas for Quantum Communication Technologies

The survey results reveal a distinct evolution in the perceived applications of quantum communication technologies. For QKD, secure communication remains the dominant long-term application, emphasizing its strategic role in safeguarding data against future quantum computing threats. Other applications such as Distributed Quantum Computing, Cloud-based Quantum Access, and Quantum-enhanced Sensing receive comparatively limited attention, indicating that QKD is primarily valued as a security enabler.

In contrast, expectations for quantum networks, evolve significantly over time. In the 10-year horizon, secure communication is the leading application, supported by 47 responses, with Distributed Quantum Sensing emerging as a promising secondary use case. Computing and cloud-based services are mentioned but remain niche expectations. By the 20-year horizon, priorities shift toward Distributed Quantum Computing and Quantum Cloud or Internet Services, each receiving 34 responses, reflecting strong confidence that quantum networks will support collaborative problem-solving and remote access to quantum resources. Distributed Sensing retains moderate relevance, while Secure Communication declines, signaling its reduced dominance in the long term.

Overall, these responses suggest a clear trajectory: security-focused applications are believed to dominate the short term, whereas the long-term vision for quantum communication technologies involves diversification. Quantum networks are expected to underpin a broad ecosystem of computing, sensing, and cloud services, reflecting both technological maturation and the integration of quantum capabilities into future digital infrastructures.

4.4.5 Timeline Perspectives on Quantum Communication and Network Developments

This section presents a consolidated analysis of survey responses addressing the temporal evolution of quantum communication and quantum network technologies. It synthesizes expectations regarding technological impact, application relevance, market potential, and deployment timelines. Several questions explored how these technologies are anticipated to evolve over time, including key milestones and sector-specific developments, providing a strategic outlook on the field over the coming decades.

Potential Impact of recent Research Trends

Building on the timeline-oriented analysis, the survey results allow for several assessments regarding the expected development and application of quantum communication technologies. Some questions were specifically designed to capture expectations for the next decade and beyond. One such question invited respondents to assess the potential impact that various research areas may have on quantum communication over the next ten years, e.g., Continuous-Variable QKD, Prepare-and-Measure QKD, and Quantum Repeaters. Responses were collected from 59 participants, revealing clear prioritization trends (cf. Figure 9).

Fiber-based Quantum Communication (n = 55) and Integrated Quantum Photonics (n = 52) were most frequently identified as highly promising, suggesting they are expected to play a leading role in the coming decade. Strong support was also expressed for Discrete-Variable QKD (n = 47),

Prepare-and-Measure QKD (n = 40), and Entanglement-Based QKD (n = 40), which are likewise anticipated to be major contributors to near-term technological development.

Technologies such as Quantum Repeaters (n = 37), Satellite-Based Quantum Communication (n = 35), and Quantum-assisted Classical Communication (n = 33), were considered important enablers, though their relevance is expected to be more selective or application-specific. By contrast, Terrestrial Free-Space Quantum Communication (n = 17), Device-Independent QKD (n = 20), Twin-Field QKD (n = 23), Measurement-Device-Independent QKD (n = 26), and Continuous-Variable QKD (n = 27) were more often viewed as uncertain or still largely theoretical within the ten-year timeframe.

Overall, the results suggest that fiber-based approaches and integrated photonics are expected to dominate near- to mid-term developments, while other methods may remain niche or exploratory until further technological advances are achieved.

Long-term Application Areas of Quantum Communication

As part of the timeline-oriented analysis, the survey explored long-term expectations regarding the application of quantum communication technologies. Participants were asked to indicate which application area they believe will benefit most from these technologies in the long term, focusing on strategic relevance rather than short-term feasibility. The predefined options included: a) Secure Communications, b) Distributed Quantum Computing, c) Quantum-enhanced Sensing / Metrology, and d) Cloud-based Quantum Computing Access, with the opportunity to provide additional suggestions in a free-text field (cf. Figure 11).

Responses from 61 participants reveal a strong consensus that secure communication infrastructures will remain the primary beneficiary of Quantum Communication Technologies (n = 43). This underscores the enduring importance of highly secure channels that remain resistant to future quantum computer attacks. Sectors identified as key long-term drivers of adoption include healthcare, energy and utilities, and financial services, with additional emphasis on the government and public sector as well as defense and military, where secure quantum links are expected to provide lasting value.

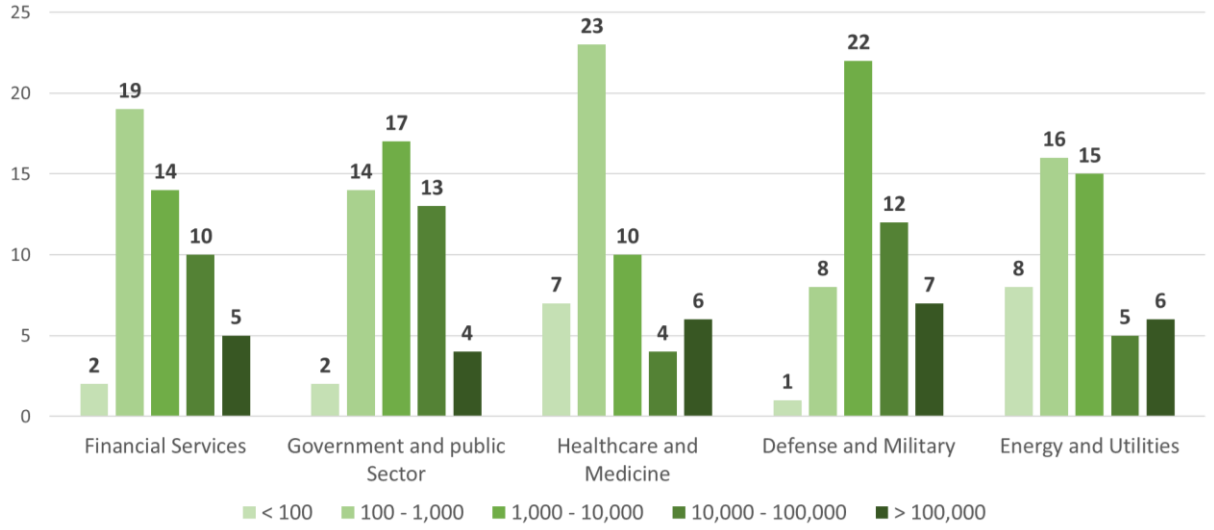
Other application areas were cited considerably less frequently. Distributed Quantum Computing (n = 8), Cloud-based Quantum Computing Access (n = 5), and Quantum-enhanced Sensing and Metrology (n = 4) were each recognized as promising but secondary application domains.

These findings suggest that, while a diverse range of applications is envisioned, the community sees the most transformative long-term impact of quantum communication in enabling secure communication infrastructures. Other use cases are expected to evolve more gradually and will likely depend on advances in scalability, interoperability, and the broader integration of quantum communication technologies into existing networks.

Projected Market Potential for QKD Devices

To assess the market potential for QKD devices, the survey asked respondents to estimate how many units could be sold globally over the next decade across five market segments: a) > 100, b) 100–1,000, c) 1,000–10,000, d) 10,000–100,000, and e) <100,000 units. This question aimed to capture quantitative expectations for future demand and provide insights into sector-specific growth opportunities. Responses from 50 participants reveal a strong prioritization of security-critical markets, in line with earlier findings that identified secure communications as the most important long-term application of quantum communication technologies. The values of the assessments are shown in Figure 13.

Figure 13: Expected global sales of QKD devices in the next ten years



Source: Survey by UDS/Fh ISI

The defense and military sector tops the ranking with respondents anticipating large-scale adoption: 22 participants protected sales of 1,000–10,000 devices, twelve expected 10,000–100,000, and seven foresaw more than 100,000 units. This reflects the central role of secure communications in military operations, intelligence sharing, and defense infrastructure.

The government and public sector follows closely, with 17 respondents projecting 1,000–10,000 devices and 13 expecting 10,000–100,000. Only four anticipated sales above 100,000 units, yet the distribution indicates a robust role for QKD in national security and secure administrative infrastructures, where the protection of sensitive governmental data and communication channels is critical.

The financial services sector was also identified as a key driver of adoption. While 19 respondents anticipated 100–1,000 devices, a substantial group projected larger volumes: 14 expected 1,000–10,000, and ten foresaw 10,000–100,000 devices. This outlook reflects the sector's reliance on highly secure communication channels for financial transactions and fraud prevention, consistent with the broader survey emphasis on secure communications.

By contrast, the energy and utilities sector is associated with more modest projections. 16 respondents estimated 100–1,000 devices, and 15 anticipated 1,000–10,000, with only a small number expecting higher adoption.

Finally, the healthcare and medical sector appears as the least dynamic market in relative terms. The majority (n = 23) projected 100–1,000 devices, with fewer respondents expecting mid- or large-scale adoption.

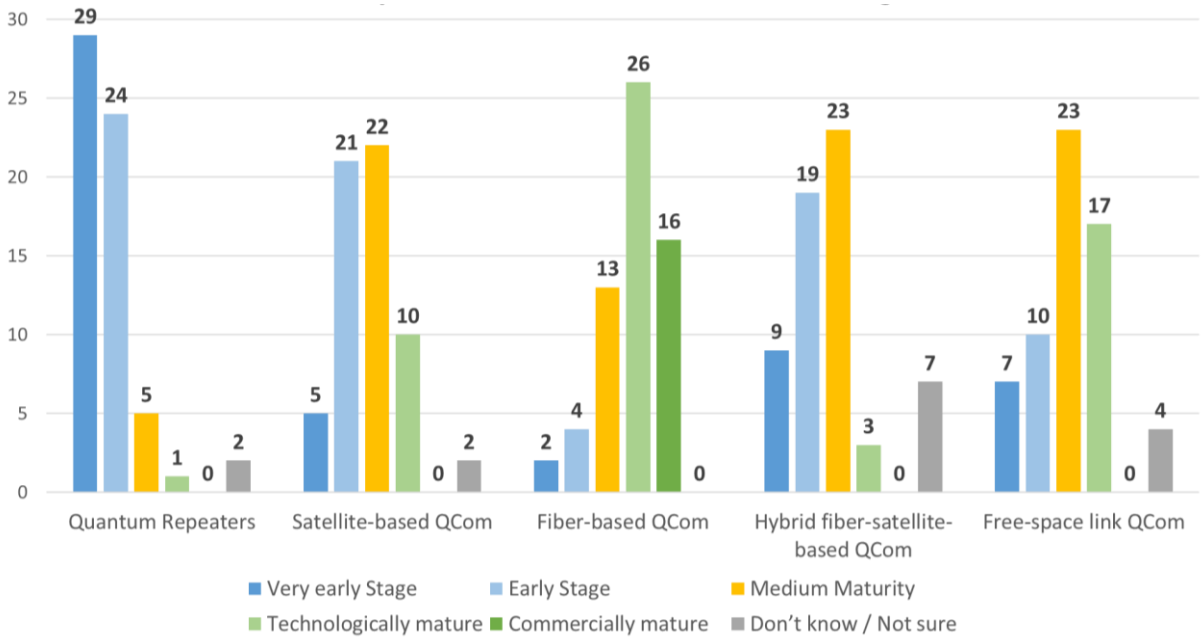
Overall, the results indicate that defense, government, and financial services are expected to be the primary drivers of QKD adoption These projections align closely with the survey's earlier finding that secure communications represent the most critical long-term application of quantum communication technologies. In contrast, sectors such as energy and healthcare are expected to play a secondary role, with comparatively limited growth potential over the next decade.

Timeline Expectations for Quantum Communication Advances

To assess the expected timeline for key technological advances in quantum communication, respondents were asked to estimate when specific developments might move beyond research

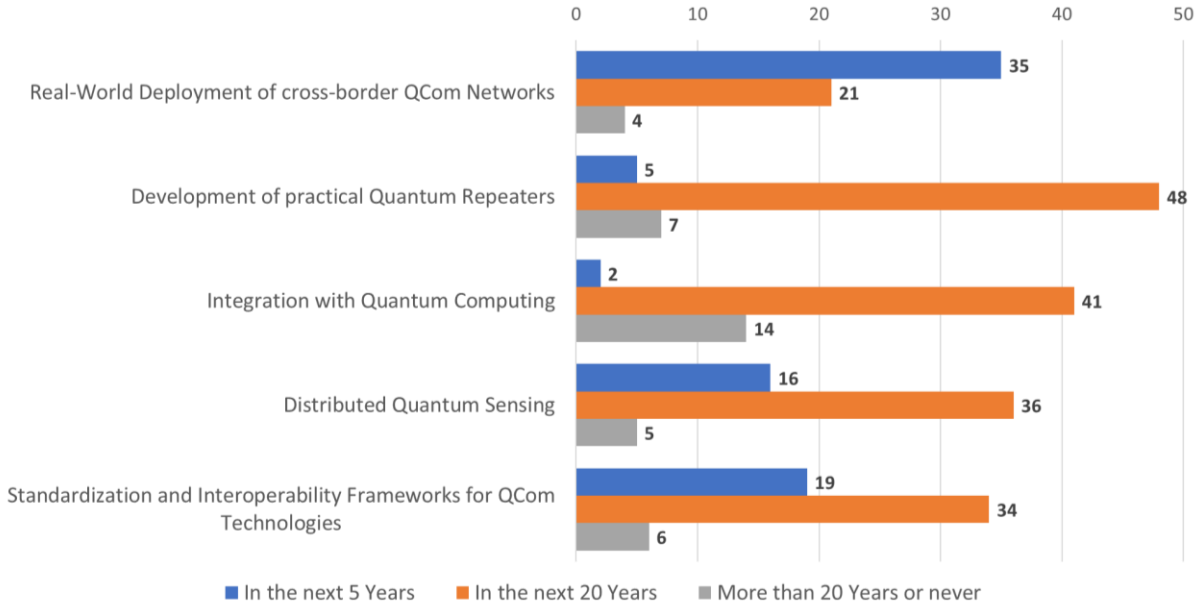
environments and become commercially available. The question focused on innovations such as integration with quantum computing, development of practical quantum repeaters, and real-world deployment of cross-border quantum communication networks, with the option to provide additional suggestions in a free-text field. Responses from 61 participants reveal a differentiated outlook, with some technologies anticipated in the near term and others seen as longer-term milestones. The values of the assessment are summarized in Figure 14 and Figure 15.

Figure 14: Assessment of the maturity of quantum communication technologies



Source: Survey by UDS/Fh ISI

Figure 15: Expected commercial availability of quantum communication advances



Source: Survey by UDS/Fh ISI

Cross-border quantum communication networks, including satellite-based links and backbone infrastructures, received the most optimistic outlook: 35 respondents expect deployment within the next five years, 21 within 20 years, and only four believe it will take more than 20 years or never. This reflects the maturity of satellite-based QKD initiatives and growing international interest in quantum-secure infrastructure.

Practical Quantum Repeaters – including quantum memories and fault-tolerant designs – are considered a longer-term challenge. Only five participants expect progress within five years, while 48 anticipate deployment within 20 years. Seven participants believe it will take longer or may never materialize. This cautious outlook highlights the technical complexity of repeater technologies and their critical role in enabling scalable quantum networks.

The integration of quantum communication with quantum computing, such as secure Quantum Cloud Access or Distributed Quantum Processing, is similarly viewed as a mid- to long-term goal. Only two participants expect progress within five years, 41 within 20 years, and 14 foresee a longer horizon. This underscores the emerging nature of quantum network architectures and the need for foundational progress in both fields.

Distributed Quantum Sensing, including entanglement-enhanced timing and navigation, shows a more balanced distribution. 16 respondents anticipate it within five years, 36 within 20 years, and five beyond that or never. This suggests growing interest in quantum-enhanced metrology and its potential for earlier adoption in specialized applications.

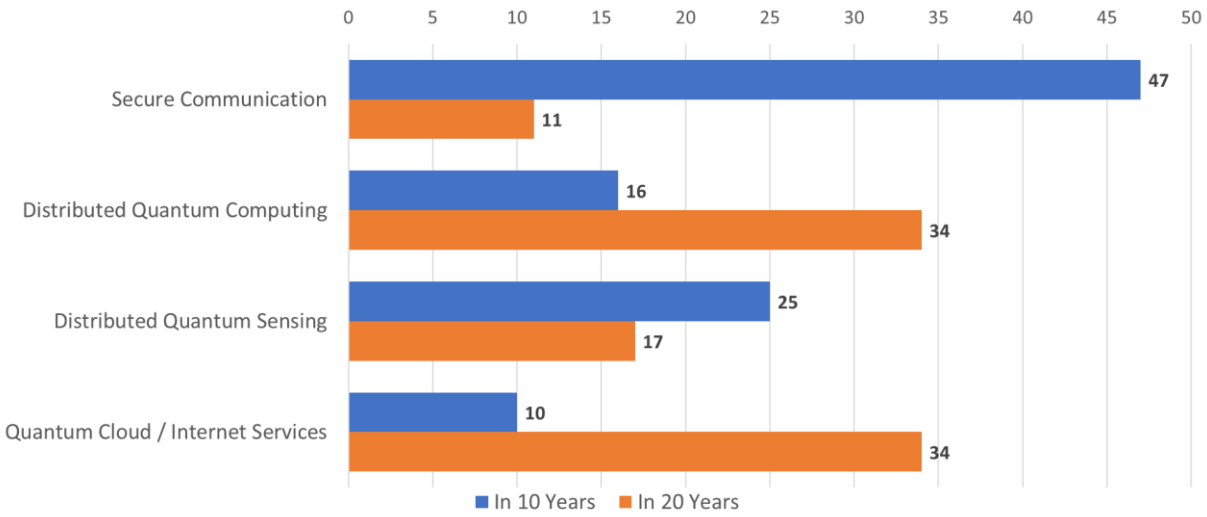
Finally, standardization and interoperability frameworks for quantum communication technologies are expected to evolve steadily. 19 participants anticipate progress within five years, 34 within 20 years, and six beyond that or never, emphasizing the importance of interoperability as a critical enabler for global quantum networks.

Taken together, these results indicate a clear differentiation in expected timelines. While some technologies – particularly satellite-based networks and distributed sensing – are expected to mature within the next five years, others – such as Quantum Repeaters and secure Quantum Cloud Access or Distributed Quantum Processing – remain dependent on significant breakthroughs in scalability and architecture design. This highlights that the pace of quantum communication advances will vary widely across technology domains, with near-term progress concentrated in network deployment and specialized sensing, and longer-term milestones tied to enabling technologies for large-scale, interoperable quantum infrastructures.

4.4.6 Timeline Expectations for Applications of Quantum Networks

To explore expectations regarding the timeline for key applications of quantum networks, the survey asked respondents to estimate when specific use cases are likely to become relevant. The predefined options included: a) Secure Communication, b) Distributed Quantum Computing, c) Distributed Quantum Sensing, and d) Quantum Cloud / Internet Services. Participants could indicate whether they expect these applications to gain importance within the next ten years or within the next twenty years, and were also invited to share additional suggestions in a free-text field. Responses from 61 participants reveal a clear prioritization of secure communication, with other applications expected to follow over a longer horizon. The values of the assessment are presented in Figure 16.

Figure 16: Expected key applications of quantum networks



Source: Survey by UDS/Fh ISI

Secure Communication stands out as the most immediate application. 47 respondents expect it to become relevant within ten years, while only eleven anticipate a timeline of 20 years. This strong consensus reflects the maturity of quantum encryption technologies and their growing importance in safeguarding sensitive data against evolving cyber threats.

Distributed Quantum Computing, which involves linking quantum processors to solve complex problems collaboratively, is regarded as a longer-term goal. Only 16 participants expect it to become relevant within ten years, whereas 34 foresee this within 20 years. This cautious outlook reflects the technical challenges of synchronizing quantum systems across networks and the need for robust and scalable infrastructure.

Distributed Quantum Sensing, which leverages entanglement-based networks to enhance measurement precision in scientific and industrial contexts, presents a more balanced outlook. 25 respondents expect its emergence within ten years, and 17 within 20 years. This indicates growing belief in its potential for earlier adoption in specialized domains such as navigation, metrology, and environmental monitoring.

Quantum Cloud and Internet Services, providing remote access to quantum computing and networked quantum resources, are expected to evolve more gradually. Only ten participants anticipate relevance within ten years, while 34 expect it within 20 years. This reflects the ongoing foundational work required to establish scalable and interoperable quantum network architectures.

Overall, the results indicate a phased development trajectory. Secure Communication is expected to dominate the near term due to technological maturity and pressing security demands. In contrast, Distributed Quantum Computing, Distributed Quantum Sensing, and Quantum Cloud Services are viewed as longer-term milestones that will emerge as infrastructure, interoperability, and system integration mature.

Summary and Outlook on Timeline Expectations for Applications of Quantum Networks

The survey responses provide a comprehensive temporal perspective on the evolution of quantum communication and quantum network technologies. Across all time-related questions, a consistent

pattern emerges secure communication is expected to drive short-term technological impact and market adoption, particularly in sectors such as defense, government, and finance.

In the near term, fiber-based quantum communication and integrated quantum photonics are seen as key enablers, paving the way for early deployment. In contrast, more complex systems such as quantum repeaters and integration of quantum communication with quantum computing are regarded as longer-term milestones, dependent on significant progress in scalability, interoperability, and network architecture. Together, these findings point toward a gradual yet transformative evolution of quantum network application – from security-focused systems in the coming decade toward distributed quantum computing, distributed quantum sensing, and cloud-based infrastructures in the longer term.

4.5 Recent Trends in Quantum Communication

Inspired by the survey results, this update takes a closer look at several developments that have gained considerable momentum in recent years but were not covered in detail in the previous edition of the monitoring report. It serves both as an update and as an emphasis on particularly prominent trends.

4.5.1 Twin-Field Quantum Key Distribution

Twin-Field QKD (TF-QKD) has become a hot topic in quantum key distribution, as compared to other QKD protocols it changes the effective scaling of the secret key rate with distance from linear to approximately square-root, yielding repeater-like performance without actual quantum repeaters. In conventional point-to-point decoy-state QKD, the probability that a photon sent by Alice reaches Bob and is successfully detected is proportional to the total channel transmittance η, so the secret key rate scales roughly as $R \propto \eta$ and therefore decays exponentially with distance. In TF-QKD, Alice and Bob each send phase-randomized very weak coherent states to a middle station. The fields arriving at the relay have amplitudes $\propto\sqrt{\eta}$, and the interference pattern (which determines which detector clicks) depends on these amplitudes, not on a single photon having survived the full distance. After optimizing the signal intensities and using decoy-state analysis, Lucamarini et al. show that the secret key rate can scale asymptotically as $\propto\sqrt{\eta}$ rather than η [119]. From a security-model perspective, TF-QKD can be regarded as a special single-photon-interference variant of measurement-device-independent QKD. As in MDI-QKD, all detection events occur at an untrusted relay, and security can be established without assumptions on the measurement apparatus. The essential distinction is that, unlike conventional MDI-QKD based on two-photon Bell-state measurements, TF-QKD exploits first-order interference of weak coherent fields, resulting in the favorable rate-loss scaling.

TF-QKD is closely related to a family of phase-interference protocols such as Phase-Matching QKD [120] and the Sending-or-Not-Sending (SNS) protocol [121], which have become the dominant practical instantiations in long-distance demonstrations. In these schemes, decoy-state techniques are used to bound single-photon contributions, while classical post-processing extracts a secret key from correlated phase-encoded detection events.

A central experimental challenge is maintaining phase coherence between two independent remote lasers over long and noisy optical fibers. Early high-performance demonstrations relied on sophisticated phase stabilization and ultra-low-noise detection, including architectural refinements such as dual-band stabilization to mitigate scattering noise from stabilization light [122]. These efforts enabled rapid progress in record distances on low-loss spooled fibers, with landmark demonstrations around and beyond the ~800 km regime using SNS-based approaches and state-of-the-art superconducting nanowire single-photon detectors (SNSPDs) [48, 123]. While such records mainly

reflect optimized laboratory conditions, they established the TF-class rate advantage and clarified the parameter regimes where TF-QKD can outperform conventional decoy-state BB84 in the long-haul limit.

Recently, TF-QKD has progressed to operation in real telecom infrastructures. In 2024, this was illustrated by a 546 km field demonstration using independent optical frequency combs [124] and by first steps towards on-chip photonic integration [125]. In 2025, TF-QKD was demonstrated over a 254 km deployed commercial telecom link between Frankfurt and Kehl without using cryogenic detectors, showing practical long-distance coherent QKD over existing infrastructure [126]. This was complemented by systematic studies of long-fiber Sagnac interferometers as a network-friendly stabilization option [127]. In 2026, large-scale multi-user TF-QKD networking with integrated photonic client chips and a microcomb-based central node further demonstrated the architectural scalability of TF-class protocols and their suitability for chip-based metropolitan networks [128]. In parallel, security analyses showed that wavelength-switching attacks on phase-locked reference channels can open subtle side channels if stabilization light is not adequately monitored and standardized [129].

Despite these advances, several limitations remain. First, many of the best-distance and best-rate demonstrations still rely on high-performance cryogenic SNSPDs and carefully engineered ultra-low-loss fibers, translating these achievements into cost-sensitive, widely deployable systems will require continued progress in detector practicality and system integration. Second, phase and frequency referencing remains both an engineering and a security-critical layer of the stack. They require rigorous calibration, redundancy, and monitoring to remain stable under field conditions and to resist potential side-channel exploitation. Third, performance in deployed networks is reduced by practical overheads that are not captured in idealized protocol descriptions. These include the time and power budget required for phase stabilization and calibration, finite-key statistics that force more conservative security bounds, and environmental variability in real fibers (temperature drift, mechanical perturbations, and loss fluctuations). In multi-user networking scenarios, additional reductions can arise from time-multiplexing and scheduling constraints at the central measurement node.

Overall, TF-QKD has matured from a compelling theoretical proposal into a technology with convincing long-haul and early real-network credentials. The field's center of gravity is now shifting from distance records towards robust architectures and integration. If these engineering and standardization challenges are addressed, TF-QKD is well positioned to become a cornerstone of future metropolitan-to-intercity quantum key distribution. Nevertheless, it comes with a high price tag, as two points should be kept in mind. First, establishing and maintaining sub-wavelength phase coherence between two distant lasers requires enormous technical overhead. Second, although the loss-scaling is repeater-like, TF-QKD does not provide the full functionality of a quantum repeater network, as it does not enable entanglement swapping or access to quantum memories.

4.5.2 Quantum Communication beyond QKD

In the 2024 edition of this monitoring report, quantum communication was discussed with a strong emphasis on quantum key distribution (QKD). While QKD is arguably the most mature quantum communication technology, many industrial stakeholders view it as a niche security enhancement in a landscape where post-quantum cryptography (PQC) offers a scalable alternative. In contrast, distributed quantum computing is increasingly seen as a structurally necessary capability for scaling quantum processors, making it a more compelling long-term driver for quantum networks. This view is also reflected in the responses to our survey on quantum communication presented in the previous section.

It is important to note that, unlike QKD, distributed quantum computing fundamentally relies on the distribution of entanglement between remote nodes. Therefore, these applications are inherently incompatible with trusted-node network architectures, since entanglement must be preserved end-to-end. Instead, memories, spin-photon interfaces, repeaters, or, in other words, a true entanglement-based quantum communication network is required, once famously titled the "quantum internet" [130]. This is also true for the slightly more exotic, but rapidly advancing, fields of blind quantum computing and distributed quantum sensing, which will be also dealt with in this section. Finally, we will turn to a much older idea that is gaining renewed traction, namely entanglement-assisted classical communication.

4.5.2.1 Distributed Quantum Computing

Commercially impactful quantum algorithms, such as Shor's algorithm, require qubit counts, far beyond the capabilities of any existing quantum processor. This has motivated proposals for distributed quantum computing (DQC), in which multiple quantum processing units (QPUs) collectively emulate a larger quantum computer via horizontal scaling. In such architectures, local quantum operations are complemented by classical control links and the distribution of entanglement over quantum channels. When QPUs are separated by macroscopic distances, quantum communication networks become essential, requiring the generation and distribution of remote entanglement, typically via photonic links.

A central bottleneck in this approach is the interface between well-isolated quantum memories and flying photons. This interface is currently most mature in platforms based on trapped ions, neutral atoms, and atom-like defects in solids, which explains why the majority of experimental DQC demonstrations arise from these systems. A recent state-of-the-art experiment demonstrated distributed quantum computing over an optical network link between two trapped-ion modules separated by 2 meters [131]. In this work, a remote controlled-Z gate was implemented via gate teleportation with 86% fidelity between circuit qubits in separate modules, enabling the execution of a Grover search algorithm with a 71% success probability. Beyond remote entanglement generation itself, the experiment required active stabilization against optical phase drift and real-time classical feed-forward, illustrating the complexity of full-stack DQC implementations. Ongoing efforts focus on improving the robustness and quality of remote entanglement distribution, for example through time-bin photonic encoding to mitigate polarization drift [132]. At the same time, the field is expanding beyond ions and atoms, e.g. heralded entanglement and distributed quantum operations have recently been reported in silicon-based platforms using T centers [133].

In contrast, superconducting platforms face substantially greater challenges in establishing an efficient and low-loss spin-photon interface. Current demonstrations of remote entanglement between superconducting qubits rely on microwave-frequency, cryogenic links rather than optical photons, which limits distance, and compatibility with large-scale quantum networks [134, 135].

Microwave-optical transduction is often proposed as a route to integrate superconducting qubits into photonic quantum networks, thereby enabling distributed quantum computing (DQC) over long distances. In principle, a coherent transducer would convert itinerant microwave photons emitted by superconducting circuits into optical photons suitable for low-loss fiber transmission, and vice versa. However, despite substantial progress at the level of individual devices, efficient, low-noise transduction remains an open challenge [136]. State-of-the-art microwave-optical transducers demonstrate either near 50% efficiency at kHz bandwidths [137] or MHz bandwidths with few percent efficiency and near-quantum-limited noise [138–140]. An important bottleneck for superconducting DQC is that the relatively short coherence times of superconducting qubits severely constrain compatibility with heralded-entanglement and quantum-repeater-style protocols, where two-way classical communication introduces latencies comparable to or exceeding qubit coherence

times. As a result, without additional long-lived quantum memories, such architectures restrict the achievable physical distance of distributed entanglement.

In conclusion, trapped ions and atoms currently offer the most promising DQC stack with record long-lived qubits, high-fidelity local gates, and high-quality spin-photon interfaces. The dominant bottlenecks are entanglement generation rate, optical collection and loss and stability and architectural overhead as the number of nodes grows. Notably, the principal challenges of trapped-ion distributed quantum computing largely coincide with those of quantum repeater networks, enabling strong synergies in hardware, protocols, and network-level control as both fields mature.

4.5.2.2 Blind Quantum Computing

Given the scenario that quantum computing reaches commercial deployment, it is highly likely that companies will buy computation time on quantum processors that are not operated within their own facilities but instead provided by quantum data centers. However, the input, output, and algorithm of such computations may be proprietary or contain confidential information. Blind quantum computing (BQC) addresses this challenge by enabling a client to execute a quantum computation on an untrusted remote quantum processor while keeping the client's input, algorithm, and output information-theoretically hidden from the server.

Early proof-of-concept demonstrations of BQC relied on photonic cluster states to implement small-scale blind quantum computations [141, 142]. While these experiments successfully validated the core principles of blindness, the inherently low photon generation and detection rates posed severe scaling challenges. In this regard, it can be seen as a major breakthrough that, in 2025, BQC was demonstrated using solid-state qubits [143]. With silicon-vacancy centers in diamond integrated into nanophotonic cavities, a Deutsch-Jozsa-type algorithm was executed, with client-side photonic measurements secretly defining the computation while the server observed states close to a maximally mixed ensemble. This result constitutes the first end-to-end experimental demonstration of universal BQC on a realistic matter-based quantum-computing platform.

While still far from large-scale realization, the required advances (improved optical interfaces, long-lived quantum memories) are not unique to blind computation but are shared with entanglement-based quantum networks more generally. If quantum computing becomes commercially relevant, blind computation is therefore likely to emerge as a standard feature rather than an exotic add-on.

4.5.2.3 Distributed Quantum Sensing

Distributed quantum sensing leverages entanglement and other nonclassical correlations shared between spatially separated sensors to enhance the precision of measurements of global parameters beyond what is achievable with independent local sensors. The theoretical foundations are well established, showing that appropriately entangled states (e.g. GHZ states or spin-squeezed states) can improve sensitivity to collective phase shifts, frequency offsets, or field gradients [144]. A prominent example is entanglement-enhanced atomic clock networks, where shared entangled states between clocks improve frequency comparison and synchronization, with experiments demonstrating enhanced stability over independent-clock operation and extending to fiber-linked clock networks at kilometer scales [145]. A second key use case is distributed magnetometry and field-gradient sensing, in which spatially separated atomic ensembles or solid-state spin systems (such as NV centers in diamond) are entangled or classically correlated to measure magnetic-field gradients with higher sensitivity or reduced common-mode noise, a regime particularly relevant for geophysics and biomedical imaging [146, 147]. A third emerging application is baseline-enhanced interferometry, where entanglement or quantum correlations between distant sensors effectively increase the interferometric baseline, improving the resolution of phase or displacement measurements in

scenarios such as inertial sensing or gravitational-field detection [148]. By 2024–2025, the scientific focus has shifted toward quantifying the trade-offs between entanglement fidelity, distribution rate, and robustness to loss, as well as identifying concrete sensing tasks in which a provable quantum advantage can be maintained under realistic network constraints.

4.5.2.4 Entanglement-assisted classical communication

While QKD uses quantum mechanics to securely distribute cryptographic keys, entanglement-assisted classical communication is about sending ordinary classical information more efficiently or more reliably, using pre-shared quantum resources such as entanglement. In contrast to QKD the goal is improved use of the physical channel, not cryptography.

At a fundamental level, quantum-assisted classical communication asks how shared entanglement and joint quantum measurements can enhance classical information transmission over noisy physical channels. The simplest and most intuitive illustration of this idea is superdense coding, which shows that if two parties share entanglement, sending a single quantum system can convey more classical information than would otherwise be possible. This protocol is one of the earliest canonical examples of quantum communication and dates back to the original proposal by Bennett and Wiesner [149].

Beyond this idealized setting, entanglement-assisted communication is now understood at the level of channel capacities, where the advantage of entanglement persists even in the presence of noise and loss. A natural question in this broader framework is whether entanglement can make communication arbitrarily better. For bosonic (infinite-dimensional) channels, the advantage can in theory be arbitrarily large, since the only fundamental constraint is energy and the entanglement-assisted capacity can grow much faster with average power than the classical capacity. However, real optical systems are never truly infinite-dimensional as detectors saturate, bandwidth is finite, modulation alphabets are discrete, and noise floors effectively cut off high-energy states. For finite-dimensional systems, Wolff and Matthews recently proved that the gain from entanglement is universally bounded: entanglement can help substantially, but it can increase capacity only by a finite, channel-independent factor and cannot make a finite-dimensional channel arbitrarily powerful [150].

A major milestone in translating these theoretical insights into practice was the experimental demonstration that entanglement-assisted optical communication can exceed the ultimate classical capacity of a noisy, lossy channel under equal power constraints. Hao et al. achieved this using continuous-variable entanglement and joint measurements [151]. Building on this, a sequence of outdoor free-space optical experiments showed that entanglement-assisted links can operate at gigabit-per-second rates, outperform optimized classical systems in strong atmospheric turbulence, and retain a quantum advantage even when classical optical amplifiers are introduced. Representative demonstrations include kilometer-scale free-space links with adaptive optics and high-speed modulation [152, 153]. More recently, deterministic entanglement-assisted communication has been realized over 20 km of installed optical fiber, demonstrating compatibility with existing telecom infrastructure and marking an important step toward deployable fiber-based quantum-enhanced links [154].

Progress is also being made in discrete-variable systems, where entanglement-assisted protocols are increasingly realized in integrated platforms. Photonic chips have demonstrated high-dimensional encoding and nearly deterministic joint measurements, achieving more than three classical bits per transmitted carrier and showing compatibility with scalable photonic architectures [155]. Complementing this, advances in entanglement-assisted error-correcting codes show how shared entanglement can replace redundancy, enabling higher reliability or shorter blocklengths than classical codes alone [156]. In conclusion, quantum-assisted classical communication improves the

transmission of classical bits using shared quantum resources. From an architectural perspective, quantum-assisted communication aligns well with the core objective of a quantum internet, i.e., the distribution of entanglement across a network. It relies on the same underlying infrastructure as quantum repeaters, but places different demands on it. In contrast to quantum key distribution or distributed quantum computing, quantum-assisted classical communication prioritizes high entanglement generation rates and synchronization over long-lived coherence or near-perfect fidelity. This makes it more tolerant of noise and loss, while still benefiting directly from improved entanglement distribution. At the network level, quantum-assisted communication integrates cleanly with classical data transport. Classical information remains classical end-to-end, with quantum resources acting as an enhancement layer rather than a replacement for existing protocols. As a result, quantum-assisted links can be viewed as performance-boosting primitives that coexist with classical modulation, coding, and routing schemes.

These properties suggest that quantum-assisted classical communication may represent an early, practical use case for quantum internet infrastructure.

5 Quantitative Analyses

5.1 Publication Analysis

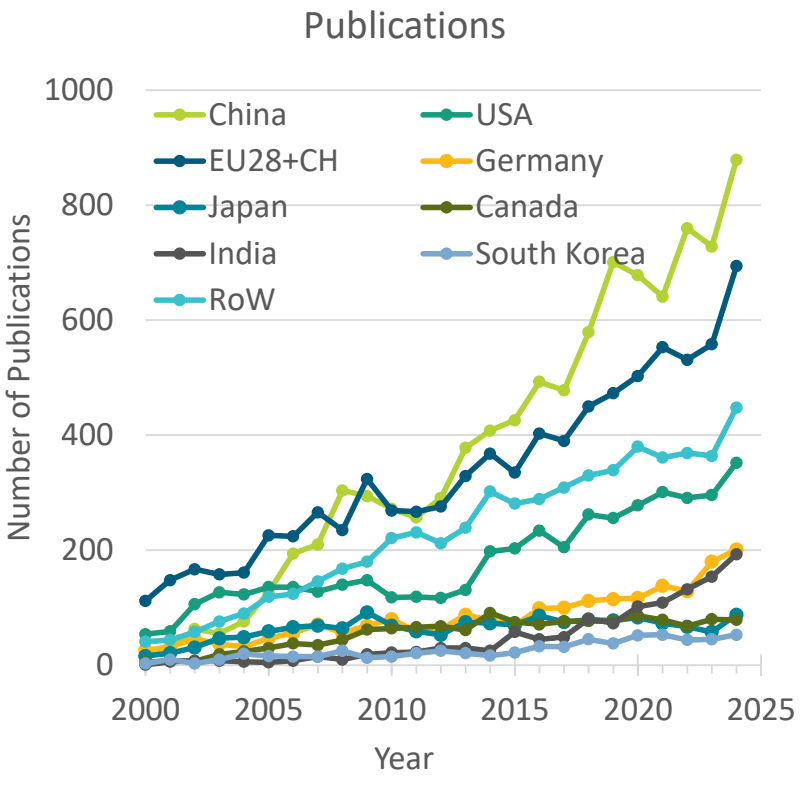
Scientific publications document scientific progress in a certain field of technology. Analyzing how their numbers develop can capture trends in scientific activities as well as the most important active players in a field.

We considered all peer-reviewed publications listed in Web of Science (WoS) for the period from 2000 to 2024 and used a keyword-based search strategy (for details see section 2). The search strategy was slightly changed compared to the first monitoring report [1] to capture more relevant publications and avoid false hits. This fine-tuning of the search strategy has little impact on the overall trends and developments.

Publication dynamics

The number of publications related to quantum communication has increased significantly and continuously over the last more than 20 years (Figure 17). While in 2000, approx. 200 publications were published globally on quantum communication, this number had risen to more than 2000 in 2024. The largest number of publications comes from authors affiliated with institutes from China, closely followed by the EU (EU28 + CH) and with approximately half the number of publications by the USA. Other countries with a relevant number of publications include India, Canada, Japan, South Korea (shown in (Figure 17), Russia, Australia, and Singapore (all bundled under "rest of world - RoW" in (Figure 17)).

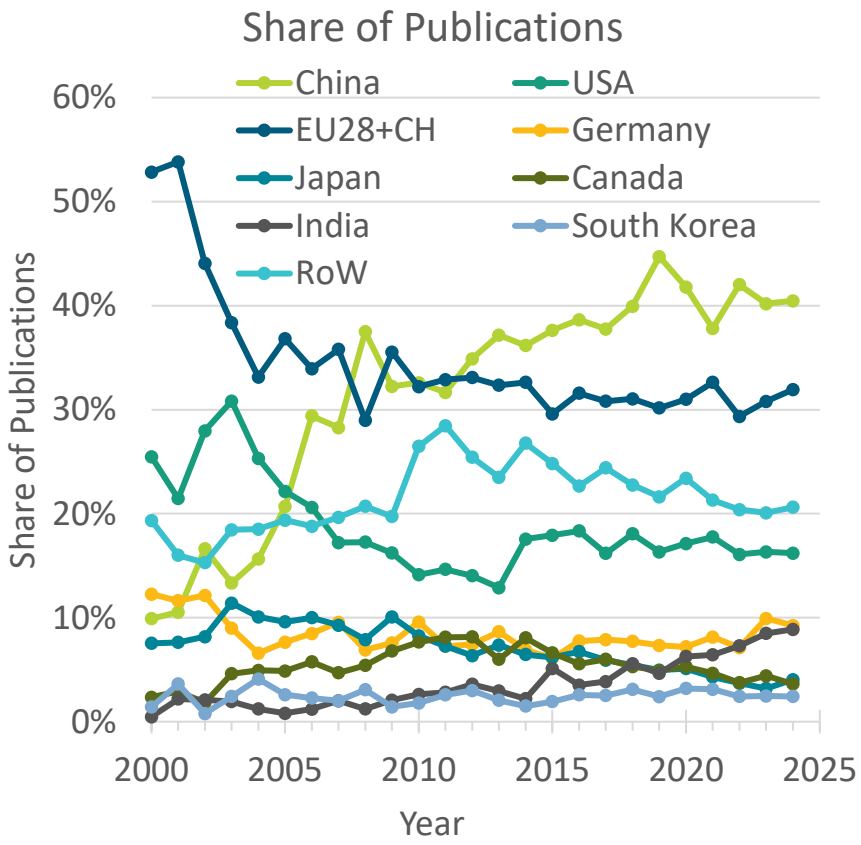
Figure 17: Peer-reviewed publications related to quantum communication of the countries with the highest number of publications from 2000 to 2024



Country comparison

To compare the publication activities in different countries/regions, we analyzed the share of QCom-related publications since 2000 (Figure 18). China started at a share of only ten percent in 2000 but has significantly increased their share to about 40 percent on average. The EU started from more than half of the QCom-related publications in 2000 and still holds a share of about 30 percent in recent years. Germany contributed almost ten percent of the global activities in the recent years. The USA holds a stable share of about 16 percent.

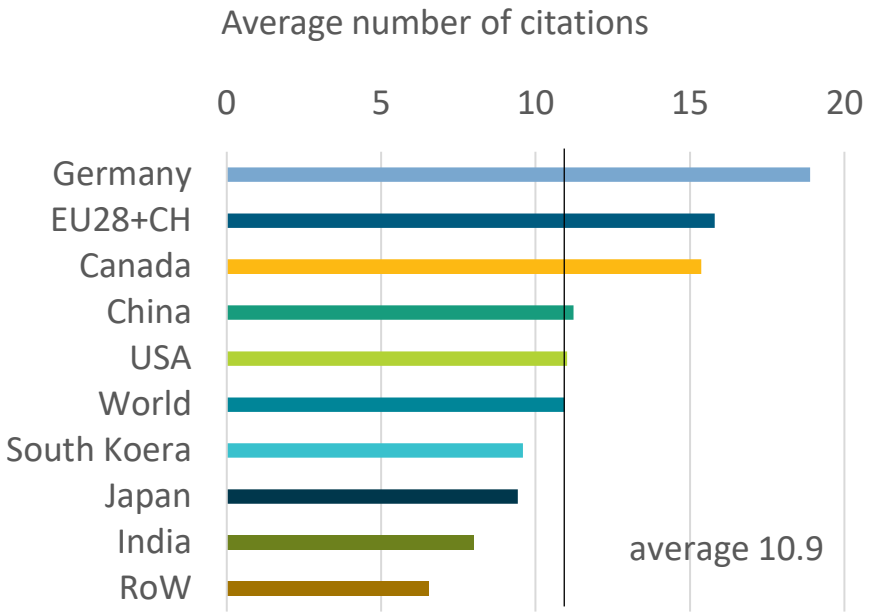
Figure 18: Share of QCom-related publications of the countries with the highest number of publications (and the EU) in the last 20 years



The mere number of publications, however, says little about the relevance and quality of the research results and findings in these publications. In order to obtain an insight into the relevance of publications, we analyzed the average number of citations of the QCom-related publications from 2022 in different countries (Figure 19). Publications from the EU were cited on average 16 times (from Germany even 19 times), those from Canada 15 times, from China and the USA 11 times, from Japan and South Korea 9.5 times. The global average was 11 citations per publication.

These average citation numbers cannot be directly linked to the quality of the publications, as they are prone to bias, e.g., toward high-impact English language journals. Nonetheless, they do indicate the relevance of the published findings to the respective academic community and the high quality of QCom publications in Europe.

Figure 19: Average number of citations of QCom-related publications from different countries (and the EU) from publications of the year 2022 (to account for the citation time lag)



Relevant players

A publication analysis makes it possible to identify the relevant institutions in a certain field. Table 1 lists the institutions and organizations with the largest number of QCom publications between 2020 and 2024. We should note that this table lists funding bodies (e.g., United States Department of Energy), research organizations (e.g., Chinese Academy of Sciences) as well as individual institutions (e.g., Shanxi University). Therefore, care must be taken not to confuse different levels when comparing different organizations and institutions. Most of the organizations and institutions in the list are from China (13), followed by Europe (6, from France, Russia, Italy, the Netherlands, Germany and Spain), the USA (3), India (1), Singapore (1), and Canada (1).

Table 1: Institutions or research organizations with the highest number of QCom-related publications in the years 2020-2024 (top-25)

Institution (country)	Number of publications (2020-24)
Chinese Academy of Sciences (CN)	709
University of Science Technology of China (CN)	494
Beijing University of Posts Telecommunications (CN)	297
Center for Excellence in Quantum Information Quantum Physics (CN)	283
Ministry of Education of the People's Republic of China (CN)	264
Centre National de la Recherche Scientifique (FR)	220

Institution (country)	Number of publications (2020-24)
Shanxi University (CN)	202
United States Department of Energy (US)	190
Tsinghua University (CN)	179
Indian Institute of Technology System (IN)	172
Hefei National Laboratory (CN)	171
Massachusetts Institute of Technology (US)	156
Nanjing University of Posts Telecommunications (CN)	153
Nanjing University (CN)	152
Central South University (CN)	147
University of California System (US)	135
National University of Singapore (SG)	129
University of the Chinese Academy of Sciences (CN)	124
Russian Academy of Sciences (RU)	122
State Key Laboratory of Quantum Optics and Quantum Optics Devices (CN)	120
Consiglio Nazionale delle Ricerche (IT)	118
Delft University of Technology (NL)	118
Max Planck Society (DE)	117
University of Waterloo (CA)	113
Universitat Politecnica de Catalunya (ES)	108

To analyze European activities in QCom publishing, we listed the top 25 European institutions and organizations with the highest number of QCom-related publications in the years 2020-2024 (Table 2). Institutions and organizations from various European countries are represented, namely France (4), the UK (4), Germany (4), Spain (3), Italy (3), Switzerland (2), Poland (2), Austria (1), the Netherlands (1), and Denmark (1). This indicates a broad R&D and knowledge base at research institutions in Europe. Of course, there are many other institutions involved in QCom R&D which cannot all be shown here. All institutions from Germany with at least 20 QCom-related publications in the years 2020-2024 are listed in Table 3.

Table 2: Institutions and organizations from EU28(+CH) with the highest number of QCom-related publications in the years 2020-2024 (top-25)

Institution (country)	Number of publications (2020-24)
Centre National de la Recherche Scientifique (FR)	220
Consiglio Nazionale delle Ricerche (IT)	118
Delft University of Technology (NL)	118
Max Planck Society (DE)	117
Universitat Politecnica de Catalunya (ES)	108
Sorbonne Universite (FR)	95
Austrian Academy of Sciences (AT)	90
Barcelona Institute of Science Technology (ES)	90
Technical University of Munich (DE)	88
University of Cambridge (UK)	87
Institut De Ciencies Fotoniques (ES)	85
Helmholtz Association (DE)	78
Technical University of Denmark (DK)	75
Swiss Federal Institutes of Technology Domain (CH)	73
University of York (UK)	73
Fahrenheit Union of Universities (PL)	72
University of Bristol (UK)	72
Istituto Nazionale di Fisica Nucleare (IT)	69
University of Gdansk (PL)	67
University of Geneva (CH)	65
Fraunhofer Gesellschaft (DE)	63
Université PSL (FR)	61
University of Naples Federico II (IT)	61
Universite Paris Saclay (FR)	60
University of Oxford (UK)	58

Table 3: Institutions and organizations from Germany with at least 20 QCom-related publications in the years 2020-2024

Institution (country)	Number of publications (2020-24)
Max Planck Society	117
Technical University of Munich	88
Helmholtz Association	78
Fraunhofer Gesellschaft	62
Technical University of Berlin	53
Friedrich Schiller University Jena	41
Munich Center for Quantum Science and Technology	40
University of Stuttgart	40
Ruhr University Bochum	31
Humboldt University of Berlin	30
University of Siegen	30
German Aerospace Center - DLR	28
University of Munich	28
University of Münster	27
Free University of Berlin	26
Paderborn University	26
Dresden University of Technology	25
Heinrich Heine University Düsseldorf	24
Leibniz University Hannover	24
Ulm University	24
Leibniz Association	23
Friedrich-Alexander University of Erlangen-Nuremberg	20

To conclude, Europe and Germany hold a good position in QCom-related R&D and publication activity. The trend of the last years has continued with China contributing the majority of publications and Europe having a stable share of 30 percent of global QCom-publications. The R&D base for QCom in Europe can thus be considered good in global comparison.

5.2 Patent Analysis

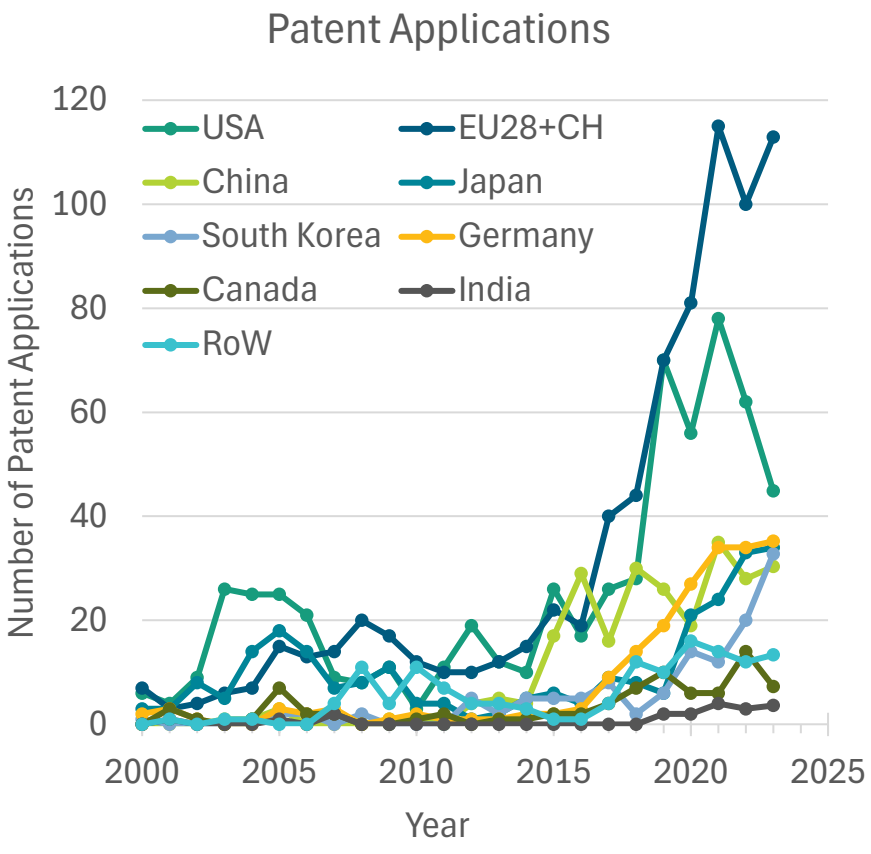
Patents often indicate commercial interest in a field of technology. Analyzing the development of patenting activities is one way to assess commercial interest trends as well as the active players in this field.

For the patent search, we used a search strategy based on both patent classification codes and a text search in title, abstract, and claims (for details, see section 2). To allow for a fair comparison between countries, the search was limited to transnational patent applications, i.e., patent applications to either the European Patent Office (EPO) or the World Intellectual Property Organization (WIPO). These patents focus on inventions with a high expected commercial value. Analogous to the publication search strategy, also the patent search strategy was updated and fine-tuned to find more relevant patents while keeping the number of false hits low.

Patent dynamics

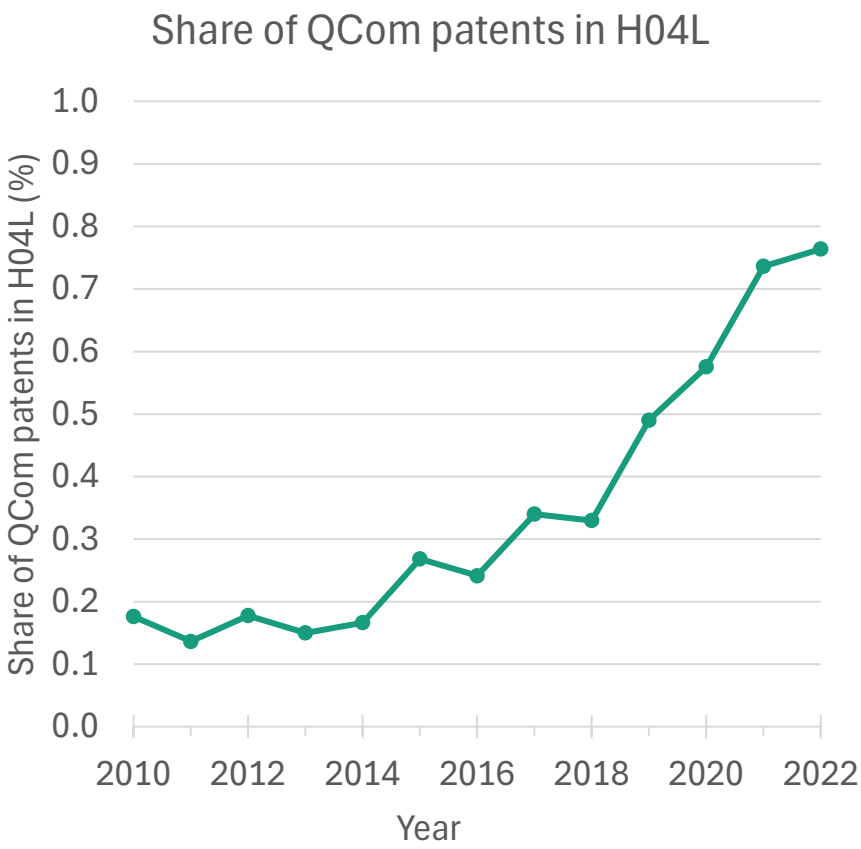
Figure 20 shows the number of QCom-related patent applications between 2000 and 2023 from different countries (and the EU). Overall, a strong increase in patenting activity (from less than 20 in 2000 to more than 250 in 2023) can be observed, especially since 2014. The highest number of patent applications are from the EU (EU28 and CH), followed by the USA, Japan, and China. Other countries with relevant patenting activity include South Korea, Canada, India (shown in Figure 20), Russia, Singapore, and Australia (all bundled under "rest of world - RoW" in Figure 20).

Figure 20: QCom-related transnational patent applications of the countries with the most patent applications (and the EU) from 2000 to 2023



The overall numbers of QCom-related patent applications are still on a low level. The share of QCom-related patents in the most relevant patent class for QCom (H04L - transmission of digital information, e.g. telegraphic communication) is still below one percent. Over the last ten years the share increased significantly (Figure 21) but remains at a low level.

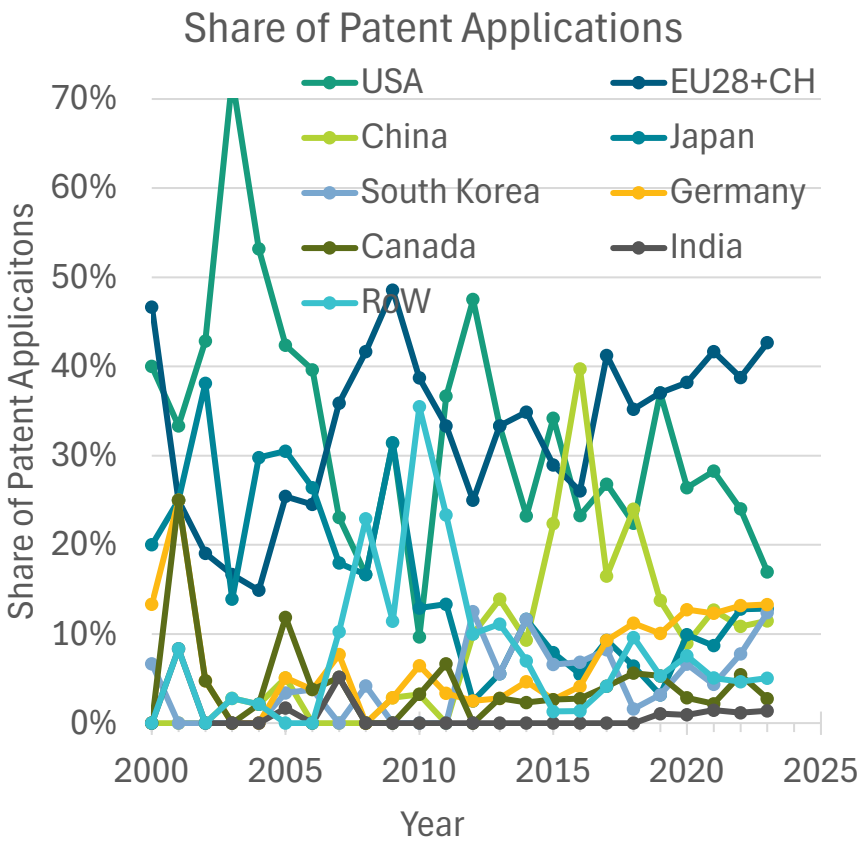
Figure 21: Share of QCom-related transnational patent applications in the patent class H04L, to which most QCom-related patents are assigned, and its development between 2010 and 2022



Country comparison

To compare patenting activities in different countries/regions, we summed up the number of patent applications of institutions located in the different countries in the last ten years of the period analyzed (2013-2022, Figure 22). The EU shows the highest patenting activity with a patent share of more than 34 percent, followed by the USA with almost 30 percent, and China with 13 percent. Germany contributes almost 10 percent of the total patent applications, i.e. almost a third of EU's activities.

Figure 22: Share of QCom-related transnational patent applications of the countries with the most patent applications (and the EU) in the last 20 years



It should be mentioned that these figures do not necessarily reflect the real commercial interest in QCom technologies, as companies might deliberately choose not to patent because they do not want to disclose any information about their systems to potential rivals. Furthermore, development dynamics are currently very high, so that new generations of QCom systems are being developed within the time it takes for a patent to be published, which reduces its protective value. In addition, secure communication technologies and their use by official institutions are highly regulated and the use of imported technologies might be prohibited by national authorities. In fact, an analysis of national QCom-related patents reveals that national patents seem to be of interest in this field, especially in the USA and Germany, where a larger share of national patent applications compared to transnational patent applications can be noted. In China, on the other hand, although the total number of national patent applications is a factor 20 higher than that of transnational patent application, this is less than usual for the Chinese patenting system (that is different compared to other patenting systems and thus comparing the total number of national patents to other national patenting numbers would result in a biased outcome).

Relevant players

The field of QCom is still largely driven by R&D from both industry and research organizations/universities. Analyzing the institutions with the highest number of patent applications in the years 2020-23 indicates the companies that are active in QCom and the universities and research organizations that are active in applied research on these topics. Table 4 lists the 20 institutions with the highest number of QCom-related patent applications in the last four years of the period analyzed. The highest patenting activity is seen in technology companies (including Toshiba, LG Electronics,

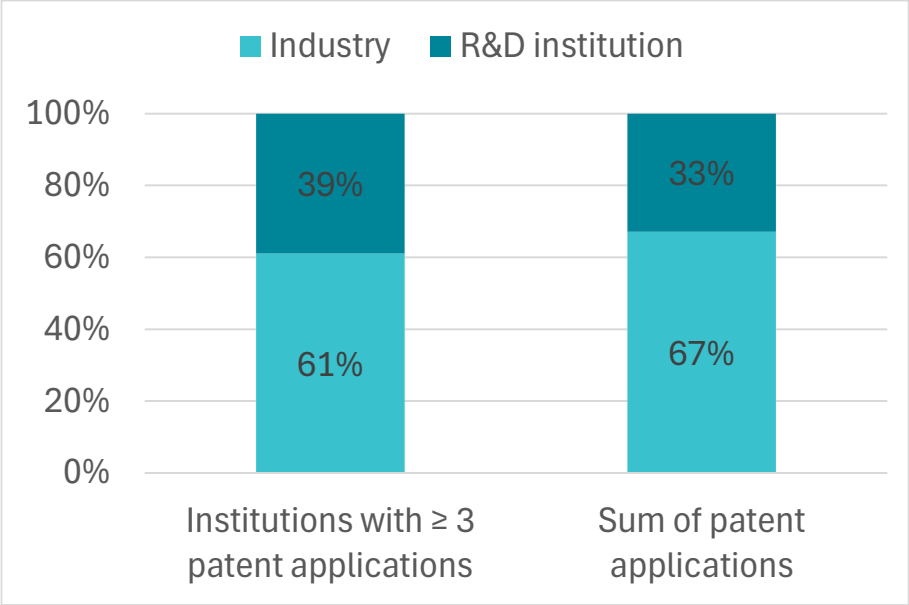
Arquit, NEC, PsiQuantum, and NTT), large telecommunications providers (including Deutsche Telekom and British Telecom) and research institutions/organizations (including Nanjing University of Posts and Telecommunications, Fraunhofer, Soochow University, Delft University of Technology, and University of Chicago). Large, international technology companies in particular tend to protect their R&D with patents, which is why they are well-represented in this list. Startups, on the other hand, often place their (financial and workforce) focus on technological development and thus do not appear in such analyses or not as prominently.

Table 4: Institutions with the highest number of QCom-related, transnational patent applications in the years 2020-2023 (top-20)

Institution (country)	Number of patent applications (2020-23)
Toshiba (JP)	50
LG Electronics (KR)	42
Deutsche Telekom (DE)	29
Arqit (UK)	25
Nanjing University of Posts and Telecommunications (CN)	24
NEC (JP)	21
PsiQuantum (US)	20
British Telecom (UK)	19
Fraunhofer (DE)	19
NTT (JP)	18
Soochow University (TW)	18
Delft University of Technology (NL)	14
Ericsson (SE)	13
Thales (FR)	13
University of Chicago (US)	13
IBM (US)	12
IonQ (US)	12
NICT (JP)	12
Qubit Moving and Storage (US)	12
Terra Quantum (CH)	12

Almost 40 percent of the institutions with at least three QCom-related patent applications between 2020 and 2023 are research institutions (Figure 23), which are also responsible for more than 30 percent of the patent applications by institutions (three or more QCom-patents) in this period. This underlines the early development stage of QCom technologies, during which R&D institutions play a major role in technology development.

Figure 23: Shares of industry and research institutions with ≥ 3 QCom-related patent applications between 2020 and 2023 and their shares in the sum of patent applications in this period



To analyze European activities in QCom patenting, we listed the European institutions with at least five QCom-related patent applications in the last four years of the period analyzed (Table 5). Again, technology companies (including Arqit, Ericsson, Thales, Terra Quantum, ID Quantique, IBM, and Quantum Optics Jena) and large telecommunications providers (including Deutsche Telekom and British Telecom) are well-represented. Although the QCom-related patenting activities are still partially driven by research institutions/organizations (including Fraunhofer, Delft University of Technology, French National Centre for Scientific Research – CNRS, Institute of Photonic Sciences – ICFO, Catalan Institution for Research and Advanced Studies – ICREA, and University of Warsaw), patenting activities of industry is becoming more prominent. Approximately one third of the institutions with at least three QCom-related patent applications are research institutions/organizations – less than a few years ago. And they are only responsible for less than one third of the patent applications (three or more QCom-patents). This implies that, in Europe, still many R&D institutions are actively working on QCom, but in terms of patent numbers they cannot keep up with the telecommunications and technology companies. Industry is becoming more and more active in patenting in the field of QCom, which could be an indication of a successful technology transfer from science to industry.

Table 5: Institutions from EU28(+CH) with at least three QCom-related, transnational patent applications between 2020 and 2023

Institution (country)	Number of patent applications (2020-23)
Deutsche Telekom AG (DE)	29
Arqit Limited (UK)	25
British Telecommunications plc (UK)	19
Fraunhofer Society (DE)	19
Delft University of Technology (NL)	14
Ericsson (SE)	13
Thales Group (FR)	13
Terra Quantum AG (CH)	12
ID Quantique SA (CH)	11
IBM Deutschland GmbH (DE)	9
Quantum Optics Jena GmbH (DE)	9
Airbus SAS (FR)	8
Elmos Semiconductor SE (DE)	8
Huawei Technologies Düsseldorf GmbH (DE)	8
French National Centre for Scientific Research (FR)	6
QBird BV (NL)	6
Bundesdruckerei GmbH (DE)	5
Institute of Photonic Sciences (ES)	5
Heqa Security Ltd. (UK)	5
Catalan Institution for Research and Advanced Studies (ES)	5
QuantLR Ltd. (IL)	5
Russian Railways (RU)	5
University of Warsaw (PL)	5

To conclude, Europe and Germany hold a good position in QCom-related patenting activity. The trend of the last years has continued with the EU contributing the majority of transnational QCom-related patent applications. A slight shift towards more patenting activity from industry in Europe, compared to recent years, can be observed.

5.3 Meta-Market Report Analysis

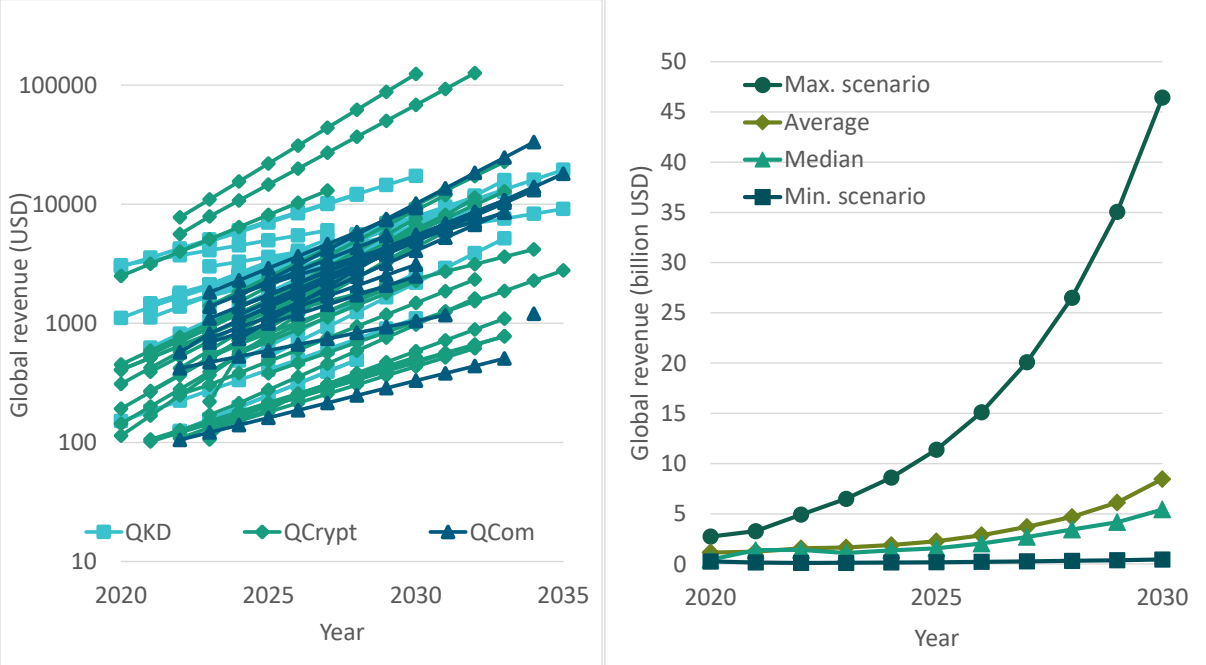
Assessing the global market size of an emerging field of technology is very challenging. Unlike established markets that are often dominated by large players and closely followed by trade associations, activities in emerging markets are typically driven by small companies, startups and R&D institutions. This makes a realistic assessment of the global market difficult.

In order to address this topic, we compare the widely diverging results of market reports and forecast scenarios (meta-market analysis). Access to commercial market reports is typically cost-intensive, which limits the possibilities of comparative analyses. However, many market report providers release limited information for advertising purposes, which is available free of charge. This publicly available information usually includes aggregated market revenue data, growth rate forecasts and the names of relevant companies in the field. We collected and analyzed relevant data from 136 market reports [157–291] published between 2019 and April 2025 on quantum communication, quantum cryptography, and quantum key distribution.

Market size and forecast trends

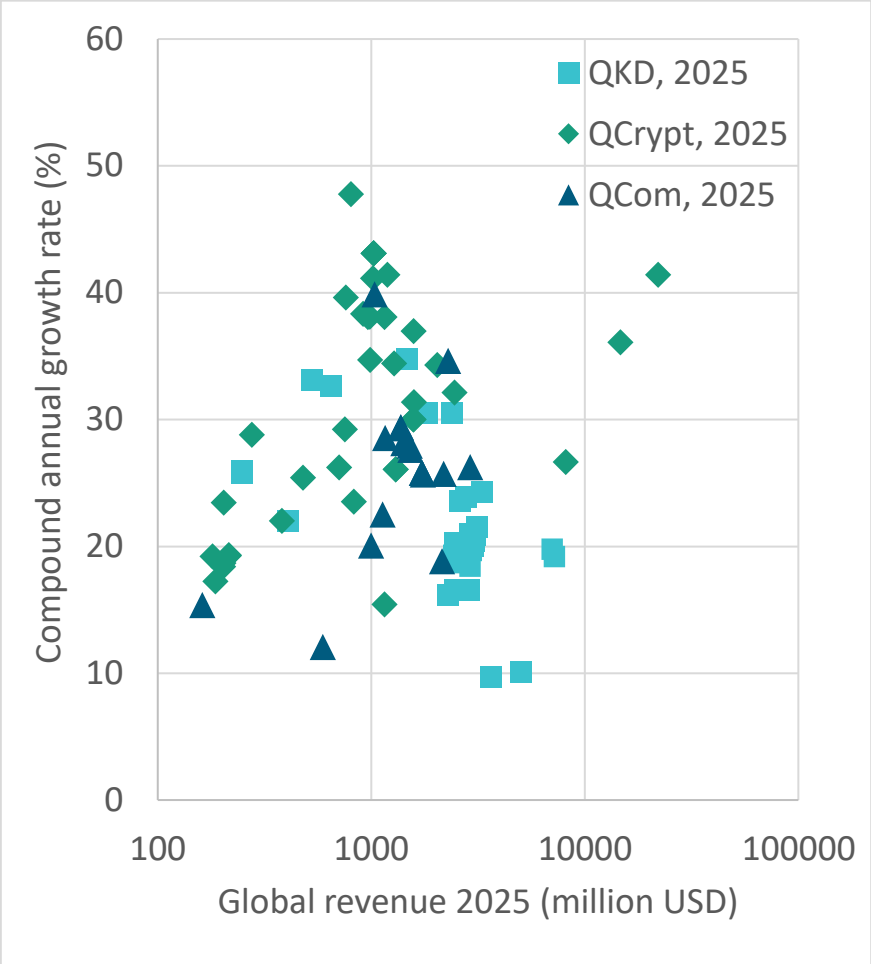
According to the analyzed market reports, global revenue in the markets for quantum communication, quantum cryptography, and quantum key distribution is expected to grow significantly in the coming years (Figure 24). Compound annual growth rates (CAGR) of between 12 and 41 percent are predicted, although the majority of studies expect CAGR of between 15 and 25 percent. The forecasted and current revenue figures differ significantly between market reports and range between 140 million and 15.6 billion dollars in 2024 and between 330 million and 124 billion in 2030 (left-hand graph in Figure 24). These extreme values can be considered rather unrealistic, and the highest estimates, in particular, seem unrealistically high for such a novel technology. To obtain a good overview of all these revenue forecasts, we calculated the median, the average, and a maximum and a minimum scenario (median of top 4 and bottom 4, respectively, see right-hand side of Figure 24). The median calculation results in global revenue values of 1.4 billion in 2024 that increase to 5.4 billion in 2030. These values as well as the average forecast figure slightly decreased in the recent market reports, compared to earlier predictions. Future development is more likely to be somewhere between the highest and lowest predictions, possibly close to the mean or median curve.

Figure 24: **Revenue estimates and forecasts from the 136 analyzed market reports on the global quantum communication market between 2020 and 2035 (left) and results of our calculations (right)**



The market reports analyzed refer to quantum communication, quantum cryptography, and quantum key distribution (QKD), respectively. These technology classes are certainly not identical and QKD can be considered a sub-class of the other two. In most market reports, however, no clear definition of the class of technologies is given—at least not in the free previews. In any case, the global market forecasts of the three classes appear very similar and no clear distinction between them can be made from either the revenue figures, or the CAGR values (Figure 25).

Figure 25: **Comparison of the global revenue estimates and CAGR figures from the analyzed market reports on quantum communication (QCom), quantum cryptography (QCrypt) and quantum key distribution (QKD). No clear distinction between the three classes of technology can be made based on the forecast figures.**



Relevant players and countries

Most of the market report providers mention companies that are active in the field of quantum communication, quantum cryptography, or quantum key distribution in the preview of their report. Analyzing the companies mentioned in the 136 reports leads to a ranking of the company names mentioned (Table 6). This analysis does not indicate which company is the technology leader or most active in the field, but rather which companies are considered relevant by market analysts and are mentioned accordingly in their market reports. It also has the limitation that it only considers English-language market reports. Therefore, only companies with publicly available information in English will have a significant number of mentions, as the majority of market report providers do not extend their search beyond the English language.

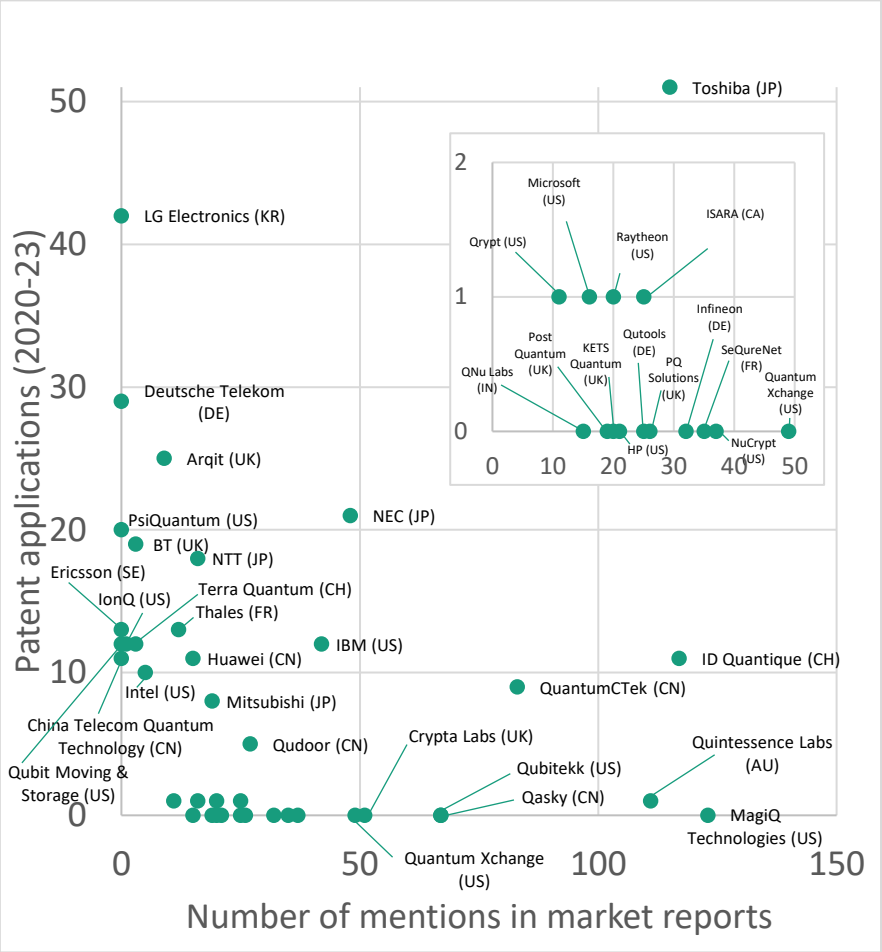
Table 6: Companies with the highest number of mentions in market reports on QKD, QCom and QCrypt (top-20)

Company/Institution (country)	Number of mentions
MagiQ Technologies (US)	123
ID Quantique (CH)	117
Toshiba (JP)	115
Quintessence Labs (AU)	111
QuantumCTek (CN)	83
Qubitekk (US)	67
Crypta Labs (UK)	51
Qasky (CN)	50
Quantum Xchange (US)	49
NEC (JP)	48
IBM (US)	42
NuCrypt (US)	37
SeQureNet (FR)	35
Infineon (DE)	32
Qudoor (CN)	27
PQ Solutions (UK)	26
Qutools (DE)	25
ISARA (CA)	25
Hewlett-Packard (US)	21
Raytheon (US)	20

When analyzing the country of origin of the mentioned companies that were mentioned at least six times in the market report, the highest number come from the USA (13), the UK (8), China (7), Japan (5), France (5), and Canada (4). The large numbers of companies from English-speaking countries again indicates the bias toward English-language companies.

In contrast to the patenting activity of companies, their mentions in market reports reflect how their activity in the field of technology is perceived by others. Figure 26 compares the number of mentions with the patenting activity of the relevant companies. It is surprising that some of the top patent applicants including LG Electronics, Deutsche Telekom, and Arqit are not mentioned frequently in the analyzed market reports (and some not at all). In contrast, some of the frequently mentioned companies such as MagiQ Technologies, Quintessence Labs, and Qasky did not show up in our patent analysis, or only with very few patent applications. Toshiba, NEC, QuantumCTek, and ID Quantique are companies with both significant patenting activity and frequent mentions in the market reports.

Figure 26: Comparison of the number of patent applications and the number of mentions in market reports of companies with a minimum of 15 mentions or a minimum of 10 patent applications



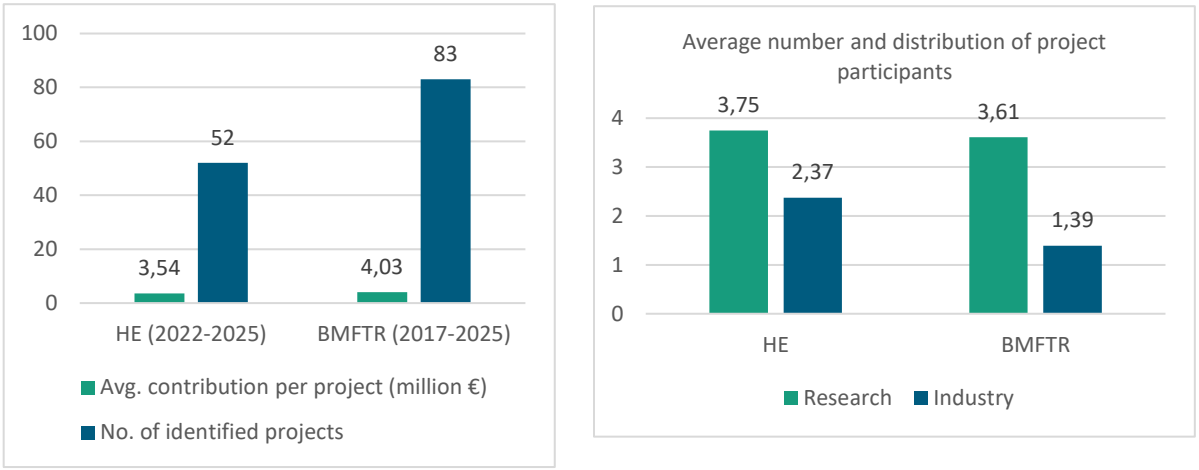
5.4 Project Monitoring

Projects conducted in a field of science or technology are regarded as a good indicator of ongoing R&I activities, research and industry trends as well as of the innovation policies in a country or region. Accordingly, we investigated recent projects funded in quantum communication as a quantitative measure of the technology landscape. For this report, we conducted analyses for Germany and the EU.

Understanding Germany's R&I landscape in quantum communication is of high significance for the objectives of this monitoring report. Additionally, Germany is a leading country in research and innovation in Europe and globally. Accordingly, quantum communication R&D programs in Germany provide a good indication of the span and scale of relevant activities across technologically advanced countries worldwide. The total expenditure on R&D in Germany in 2023 was reported to be about 132 billion euros, equal to 3.13% percent of the country's gross domestic product (GDP) [292]. The German federal government provided 26.1 billion euros of R&D expenditure in 2024, of which 13.6 billion euros was allocated by the Federal Ministry of Research, Technology and Space (BMFTR)[2]. BMFTR is one of the major R&I funding organizations in Germany and often assigns the largest share of the German government's expenditure on R&D. Therefore, BMFTR-funded projects in quantum communication were selected for analysis in this study.

The EU was selected as a leading research funder on a global scale, supporting large-scale R&I activities and initiatives within its various funding programs and frameworks. In 2024, the EU's total R&D expenditure was reported to be about 403 billion euros, corresponding to 2.24 percent of the Union's GDP [293]. In our first monitoring report, we analyzed EU framework program Horizon 2020 over its full funding period; in this report, we update the analysis by examining projects in quantum communication of the current framework program Horizon Europe (HE).

Figure 27: Number and average funding per project of identified BMFTR and Horizon Europe (HE) projects (left). Average number of project partners from industry and research institutions (right).



We identified 83 projects funded by the BMFTR in the area of quantum communication as well as 52 projects funded by EU under HE framework program, respectively (Figure 27, left). The identified

[2] In the first monitoring report, this ministry was still called Federal Ministry of Education and Research (BMBF). It was renamed in May 2025.

BMFTR projects have start times ranging from 2017 to mid-2025 and end times ranging from 2019 to 2027. The average BMFTR contribution per project is about 4.03 million euros. EU projects funded under Horizon Europe (2021–2027) in our sample started between 2022 and 2025 and end between 2024 and 2030, with an average EU contribution of 3.54 million euros per project.

Project participants in both the BMFTR and EU programs are more often from universities and research and technology organizations as shown in Figure 27 (right). On average, BMFTR-funded projects include one industry participant. Under HE, industry participation is higher, with more than two industry partners per project.

Figure 28: Distribution of projects and estimated annual funding

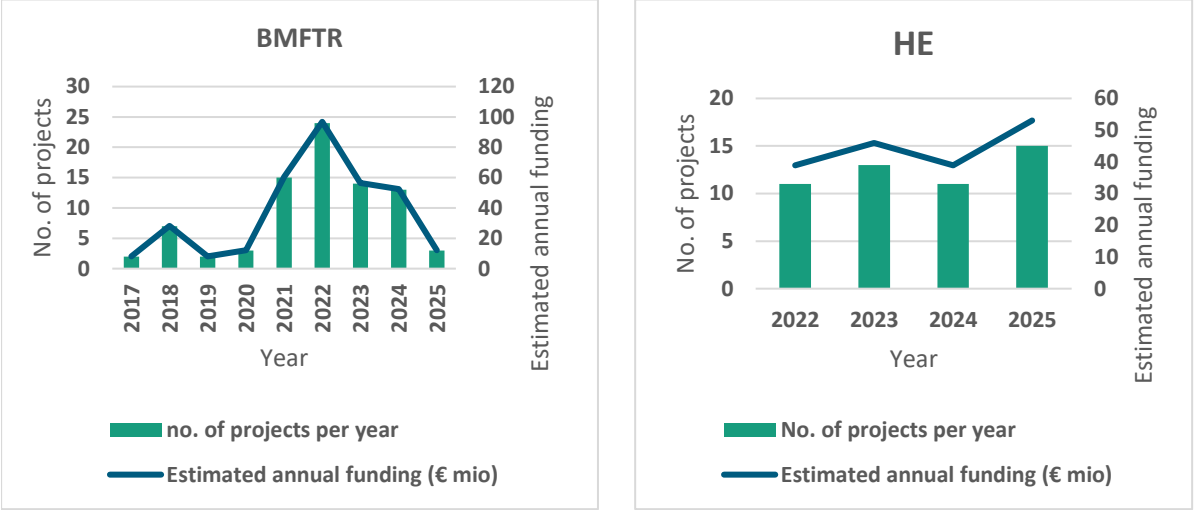
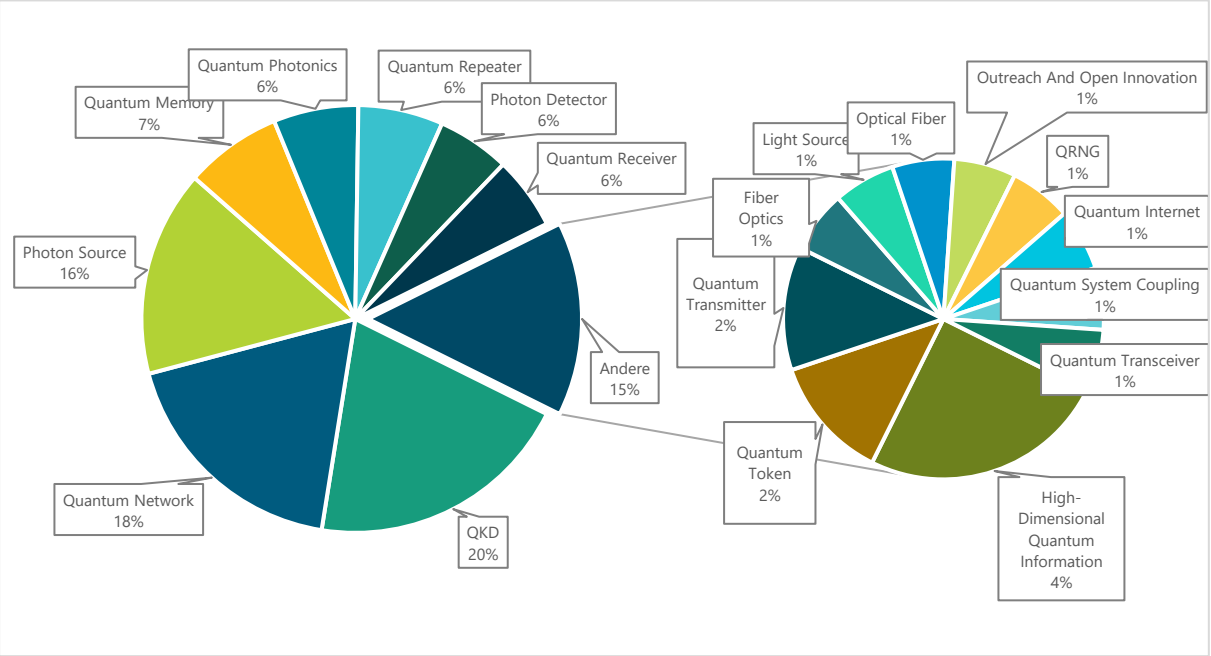


Figure 28 shows the number of projects funded and an estimation of the allocated budget based on multiplying project counts by average budgets for BMFTR and HE. The charts show BMFTR ramping up strongly from 2021, peaking in 2022, and remaining elevated in 2023–2024. The abrupt reduction in 2025 reflects mid-year data and the end of various projects from the call „Innovationshub für Quantenkommunikation" (engl. Innovation hub for quantum communication). In 2025 a new call was opened called „Transfer und Netzintegration der Quantenkommunikation" (engl. transfer and network integration of quantum communication). Hence, new projects are anticipated for 2026. HE builds steadily from its 2022 start through 2025, with rising project activity and higher average budgets than under H2020 (1.41 million euros). Overall, both, BMFTR and EU, signal sustained momentum in quantum communication R&I.

An analysis was also performed on the topics of the projects funded in Germany and the EU. Figure 29 shows the distribution of topics addressed by the identified BMFTR projects. Most projects focus on one topic, while a small number of projects address two topics according to the reported objectives and approaches.

Figure 29: Distribution of topics in the 83 identified projects funded by the BMFTR



As the figure indicates, a large proportion (20%) of BMFTR projects focus on QKD. The most relevant sub-topics within QKD are free-space QKD (35%), general QKD (22%), and QKD post-processing (9%). Besides QKD, the main topics are quantum networks (18%), photon sources (16%), quantum memory (7%), and quantum photonics, quantum repeaters, photon detectors, and quantum receivers, each with a 6% share. Topics such as high-dimensional quantum information, quantum tokens, quantum transmitters/transceivers, light sources for CV-QKD, quantum internet, QRNG and further areas are covered by a small share of projects (about 1–5%).

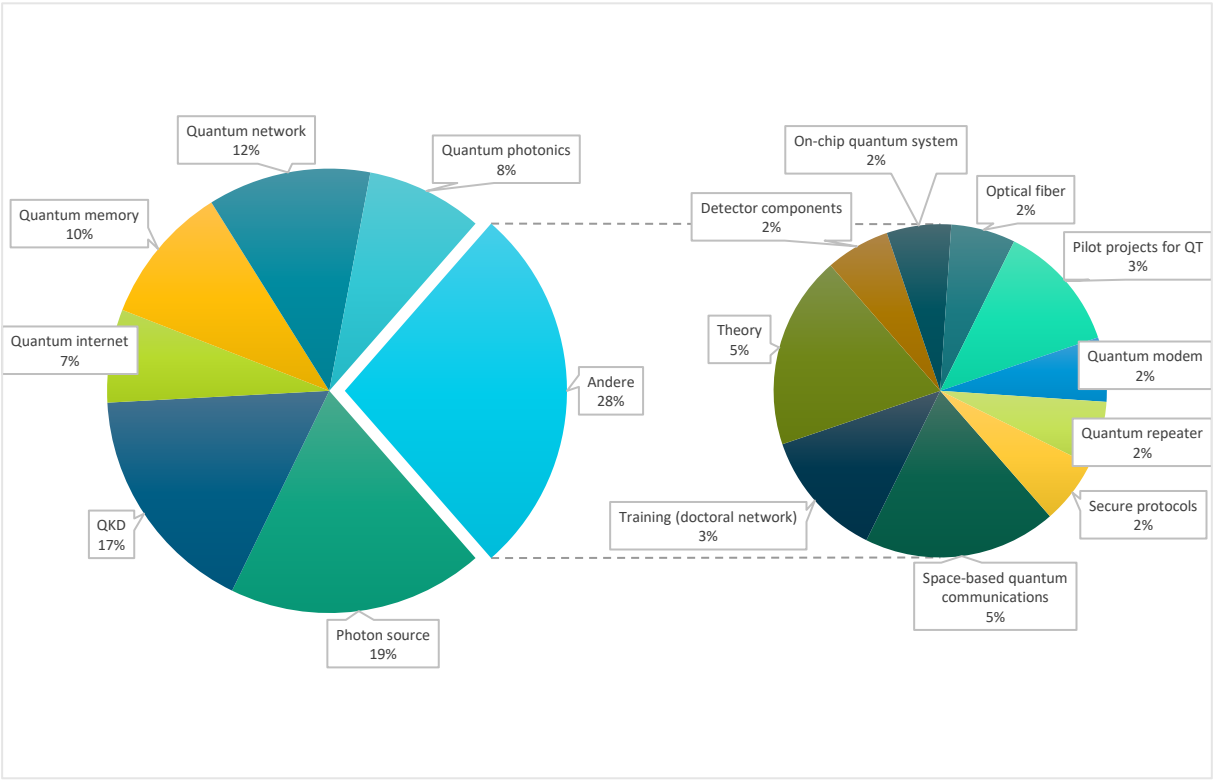
Beyond BMFTR, other German ministries also finance quantum communication R&I. The Ministry for Economic Affairs and Energy (BMWE) has financed space-oriented quantum communication (e.g., QKD transmitters and payloads, optical memories, photon sources for satellite links) through multi-year projects in recent years [294]. Additionally, the Ministry of Defense (BMVg) finances security-focused and quantum communication initiatives (e.g., infrastructure [295], QKD components [296] and quantum-secure encryption [297]), including activities at University of the Bundeswehr Munich.

Figure 30 shows the distribution of subjects among the identified EU projects funded under HE. The first pie chart shows that photon sources (19%) and QKD (17%) are the largest topics, followed by quantum networks (12%), quantum memory (10%), quantum photonics (8%), and the quantum internet (7%). Together, these six topics account for about 73% of all counted topics. The second pie chart expands the "Other" segment (about 27%, 16 projects), which includes space-based quantum communications (3), theory (3), training/doctoral networks (2), and pilot projects for quantum technologies under the Framework Partnership Agreement (FPA) model (2) including Qu-Pilot and Qu-Test projects. Together, these two projects, each with an EU contribution of approximately 19 million euros, provide complementary EU infrastructure for quantum technologies. Qu-Pilot (2023-2026) provides open access pilot line services to design, fabricate, assemble, and package quantum components and subsystems across multiple platforms, helping industry and SMEs prototype and scale products while building European supply chains. Qu-Test (2023-2026) comple-

ments this with a pan-European testing and validation network that offers standardized characterization, benchmarking, and interoperability testing for quantum devices and systems before deployment [298].

Within the QKD area, the main sub-topics are free-space QKD, satellite QKD and related protocols, CV-QKD and CV-QKD protocol development, fiber-based QKD, post-processing, and secure protocol stacks. Share of QKD projects is prominent for both funders, while there are some differences in the other topics. For example, the quantum internet is a topic with high strategic priority for the EU. The first phase of the Quantum Internet Alliance [299], as a large-scale initiative within the Quantum Flagship was funded under H2020 framework program with a budget of about 10 million euros.

Figure 30: Distribution of topics in the 52 identified projects funded by Horizon



5.5 International Situation and Initiatives

5.5.1 International Funding Initiatives

This section provides an overview of the funding initiatives and strategic goals for QCom technologies of the key international players: Germany, EU, China, USA, UK, Japan, Canada, South Korea, and India.

Since 2023, the last year analyzed in the first monitoring report, many countries have updated their quantum strategies (Germany, EU, USA in preparation) or released additional documents to outline the specific objectives for implementing their main strategies (China, UK, Japan, Canada). Some countries further promise to prepare instruments to promote industrial applications. Another important focus is that satellite projects are increasingly highlighted in strategic documents (Germany), or national space agencies are more explicitly integrated in the countries' quantum strategies/projects (USA, Japan).

Germany: In April 2023, the German Cabinet adopted a strategic document "Quantum Technologies Conceptual Framework"[300], announcing funding of approx. 2.18 billion euros for quantum technologies from 2023 to 2026, complemented with 0.85 million euros to the activities of science organizations. Following the change in administration, the government newly published the "Hightech Agenda Deutschland (HTAD)," identifying quantum technologies as one of six key areas. While this agenda anticipates an investment of at least 18 billion euros by 2029, the specific allocation for quantum technologies remains unclear [301].

QCom R&D activities in Germany are currently funded mainly by two framework programs of the Federal Ministry of Research, Technology and Space (BMFTR): "Digital. Sicher. Souverän" and "Quantensysteme". The "Digital. Sicher. Souverän" program focuses on secure and innovative IT-security solutions for citizens, businesses and the nation. In this context, QCom is considered a key technology for enhancing IT-security. In contrast, the focus of the "Quantensysteme" program does not explicitly emphasize QCom technology [302]. Nevertheless, certain projects under the research program address QCom, such as through the funding lines to support international research cooperation in quantum technologies.

Although our quantitative analysis does not include specific data, it is worth noting that state governments in Germany also play a role in supporting projects. For example, the state government of Thuringia provided 11 million euros to the Fraunhofer IOF to build a quantum communications infrastructure [303].

Germany's strategic goals in QCom:

The Hightech Agenda Deutschland (HTAD) outlines four objectives for quantum technologies, one of which focuses on establishing an innovation ecosystem for QCom [20]. The HTAD-Roadmap for quantum technology published in May 2026 includes the following QCom-related milestones with specific timelines [304]:

- Comissioning of the second QUBE research satellite [305] (2026)
- Completion of the QuNET initiative, which is a German research contribution for EuroQCI [54] (2026)
- Launch of an innovative networking platform for technology transfer in QCom in Germany (2027)
- Support for early-career research groups for the innovation pipeline through the second Grand Challenge of Quantum Communication (2028)
- Key elements for long-range terrestrial quantum communication implemented with the first technology demonstration of quantum repeaters (2028)
- Quantum information networks established in Germany (2030)

Towards these goals, research actors have reported several achievements. For example, the QuNET initiative mentioned in the roadmap aims to develop a highly secure communication systems based on state-of-the-art quantum technology in Germany, with a planned funding allocation of 125 million euros over a period of seven years. In 2023, the researchers achieved a key rate in the kilobit range per second in daylight over a hybrid (free-space and fiber) test track in an urban area of Jena [306]. In September 2024, QuNET started the main phase of the second key experiments to connect users in the Berlin metropolitan region via QKD-based systems, featuring 125 km of fiber-optic and free-beam connections [307]. Furthermore, a flight experiment between Oberpfaffenhofen and Erlangen was successfully completed in 2025 [308].

With regard to satellite-based QKD, the small research satellite QUBE was launched in 2024 with the objective of validating hardware for satellite quantum communication [305, 309]. In May 2026, QUBE II satellite, which plans to demonstrate the first-ever quantum key exchange between a CubeSat and a ground station, was successfully launched into orbit [310].

European Union: For the EU, QCom is funded by the Horizon 2020/Horizon Europe programs (focusing on R&D) and EuroQCI [47] (focusing on infrastructure and technology deployment).

The identified EuroQCI projects and calls provide the following budget for the terrestrial segment:

- 181 million euros under the Digital Europe Programme, which includes industrial projects, national projects and a coordination and support action to link them all [311].
- 90 million euros under the Connecting Europe Facility to support the interconnection of national quantum communication infrastructure networks between neighboring countries, as well as the interconnection of ground and space segments of the EuroQCI [245].
- 16 million euros for the NOSTRADAMUS project, which aims to establish a testing and evaluation infrastructure.

The European Space Agency (ESA) as well as national funds also contribute to the initiative, although specific budget data is not officially provided.

EU's strategic goals in QCom: The long-term vision of the EU is the development of a quantum internet throughout Europe. The EU Quantum Flagship has delineated its R&D priorities for different quantum technologies, including QCom, by creating a roadmap through the formulation of the Strategic Research and Industry Agenda (SRIA). The strategic objectives outlined in the latest SRIA (SRIA 2030) include, on one hand, the development of component technologies necessary to achieve its long-term vision of a quantum internet based on entanglement-distribution using quantum repeaters and quantum memories. On the other hand, the document also emphasizes the deployment of more mature technology, such as building prepare-and-measure QKD networks and the scaling of QKD solutions [312].

The EuroQCI aims to establish a secure quantum communication infrastructure spanning the entire EU. It will make use of innovative technologies developed by Horizon projects, particularly the OpenQKD project under Horizon 2020. In addition, the European Commission and ESA are working together to specify a first-generation constellation of EuroQCI satellites. The first prototype satellite, Eagle1, is scheduled to be launched in 2026.

In July 2025, the European Commission adopted the communication for the **Quantum Europe Strategy,** to make Europe a global leader in quantum technologies by 2030. In the area of QCom, the following three objectives are mentioned [313]:

- Deploying the first EU-interconnected experimental quantum terrestrial and space secure communication network by 2030
- Publishing a Quantum Communication Roadmap by 2026
- Launch a pilot facility for the European Quantum Internet by 2026

China: One of the major funding programs to support quantum information research during the 13th Five-Year-Plan period (2016-2020) was the "National Key R&D Program" of the Ministry of Science and Technology (MoST). Pan et al. reported that approx. 337 million dollars was spent on "Quantum Control and Quantum Information" projects under the program from 2016 to 2019, but it was not possible to determine the proportion of funding for QCom research [314]. During the 14th Five-Year-Plan period (2021-2025), quantum research in China was further supported through "Major Projects" under the Innovation 2030 program. However, as of September 2025, its funding guidelines have not been made publicly available, and the details are not clear.

In addition to this, the construction of the National Laboratory of Quantum Information Science was started in 2017 with an initial investment of 7 billion yuan (approx. 900 million euros). Some media also reported its plan on even larger investment [315], but experts have expressed skepticism

regarding the scale of the investment [316]. The National Laboratory not only functions as a research facility but also leads "Major Projects" as a national project manager.

In China, the central government is not the sole source of funding. Provincial governments in China also play an important role in R&D funding, such as with the new Anhui Quantum Science Industry Development Fund, which was planned to devote 10 billion yuan (approx. 1.3 billion euros) for quantum technologies [247]. In addition, state-owned enterprises also invest in QCom; China Telekom, which has a controlling stake in QuantumCTek, plans to invest over 10 billion yuan (approx. 1.3 billion euros) over the next years [317].

While the exact total amount of public funding in China is unclear, there is no doubt that China has made significant efforts and achieved notable milestones in QCom technologies. For instance, in August 2016, China launched the world's first quantum communications satellite called "Micius (Mozi)" and achieved the first intercontinental QKD in 2017. The first Micius satellite was developed at an estimated cost of 100 million dollars within China's Strategic Priority Programme on Space Science [318] as part of the Quantum Experiments at Space Scale (QUESS) project. Another important achievement is the establishment of a quantum communication network, currently spanning over 10,000 km, incorporating 145 fiber backbone nodes and 20 metropolitan networks and deploying 6 ground stations linked with a microsatellite [37].

Recently, China has demonstrated a strong commitment to expanding its communication network with international partners. In 2024, the establishment of a QKD link utilizing the Micius satellite between ground stations in Zvenigorod, Russian Federation, and Nanshan was reported [319]. Additionally, a Chinese research team successfully transmitted quantum-encrypted signals over a distance of 12,900 km from China to South Africa, employing a lightweight microsatellite, called Jinan-1. [320]

China's strategic goals in QCom: Quantum technology is included as one of the prioritized frontier technologies in the 14th Five-Year Plan in China [321], although a QCom-specific strategic objective is not mentioned directly in the plan. In 2025, the Ministry of Industry and Information Technologies has released its innovation tasks for future industry, which includes the objectives with specific performance indicators for distributed quantum key resources [322].

In 2014, the influential Chinese quantum researcher Prof. Jian-Wei Pan, who led the launch of the Micius satellite, stated that China would demonstrate an Asia-Europe intercontinental QKD in 2020, which was actually realized in 2017. At that time, Prof. Pan also said that China aims to build a global quantum communication network by 2030 [250]. Recently, he presented a more expedited vision, stating that "China is aiming to launch an ultra-secure global communications service by 2027", leveraging its quantum satellite and ground-based networks [323]. The Pan group also plans to deploy a satellite constellation and a large geostationary quantum satellite that is scheduled for launch in the late 2027 or early 2028 [324].

United States: Since the enactment of the National Quantum Initiative (NQI) Act in 2018, followed by the CHIPS and Science Act in 2022, the US government has recently further intensified the investment in quantum research. According to the most recent budget report, the US government has designated approximately 6 billion dollars for quantum information science within relevant agencies for the fiscal years (FY) 2019 to 2025. Nearly half of this allocation (approximately 3.2 billion dollars) is directed towards activities authorized by the NQI, in addition to baseline R&D activities [8]. The NQI Act authorizes the budget for the National Science Foundation (NSF), the Department of Energy (DOE), and the National Institute of Standards and Technology (NIST).

The NQI categorizes its activities into five different component areas, one of which is "Quantum Networks and Communications (QNET)", accounting for approximately 10% of the NQI budget. Examples of the NQI instruments for QNET R&D are:

- NSF selected the University of Arizona for a five-year, 26 million dollars grant with an additional five-year option for 24.6 million dollars to establish and lead the Center for Quantum Networks.
- DOE awarded a total of 25 million dollars to two testbeds projects to develop a quantum internet.

In addition to the R&D activities in the NQI-authorized agencies, the Defense Advanced Research Projects Agency (DARPA) launched the Quantum-Augmented Network program in 2024, aiming for the integration of quantum communications into classical networks [325].

After the expiration of the authorization for some R&D activities in the NQI Act in 2023, its reauthorization and amendment are under discussion, as the Act was originally framed as a ten-year initiative. From 2024 to 2025, a couple of relevant bills have been introduced but not enacted:

- The National Quantum Initiative Reauthorization Act promises 2.7 billion dollars from FY 2025 to FY 2029 for R&D activities. In addition to the above-mentioned agencies, the National Aeronautics and Space Administration (NASA) will be authorized for the budget, in particular for the research on quantum satellite communication. The new Act will also focus on the practical application, for example, with the creation of quantum testbeds, which is recommended by the NQI committee [326].
- DOE Quantum Leadership Act of 2025 proposes 2.5 billion dollars for five years to reauthorize and expand the DOE's activities, including those in Qcoms and networking [327].
- Quantum Sandbox for Near-Term Applications Act of 2025 aims to establish a public-private partnership to accelerate quantum applications, including QCom [328].

USA's strategic goals in QCom: A Strategic Vision for America's Quantum Network, published as one of the strategic documents under the NQI, outlines the US's short- to medium-term vision for quantum network technologies: [329]

- Over the next five years, companies and laboratories in the US will demonstrate the foundational science and key technologies to enable quantum networks and identify the potential impacts and improved applications.
- Over the next twenty years, quantum internet links will leverage networked quantum devices to enable new capabilities not possible with conventional technology.

To develop a technology roadmap, the DOE hosted the Quantum Internet Blueprint Workshop in 2020, identifying scientific application areas, priority research directions and key milestones to facilitate an eventual national quantum internet [330].

United Kingdom: The UK National Quantum Technologies Programme (NQTP) was launched in 2014, representing a one-billion-pound partnership between government, academia, and industry. QCom-related projects and programs were identified on the NQTP website, providing insights into its research focus [5]. These include the Quantum Communication Hub (2014-2024 with 49.8 million pounds), a quantum satellite project with Singapore (with 10 million pounds), and 38 projects supported by the Industrial Strategy Challenge Fund.

As the culmination of the 10-year initiative in quantum communication, in 2025, the research team from the Universities of Bristol and Cambridge reported their success in demonstrating quantum communications network over a fiber distance of over 410 km, supporting BBM92 and two DV-QKD protocols [331].

In the final year of the NQTP initiative, the UK government published its new strategy for the period 2024–2033 with plans to invest more than 2.5 billion pounds (approx. 2.9 billion euros) in QT. This is more than double the amount allocated in the previous strategy. This means that the funding budget in the UK is expected to increase significantly in the near future [255].

UK's strategic goals in QCom: The UK Quantum strategy has established four goals: 1) world-leading research and skills; 2) supporting business; 3) driving the adoption of quantum technologies, and 4) leading quantum regulation and protecting the sector. These goals have clearly defined targets to be achieved by 2033 (e.g., "By 2033, the UK will maintain a top 3 position in the quality of scientific publications, whilst increasing the volume.").

As the UK Innovation Strategy highlights the mission-oriented innovation approach, the government has worked to define the long-term and time-bound Quantum Strategy Missions to bring the impacts to the economy and society. Among the five mission headlines, Mission 2 states that "By 2035, the UK will have deployed the world's most advanced quantum network at scale, pioneering the future quantum internet." Another Mission also mentions the potential use of networked quantum sensor technology [332].

Japan: The Japanese government released its Quantum Technology Innovation Strategy in 2020 (FY2019[3]) as a cross-ministerial strategy. Although the document itself does not provide specific information on the expected amount of public funding for a specific period, the government has published a list of relevant programs/projects along with the annual budget allocation. For this analysis, we focused on those programs/projects categorized as "quantum cryptography" or "quantum security" topics and summed up their budgets from FY2018 to FY2025.

The majority of public funding for QCom in Japan, more than 90 percent, has been allocated to projects led by the Ministry of Internal Affairs and Communications (MIC). Since FY2018, the MIC has supported various projects such as testbed development, quantum cryptography in satellite communications, R&D for the establishment of a global quantum network, and elemental technologies for the quantum internet. However, since 2024, a project focused on satellite quantum encryption communication has been supported not directly by MIC funding, but through the Space Strategy Fund established at the Japan Aerospace Exploration Agency (JAXA), with a maximum funding of 14.5 billion yen (approx. 86 million euros) over a period of five years.

Another important national program is the Cross-Ministerial Strategic Innovation Promotion Program (SIP). In the current phase of the SIP, the emphasis is on the development of the "Quantum Secure Cloud" and its use cases, which involves the integration of quantum cryptography, secret dispersion, and secret computation [333].

Japan's strategic goals in QCom: The Quantum Innovation Strategy includes technology roadmaps for key areas. With respect to QCom, there are three roadmaps: one roadmap for communications and cryptography, one for quantum repeaters, and one for networking technologies. The goals for each area are:

- Demonstration of 10 Mbps quantum cryptographic communication in a metropolitan area by 2025, expansion to intercity scale (long-distance application) by 2030.
- Quantum entanglement distribution among three points by 2030, key generation beyond 1 kbps using quantum entanglement distribution by 2040, realization of quantum computer network by 2040.

[3] Japanese fiscal year (FY) 2019 starts in April 2019 and ends in March 2020

- Demonstration of a mesh network in urban areas by 2030, realization of a global quantum cryptography network by 2040, demonstration of deep space quantum communication and a quantum internet by 2040.

Since 2023, the government has published a couple of strategic documents to show their visions and action items to realize the benefits of quantum technologies for society and industry. According to the country's Strategy of Quantum Future Industry Development, efforts will be made for the application of quantum security networks, for example, by creating use cases, promoting the use in public authorities, and supporting [334].

South Korea: In 2023, South Korea unveiled its first comprehensive quantum strategy, pledging more than 3 trillion won (approx. 2 billion euros) in public-private co-investment by 2035 to establish itself as a global hub of the quantum economy. According to the Ministry of Science and ICT, the budget related to quantum science and technology in 2025 was 198 billion won, representing a 54.1% increase from the previous year [335].

In terms of QCom, the strategy aims to develop a 100 km-scale quantum network in the 2030s and promote intercity experimentation [257]. In 2025, the government initiated the "Quantum Information Communication Engineering Technology Development Project", which aims to promote domestic production of component technologies and self-reliance of technological development.

The National Convergence Network Project is one example of recent achievements in South Korea. In 2022, SK Broadband and IDQ, a Geneva-based quantum communication system provider, completed the first phase of this project. The project aims to secure the communications network of 48 Korean government organizations spread across the country. In this first phase, the companies developed a QKD network infrastructure with a total length of 800 km [336]. Backed by this experience, the Korean National Intelligence Service provided ID Quantique's QKD system with a national security certification in 2025, which is the first national security approval globally [337]. However, this certification is not comparable to a European certification.

Canada: The government of Canada released a new National Quantum Strategy in 2022 with one of its three missions focused on the development of QCom technologies and post quantum cryptography [338]. In order to identify the milestones necessary for accomplishing the NQS, NQS roadmaps were developed and published in 2025. Regarding QCom, several action items have been delineated pertaining to R&D activities, the creation of testbeds, the identification of use cases, the establishment of international standards and partnerships, as well as addressing supply chain challenges and enhancing domestic capacities [339].

Prior to releasing this strategy, Canada had already invested over one billion Canadian dollars (approx. 0.6 billion euros) in quantum science between 2012 and 2022. One of the key national QCom projects in Canada is the Quantum Encryption and Science Satellite mission (QEYSSat), which started in 2017 led by the Canadian Space Agency. Although the total investment in the project is not clear, it has been reported that the American corporation Honeywell was awarded a contract worth 30 million Canadian dollars (approx. 20 million euros) for the design and implementation phases of the QEYSSat mission [340]. The satellite is scheduled for launch in 2026 and will connect ground stations more than 400 km apart using BB84 and BBM92 protocols [341].

India: In April 2023, the Union Cabinet of India approved the National Quantum Mission with a total cost of 60 billion rupees (approx. 0.6 billion euros) from 2023/24 to 2030/31. The expected deliverables of the Mission include satellite-based secure quantum communications between ground stations over a range of 2000 km within India, long-distance secure quantum communications with other countries, intercity QKD over 2000 km, and a multi-node quantum network with quantum memories. The mission established four thematic hubs in top academic and national R&D

institutes [342]. The Thematic Hub for QCom, IITM CDOT Samgnya Technologies Foundation was initiated at Indian Institute of Technology Madras. The Hub not only promotes R&D activities in the academic field but also opened a call for proposals to support innovative startups [343].

India seems positive to deploy QCom technology in the public sector. In 2024, the Indian Army signed the procurement contract for QKD technology with a Qu NuLabs, an Indian company developing quantum-cryptography-based products and solutions [344].

The following Table 7 summarizes the recent projects on quantum satellite or space QCom in the above-mentioned countries.

Table 7: Examples of recent satellite projects related to QCom research

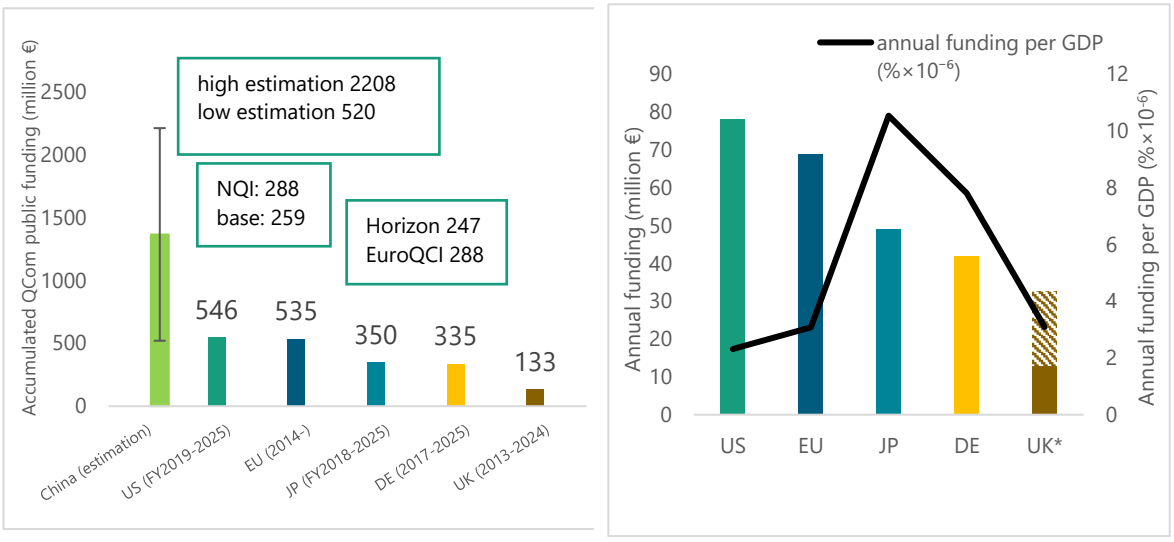
Project, Country	(planed) Year of launch	Project budget
QUBE-I and -II, Germany	Research satellite launched in 2024, the second satellite was launched in 2026	€15m (2017-2025) in total for two projects [305, 309]
Eagle-1, EU	Planned for launch in 2026	No official announcement; one media reported that the mission budgeted at €130m [345]
Micius/Jinan-1 China	Micius was launched in 2016, intercontinental QKD in 2017; Jinan was launched in 2022, QKD between China and South Africa in 2025	No official announcement; one media estimated $100m for Micius [318]
China	A large geo-stationary quantum satellite, scheduled for launch in late 2027 or early 2028 [324]	No official announcement
SEAQUE, the USA	Entanglement-based technology with a technique to help space-based nodes self-heal from radiation damage tested in the International Space Station in 2025 [346]	No official announcement
SpeQtre, the UK and Singapore	Launched in November 2025[347]	£10m (2018-) in the initial plan [348]
QEYSSat, Canada	Planned for launch in 2026	C$30m for design and implementation (2019-2022)
Japan	The launch of the satellite carrying technology developed under the Space Strategy Fund is planned for 2028 [349]	JP¥15.9b from MIC (2018-2023) including ground testbeds; JP¥14.5b from Space Strategy Fund (2025-2029)
National Quantum Mission, India	Indian Space Research Organisation aims to launch a dedicated satellite in 2026-2027, and full integration by 2030 [350]	No official announcement

5.5.2 Comparison of International QCom Funding

This section examines the public funding allocated to support the research, development, and deployment of QCom technologies to assess the level of commitment of key international players. We analyzed the estimated amount of public funding invested through national projects/programs for the US, UK, Japan, EU, Germany, and China, which were selected based on their R&D productivity and availability of budgetary information (details in section 2).

Figure 31 compares the total amount of funding allocated to the identified national QCom programs/projects. Despite the limitations mentioned below (last paragraph of this section), this comparison makes it possible to estimate the R&D interest in QCom in the different countries.

Figure 31: Accumulated identified public funding forin QCom, announced up to 2025 (left) and total annual amount of public funding in QCom (bar graph) and per GDP (line graph) (right). *The dashed segment in the right graph shows the estimated annual funding with the new UK strategy.



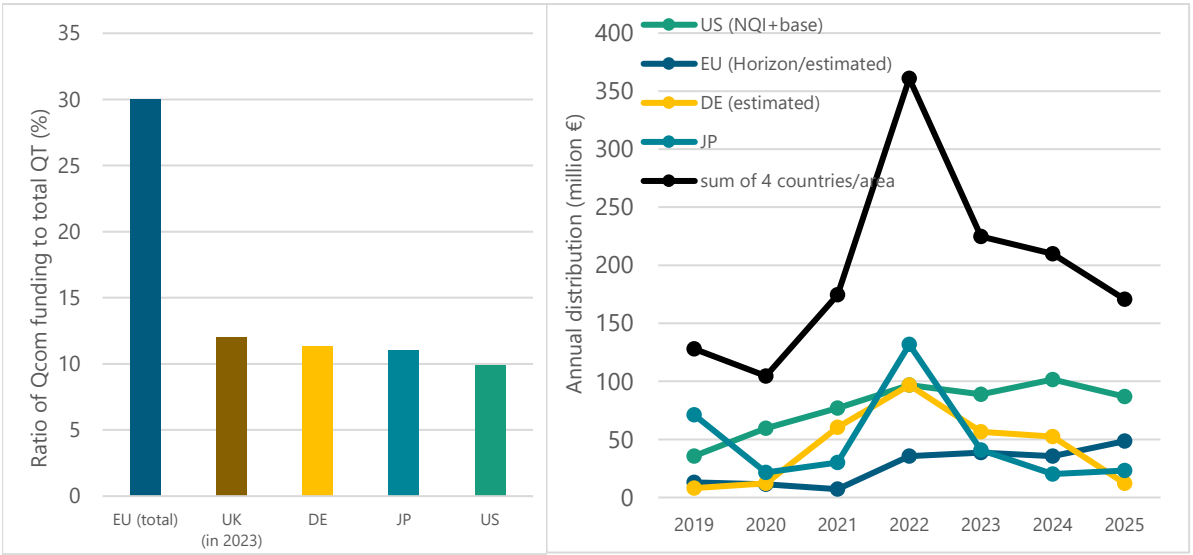
Even under the lowest estimate, China appears comparable to the US and the EU. For the EU, funding under EuroQCI accounts for a larger share of total funding than the Horizon programs. Germany and Japan are at similar levels in QCom. In the figure, the UK's investment was lower than that of the other countries analyzed; however, the UK's funding is most likely underestimated due to comparatively greater information availability for other countries (see "Methodological limitations") and should be interpreted as a lower-bound estimate.

Due to the different time horizons of the funding programs in the analyzed countries, comparing overall funding volumes may give a slightly distorted picture. Therefore, we calculated annual funding (see bar graph on the right-hand side of Figure 31) by dividing cumulative funding by the duration of the relevant strategy. For the US, Japan, and Germany, data from 2019 to 2025 were used due to the availability. For the UK, total funding from the NQTP (2013–2024) was used because of limited access to data for the most recent program. Because the time period of China's initiative is unclear, China is omitted from this graph. The US leads this comparison, followed by the EU, Japan, Germany, and the UK. With the UK's new initiative promising a budget 2.5 times larger than the previous program (including the semi-transparent segment in the bar chart), it is expected in the next years to reach at least a closer level to Japan and Germany, even with the lowest estimation. It should also be noted that Japan's funding for QCom is highly fluctuating and has been allocated at only around 20 million euros annually in these two years (for details, please see the next figure).

To enable a fair comparison of the amounts of QCom funding despite the different size and financial basis, we related the annual QCom funding to the gross domestic product (GDP) of the country (line graph on the right-hand side of Figure 31). Figure 31 (right) shows that the figures for Germany and Japan and the UK exceed those of the US. Since EU funding only includes EU-wide initiatives and not national funding, the figure for the EU should be interpreted as "add-on" funding for Member States (including Germany) rather than an indicator of EU activity in QCom. Taking into account the contribution of EU funding, Germany's funding related to GDP will exceed that of Japan's.

The topic of quantum technologies in general has recently attracted a huge amount of attention from governments and industry and is currently well funded by public bodies. Some countries seem to focus on certain QT (e.g., quantum computers) more than others. In order to analyze whether some countries have a specific focus on QCom, we compared the ratio of QCom to total announced funding in quantum technologies. Due to the lack of sufficient data, the UK refers to the QCom ratio calculated in the previous monitoring report, without update. Although no numerical data was found for China, experts say that historically China has invested a much larger fraction into QCom compared with quantum computing and sensing. Consequently, it is presumed that the country would show higher figures than other nations.

Figure 32: Estimated ratio of QCom funding to total government investment in quantum technologies (left). Trend of annual distribution of QCom funding in the US, the EU, Germany, and Japan (2019-2025) (right).



According to Figure 32 (left), the EU appears to by far have the most focus on QCom (30,0%). In particular, the funding related to EuroQCI makes a significant contribution. After the EU, the UK, Germany, Japan and the US show a similar level of concentration on QCom, with around 10 to 12 percent of total funding. Japan lowers the proportion compared to the value in the previous report (15.7%), reflecting the recent decrease in QCom project budget (see the time-series data for details).

To examine the development over time, the data on the annual distribution of estimated funding for Germany and the EU were derived from our project monitoring. The UK was not analyzed here due to the lack of suitable data. Despite differences in the definition of "annual budget" (details in section 2, Methods), Figure 32 (right) shows the general development of funding over these five

years in the US, EU (Horizon 2020 and Horizon Europe), Germany, and Japan. It should be noted that the EuroQCI was excluded from the EU data due to missing time series data; therefore, the EU graph reflects only the trend in R&D funding.

Overall, four countries have shown different chronological tendencies. While the US and the EU have consistently spent certain amount of funding in these years, funding in Germany, and Japan has fluctuated from year to year.

The sudden increase in funding in Germany since 2021 reflects the launch of many new projects from that year onwards. In contrast, the increase in EU funding can be traced back to a larger average project budget in Horizon Europe than in H2020. It should be noted that the 2025 figures do not fully reflect the entire project budget for the EU and Germany, as data is only available through November 2025. Furthermore, as many projects in Germany concluded, the BMFTR opened a new call for QCom activities in 2025 and new projects are anticipated in 2026.

The sudden jumps in Japanese funding in FY 2019 and 2022 are primarily attributed to one-year funding from the supplementary budget, which is reserved for urgent needs. In particular, the two testbed projects in FY 2022 by the MIC have contributed significantly to these increases, which aim for ensuring strategically important technology in terms of national security, against the backdrop of the enactment of the Economic Security Act. Over the past two years, funding levels have returned to the levels seen in the year the quantum strategy initiative began.

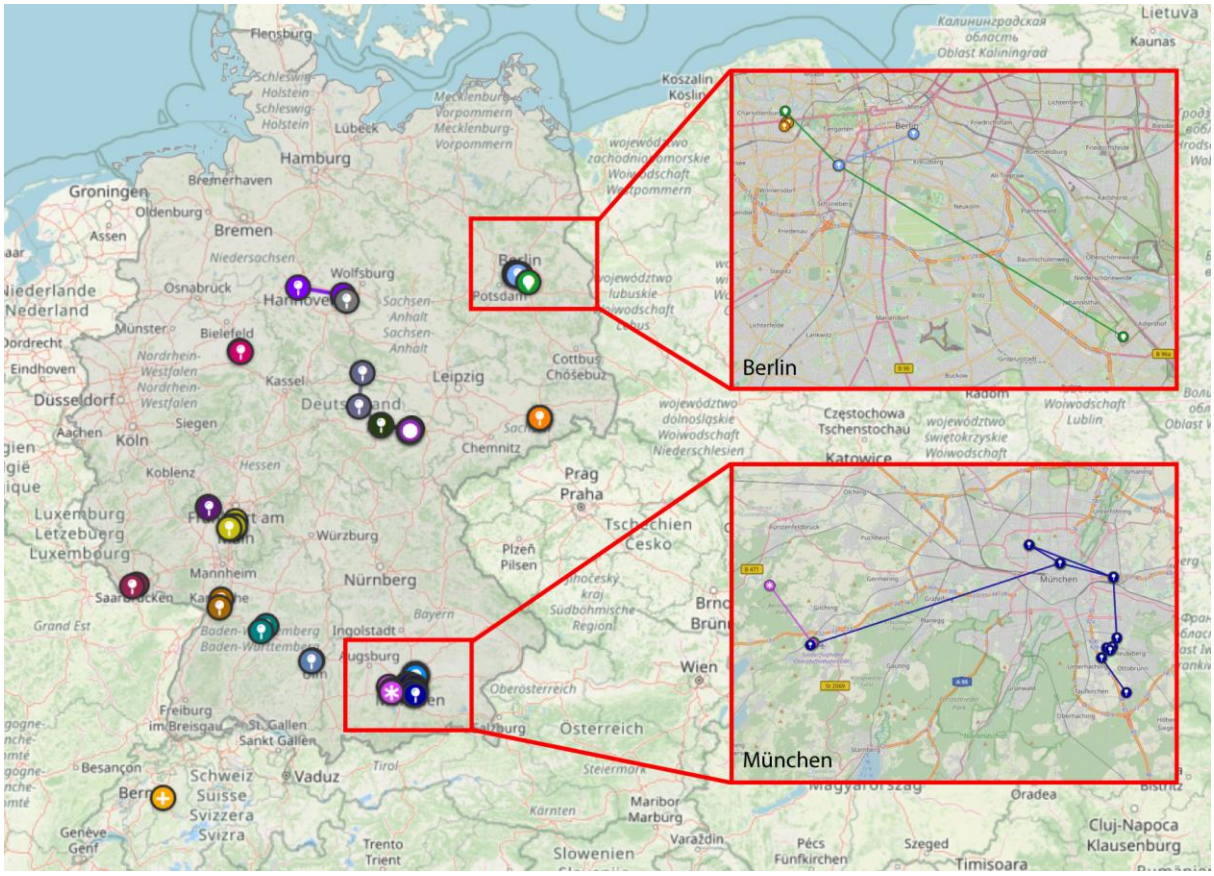
Methodological Limitations

- The comprehensiveness of the available information varies from country to country, which may lead to an underestimation of QCom funding in some countries. For example, the US provides annual budget information for both the NQI and the baseline funding of the relevant agencies. On the other hand, it is difficult to find out the amount of DFG (the German funding agency "Deutsche Forschungsgemeinschaft") funding specifically allocated to QCom. In addition, the UK NQTP also encompasses funding for skills and training. Here, it is difficult to find sufficient data to identify QCom-specific projects.
- Due to the limited availability of information concerning China, our analysis can only provide a rough estimate of Chinese funding based on total quantum technology funding from previous research, which ranges from 17 billion dollars to 4 billion dollars in different studies [13], and our calculation on the averaged QCom ratio among the countries in the Figure 32 (15%).
- In our analysis on the development of funding over time, the definition of "annual distribution" necessarily varies across countries due to the different availability of information. Since the EU and Germany only disclose the project budget for the entire period, the annual distribution is estimated based on the number of projects and their average budget.
- Our research only considers public funding, but it is likely that there are other financial resources that complement public funding, such as the funding from state governments and private investments, especially in the US. According to the McKinsey Quantum Technology Monitor 2023, US QT startups received five times more investment from private investors between 2001 and 2022 than EU-based companies as a whole [351].

5.6 Testbeds for QKD in Germany

Testbed infrastructure can be a key facilitator for QKD providers and developers to test and verify their novel technologies, protocols, and use cases, accelerating development, standardization and deployment of QKD-components. The development of testbeds in Germany is advanced on several fronts: via several third-party funded projects, via private or commercial activities i.e. by T-Labs [352], and via comprehensive technical concepts for establishing a national R&D testbed [353]. Prominent examples are the EU- and BMFTR-funded projects in the field of quantum communication in Germany like the QuNET-consortium and the Q-net-Q-initiative, which is the German national branch of the EuroQCI-initiative. Further testbed infrastructure was established and used in the Umbrella Project for Quantum Communication in Germany (SQuaD), the QR.N-consortium as well as in projects funded by the so-called "state initiatives" (Länder-Initiativen) or beyond as for instance the Munich Quantum Network (MuQuaNet) [See [353] for an overview].

Figure 33: Overview about the existing and planned testbed infrastructures in Germany in the field of Qcom. Most of the testbeds are fiber or free-space links. The testbeds consist either of point-to-point links or networks. Examples are the Berlin Quantum Communication testbed (top right) and the MuQuaNet (bottom right).



Source: Map data from OpenStreetMap (2026).

Testbeds allow for operating and evaluating devices in realistic operational environments. Most of the QKD-testbeds available in Germany focus on the transmission of the QKD-signal. In particular, there exist several dark fiber connections enabling the test of devices without the interference of optical amplifiers and scattering of co-propagating signals at potentially overlapping wavelengths

as the quantum signal. In addition, there are also free-space links and optical ground stations for satellite or airborne QKD available. The Umbrella Project on Quantum Communication (SQuaD) within the BMFTR-funded innovation hub for quantum communication started a summary of the available QKD testbeds in Germany and published a testbed map on its website (Figure 33) [354].

Over the course of 2025, the map was redefined as more testbeds were identified throughout Germany. As of June 2026, it includes 27 officially listed and designated testbeds. Among the newly identified testbeds, examples include the Darmstadt Quantum Local Area Network (DaQLAN), PTB's Calibration and Measurement Capabilities for QKD, the intracity fiber Link PTB–Rolleiwerke, and TESAT Spacecom's Alphasat/TDP1. A detailed technical description of all the listed testbeds is now available in the **Testbed Catalogue for QKD in Germany**, which is publicly accessible [354]. In addition, individual information for each testbed is provided in a table on the SQuaD testbed homepage [354]. On zooming in one can identify the detailed network architectures that consist in most cases of simple point-to-point links, but there are also more complex networks. In the top-right of Figure 33. the Berlin Quantum Communication Testbed is shown, which consists of many fiber links and a free space link. In the bottom right, the MuQuaNet is shown.

The specifications of the testbeds can be found in Table 8. The fiber testbeds have a length from several hundred meters with the inhouse Dresden Qcom Fiber Testbed in Saxony, to up to about 78 km in the Niedersachsen Quantum Link in Lower Saxony. The latter link length resembles the typical maximum link limit for achieving secure quantum key distribution with a Quantum Bit Error Rate (QBER) of less than 11% with fiber-based QKD systems without the need of trusted nodes or quantum repeaters. The distance for transmission of QKD signals is limited due to the attenuation of the optical signal inside the fiber. We note that the fiber links are partially inhouse, but mostly intercity and intracity links and therefore close to the conditions of later applications. Intracity and intercity dark fibers are rented from commercial providers. As can be seen from Table 8, the fiber-bound testbeds focus on the telecom wavelength regime of the O-band (around 1310 nm) and C-band (around 1550 nm). However, for the free-space optics and especially the optical ground stations, the visible spectrum is additionally considered.

Most of the links shown originate from dedicated projects and feature individual characteristics, infrastructure, and demonstrated milestones. The Saarbrücken Qcom Fiber Testbed and the Niedersachsen Quantum Link are both embedded in the QR.N project that focuses on the development of quantum repeaters and quantum networks. One milestone demonstrated by the Saarbrücken Qcom Fiber Testbed is the distribution of photon-photon and qubit-photon entanglement over 14 km of deployed fiber, and the quantum teleportation from an ion qubit to a photonic qubit.

The Niedersachsen Quantum link that consists of a pair of dark fibers, is at the same time a time & frequency dissemination link between Physikalisch-Technische Bundesanstalt (PTB) and Leibniz Universität Hannover (LUH): One fiber can be used for quantum applications whilst the other fiber can be used for the dissemination of time and frequency references as well as classical communication signals. Here, first experiments test high-repetition rate QKD with semiconductor quantum dot single photon sources. In 2025 a second, 14 km long intracity fiber link starting from PTB and connecting to the Quantum Valley Lower Saxony Hightech-Incubator in the Rolleiwerke has been established, allowing for tests elementary star-like QKD network topologies from the PTB campus.

The Berlin Quantum Communication Testbed was used for several proof-of-principle experiments of QKD over free-space and fiber, including entanglement distribution, co- and counter propagation of quantum signals and conventional "dense wavelength division multiplexing" (DWDM) data channels. In the QuNET Key Experiment 1 performed 2023 in Jena, the consortium demonstrated full QKD on a heterogeneous link consisting of a 1.7 km free space link and afterwards several hundreds of meter fiber connection on the local Campus Network Beutenberg. Another testbed connecting Jena and Erfurt via 76 km of fiber is not only used by the Fraunhofer IOF for internal

experiments but was also used by Quantum Optics Jena to test their devices. Among other goals, the anticipated focus of the MuQuaNet testbed is the demonstration of quantum communication for civil and defense applications. Air-ground communications experiments were performed using the Optical Ground Station (OGS) Oberpfaffenhofen. Optical link measurements with several satellites were achieved.

A promising network for the development of a future Quantum Internet and its diverse applications, e.g. entanglement distribution and quantum key distribution (QKD), is the QTFC (Quantum, Time & Frequency, Classical) network operated by T-Labs. QTFC represents the successor to the R&D-oriented SASER network, which originated from the BMFTR-funded SASER project. The nationwide SASER network, together with the 2,412 km long QTFC fiber infrastructure, have been established and are continuously expanded with the objective of supporting research and development experiments in both classical and quantum communication networks.

The fully meshed network architecture enables dense wavelength division multiplexing (DWDM) for classical communication channels, passive wavelength-assigned optical switching to facilitate the transmission of quantum channels, and the distribution of time and frequency signals. The latter is essential for synchronized experiments, which are prerequisites for the operation and evaluation of quantum networks.

Within the Berlin metropolitan area, the Berlin-QTFC test network is implemented in a star-shaped topology with the central node located at Deutsche Telekom's Winterfeldstraße (WFD) site. The network comprises dark fiber links to several research institutions, including Fraunhofer HHI, Humboldt University, and additional partner locations, resulting in a total fiber length exceeding 500 km. This infrastructure formed the basis of the QKD TestNet Berlin, which was selected as one of the three European test networks within the EU flagship project OpenQKD.

Apart from QKD transmission testbeds, there are also testbeds focusing on individual key components of QKD devices. At PTB, for instance, a testbed provides Calibration and Measurement Capabilities for QKD including the characterization of single photon sources and single photon detectors. For a reliable and safe application of QKD, testing of the individual components of QKD setups is as important as the testbeds for the transmission of the signals.

Though the optical transmission testbeds are distributed all over Germany, a consistent QKD backbone throughout Germany is not yet existent and there are mostly separated individual links. Within the national QCI project within EuroQCI Q-net-Q, the QuNET initiative and the Länder-Initiativen, longer testbed links are considered that will connect several states like Berlin, Hessen, Saxony, Thuringia, and Bavaria (i.e. Dresden – Erfurt – Nuremberg, or Berlin – Erfurt – Frankfurt). However, most of the testbeds are linked to temporary projects and their existence is limited to a few years at maximum. Therefore, a continuous and changing testbed map is expected.

To address this long-term need for an R&D test net, stakeholders have proposed a national fiber optic network, a "QTF-Backbone", to connect and provide research facilities across Germany with a dedicated infrastructure for experimental **q**uantum links (Q) alongside **t**ime and **f**requency (T&F) distribution. This proposal includes (1) a comprehensive technical design including integration into and of EU and Germany testbeds, (2) a cost analysis and funding concept, (3) a proposed implementation pathway to reach the most stakeholders as possible, (4) recommendations for user access models and a governance to enable wide-reaching and long-term use of the infrastructure, and (5) a detailed analysis of the impact of the infrastructure on Germany's R&D landscape describing ten transformative R&D topics. The QTF-Backbone is envisioned as a wide-meshed national fiber-optic core network integrating services and facilities for experiments, enabling scientific and industrial R&D in quantum technologies and precision time-frequency applications.

Table 8: Overview of the QCom testbeds included on the testbed map from the SQuaD project. Most of the QKD links are fiber-based, however there are also links based on free-space optics (FSO) and optical ground stations (OGS).

No.	Name	State	Type	Length [Km]	Wavelength	Status
1	Karlsruhe Quantum Communication Fiber Testbed	Baden-Württemberg	dark fiber	~ 22.0	o-band (1330 nm) to c-band (1550 nm)	operational
2	Stuttgart Quantum Communication Fiber Testbed	Baden-Württemberg	fiber	17.9	Related to the standard SSMF, including O-, E-, S-, C-, L-, and U-Bands	operational
3	FSO Testbed Optical Ground Station Oberpfaffenhofen	Bavaria	FSO	~7.0	VIS, 589 nm, 850 nm,1064 nm, 1550 nm	operational
4	Munich Quantum Network (MuQuaNet)	Bavaria	fiber and FSO	0.7-17.4	810 nm, C-band (1550 nm)	partially operational
5	Optical Ground Station Oberpfaffenhofen	Bavaria	OGS	n/a	VIS, 589, 850, 1064, 1550 nm	operational
6	Quantum Network at the Technical University of Munich (QuaNTUM)	Bavaria	dark fiber	10.8	780 nm – 1600 nm	Planned
7	Berlin Quantum Communication Testbed	Berlin	FSO and fiber	0.3 - 47.3	O-band (1310 nm), C-band (1550 nm)	operational
8	Testbed Bundesdruckerei – T-Labs	Berlin	fiber	8.0	1550 nm	operational
9	TU Berlin Quantum Communication Testbed	Berlin	fiber and FSO	3.9 and 0.4	O-band (1310 nm) to C-band (1550 nm) for fiber 780 to 950 nm for FSO	Active
10	TESAT Spacecom, Alphasat/TDP1	Bern	FSO	~38000	1064 nm	operational
11	Darmstadt Quantum Local Area Network (DaQLAN)	Hesse	fiber	0.27 – 37.06	C-band (1550 nm)	operational
12	Niedersachsen Quantum Link/ PTB Time & Frequency Link	Lower-Saxony	fiber	78	C-band (1530-1565 nm)	operational
13	Intracity Link PTB-Rollei	Lower-Saxony	dark fiber	14.0 (28 looped test)	1550 nm	operational

No.	Name	State	Type	Length [Km]	Wavelength	Status
14	PTB Calibration and Measurement Capabilities for QKD	Lower-Saxony	component calibration and characterization	n/a	n/a	operational
15	PhoQSNet	North-Rhine-Westphalia	fiber	9	O-band (1310 nm), C-band (1550 nm)	Planned
16	Saarbrücken QCom Fiber Testbed	Saarland	fiber	14	O-band (1310 nm) to C-band (1550 nm)	operational
17	Dresden Quantum Communication Fiber Testbed IIS/IVI	Saxony	dark fiber	10.0 (20 with circulator)	O-band (1310 nm) to C-band (1550 nm)	operational
18	Dresden Quantum Communication Fiber Testbed in-house	Saxony	fiber	0.2	810 nm; O-band (1310 nm) to C-band (1550 nm)	operational
19	Campus Network (Beutenberg Campus Jena)	Thuringia	fiber	< 1	C-band (1550 nm)	operational
20	Free-space Link Jena	Thuringia	FSO	1.7 – 7.0	500 nm to 2 µm	operational
21	Jena – Erfurt Fiber Link	Thuringia	fiber	~76.0	C-band (1550 nm)	operational
22	Jena-Erfurt Fiber Link Extension I	Thuringia	fiber	~24.0	n/a	Planned
23	Jena-Erfurt Fiber Link Extension II & III	Thuringia	fiber	~50.0	n/a	Planned
24	Optical Ground Station Jena	Thuringia	OGS	n/a	multiple wavelengths possible upon request	installed
25	Quantum Information Network Ulm	Baden-Württemberg	fiber	2x 2.5	1310 nm and 1550 nm	operational
26	QSyncNextG – Quantum Synchronisation for Resilient and Secure Next Generation (5G/6G) Campus Networks	Saxony	fiber	0.009	1550 nm and 850 nm	operational
27	Quantensichere Kommunikation Proof of Concept Hessisches Landesnetz	Hesse	dark fiber	6.5	C-band (1530-1560 nm)	operational

6 Technology Sovereignty Considerations

The German government has reaffirmed its goal of achieving technology sovereignty in quantum technologies in the recently published Hightech Agenda [20]. The plan was originally formulated in the Action Plan for Quantum Technologies ("Handlungskonzept Quantentechnologien"), explicitly including quantum communication [300]. Technology sovereignty involves many facets and aspects that we want to discuss in this section in relation to the topic of quantum communication. We base our discussion on the policy paper "Technology sovereignty - From demand to concept" by Fraunhofer ISI [12]. Building on this, experts' opinions and the survey conducted in the quantum communication community, the need to achieve technology sovereignty in QCom is discussed (section 6.2), current challenges are presented (section 6.3) and potential measures to overcome them are highlighted (section 6.4).

6.1 Context and Background

The discussion about the need to secure technological sovereignty for critical technologies within Germany and Europe has gained momentum in recent years. Geopolitical tensions, the reemergence of international conflicts, war on the European continent and the restructuring of the global economy have led to the increasing relevance of policies and strategies that aim to secure domestic capabilities and value creation within the European Union.

The goal of achieving technology sovereignty is formulated in German funding programs for technologies that are identified as critical for the current and upcoming transformations [355]. The recent emphasis on technology sovereignty has appeared not only in Germany and the European Union but in other nations all over the world. The Inflation Reduction Act in the USA includes policies focused on the goal of safeguarding domestic value creation. This Act is therefore often mentioned as a prominent way to push for high degrees of technological sovereignty.

Technology sovereignty can be defined as "the ability of a state or a federation of states to provide the technologies it deems critical for its welfare, competitiveness, and ability to act, and to be able to develop these or source them from other economic areas without one-sided structural dependency" [356]. As this definition is rather conservative compared to what is often meant when politicians and policies use this expression, further degrees of sovereignty have been introduced that go beyond technology: innovation sovereignty and economic sovereignty. While technology sovereignty includes the ability to research a technology and produce the corresponding product at least on a lab-scale, innovation sovereignty additionally includes the ability to use the technology to realize new solutions for the market or within society. Achieving economic sovereignty includes the ability to reap economic benefits from the technology (Table 9).

Table 9: Degrees of technological sovereignty

Degree of technological sovereignty	Translates to being able to…	Necessary precondition to…
Technology sovereignty	…set globally relevant impulses for technological development	…maintain technological leadership

Degree of technological sovereignty	Translates to being able to…	Necessary precondition to…
Innovation sovereignty	…pilot solutions under real-world conditions and develop market-ready products	…shape future markets
Economic sovereignty	…produce relevant components and systems along the value chain	…create domestic value added

For the countries that are part of the European Union, technological sovereignty should not be regarded at the national level but at the EU level due to the significant degree of economic and political interconnectedness. Therefore, this report focuses on European technology sovereignty. Nevertheless, it should be kept in mind that some aspects should also be discussed on a national level.

With the rise of quantum computing, encryptions based on certain classical algorithms (e.g., RSA) could be decrypted within reasonable time frames, making large quantities of exchanged data vulnerable to eavesdropping attacks. Even though it is not easy to predict when this threat could become reality, the need for substantial technological advancements in encryption algorithms is beyond doubt. The German Federal Ministry of Research, Technology and Space (BMFTR) has specifically included quantum technologies as one of six key technology fields and quantum communication as a subfield in the Hightech Agenda with the goal of achieving technology sovereignty [357]. Other actors from science, industry, and politics have already formulated their perspectives of the potential measures to be taken [358–362].

The following discussion aims to give an overview of the various perspectives on technology sovereignty. Expert interviews are complemented by survey results about the main challenges of quantum communication (see section 2) "Methods"). The discussion is not exhaustive, but merely a starting point for further analyses of needs, motivations, challenges, and potential measures to achieve technological sovereignty within quantum communication in Germany and Europe.

Sections 6.2, 6.3 and 6.4 reflect the perspectives of the five experts from science, industry and a public authority, all active in the quantum communication community, interviewed and the attendees of the workshop and do not necessarily represent the authors' viewpoint.

6.2 Needs and Requirements

Secure communication is a central pillar for democratic systems and societies, as it is a prerequisite for national security, protection of secrets at governmental, company and individual level, individual privacy, economic transactions, elections and so on. The communication infrastructure used is therefore part of a nation's critical infrastructure and their security of paramount interest [363].

The interviewed experts and public stakeholders see an urgent need to address the cryptographic challenges that the rise of quantum computers poses. However, different technological paths could offer solutions. Furthermore, different stakeholders have different opinions about whether these capabilities should be established domestically or merely accessed via international trade relations.

One approach to make communication secure against cryptanalytic attacks by quantum computers is the use of "post quantum cryptography" (PQC) algorithms. In principle, PQC algorithms could turn out to be secure over very long timescales, potentially limiting the added-value of quantum communication approaches (in retrospect). . Furthermore, current QCom technologies face several practical limitations. In particular, they are difficult to deploy in some real-world scenarios that require high security, such as mass-market mobile applications. QKD provides information-theoretic security for key distribution itself, but the overall encryption process is only information-theoretically secure if the QKD-generated keys are used with a one-time pad.

However, there is currently no proof (or counter-proof) that PQC algorithms can resist quantum computer or classical computer attacks. Therefore, the experts interviewed see a high relevance for complementing the R&D and rollout of post quantum cryptography with the development of QCom technologies, such as QKD. While conventional algorithms always need to address the advances made in (quantum) computer technologies (unless mathematically proven to be completely safe against attacks), quantum communication approaches could potentially provide encryption based on fundamental physical principles that are not decipherable on the respective transmission paths. Two important notes have to be made here: First, it cannot be excluded that PQC algorithms could be developed that offer perfect mathematical security equal in quality to the potential that QKD has. Second, the perfect security often claimed for quantum communication technologies has to be taken with a grain of salt, as potential security threats still have to be addressed (implementation attacks against QKD systems). Nevertheless, QCom technologies are often described as offering a peace-of-mind solution with perfect security on the transmission path. At the least, they can provide additional security by complementing PQC approaches. The experts interviewed agreed that further development of QCom technologies is therefore required to prepare high security sectors for expected future scenarios.

Furthermore, domestic competencies should go beyond the aspects formulated in the basic concept of technology sovereignty. Owning the expertise needed to develop and produce technologies was deemed necessary to a certain extent by the experts interviewed. In general, importing components for QCom technologies was considered tolerable, as long as there are sufficient domestic competences to critically examine and test all components to ensure the required security standards. However, this requires such a profound grasp of the technologies involved that it would be equivalent to having the skills required to enable domestic production. Most experts would also tolerate the import of technologies on a system level (e.g., QKD systems), if the same prerequisites were given. Nevertheless, all the experts interviewed considered the ability to produce the technologies at least on a system level as indispensable for Europe for different reasons. First, there is considerable economic potential associated with the domestic production of a QCom system, which could be a crucial stepping stone to enable future value creation in related technological fields with potentially even larger markets (e.g., communication between quantum computers). Second, this ability might be needed to prevent one-sided dependencies and provide multiple sourcing opportunities, especially as currently some countries, such as the USA, seem to be focusing more on PQC-based approaches. Furthermore, Europe could strive for technological leadership in quantum technologies or related enabling technologies, which could stabilize reciprocal dependencies, paving the way for technology sovereignty in unrelated technologies. Finally, the recommendation of some experts was to not consider importing technologies on a system level at all to minimize security risks.

Table 10: Need for competencies in quantum communication:

	Need	Motivation
R&D	• Ability to understand and develop technologies at least on a system level • Ability to test (imported) components and systems with respect to their security	• Guarantee the security of implemented communication networks
Manufacturing	• Ability to manufacture technologies at least on a system level • Ability to import required components without one-sided dependencies	• Avoid dependencies through multiple sourcing strategies • Avoid the security risk posed by non-domestic technologies • Enable value creation

Overall, the need for technology sovereignty in QCom was emphasized strongly by all the interviewed experts. Some went even further and stressed the economic potential that quantum communication technologies could leverage in the future.

6.3 Status Quo and Challenges

As QCom is an emerging field of technology, Europe and Germany are still in a position to realize strategies for all degrees of technology sovereignty and technology leadership. In the following, we present the most important challenges that will need to be addressed and, where applicable, the status quo. We asked the experts to identify factors hampering QCom innovation activities along four dimensions, inspired by the factors and dimensions proposed by the OECD's Committee for Scientific and Technological Policy [13]. These dimensions are cost factors, knowledge factors, market factors, and institutional factors. As the results are based solely on the experts' opinions, the list of the hampering factors discussed is not exhaustive.

Table 11: Starting point for achieving technology sovereignty in quantum communication technologies within Europe:

Dimension	Guiding question	Status quo
Cost factors	Can Europe acquire the knowledge needed to develop QCom technologies, train experts, and secure jobs (to the necessary extent)?	+ Public funding – Private investments
Knowledge factors	Can Europe invest in and develop a competitive QCom industry and compete and/or cooperate with non-European players?	+ Enabling technologies – Interface to classical technologies

Dimension	Guiding question	Status quo
Market factors	Can Europe enter or build supply chains and generate a relevant market?	+ Potential market (several sectors) – End users from industry
Institutional factors	What are the relevant framework conditions (political, regulatory, societal, environmental, etc.)?	+ Commitment of authorities – Approvals and certifications

To complement the experts' opinions on the most important obstacles and hampering factors with a complementary quantitative picture based on the opinions of the community, a survey within the quantum communication community was conducted. Survey participants were asked to evaluate the main factors that could hinder progress. The survey focused on the four broad categories of potential barriers factors (multiple answers were possible in each category): a) cost factors, b) knowledge factors, c) market factors, and d) institutional factors. The following analysis includes a summary of the perceptions of 61 respondents regarding the most significant challenges to advancing QCom technologies in real-world applications.

Cost factors

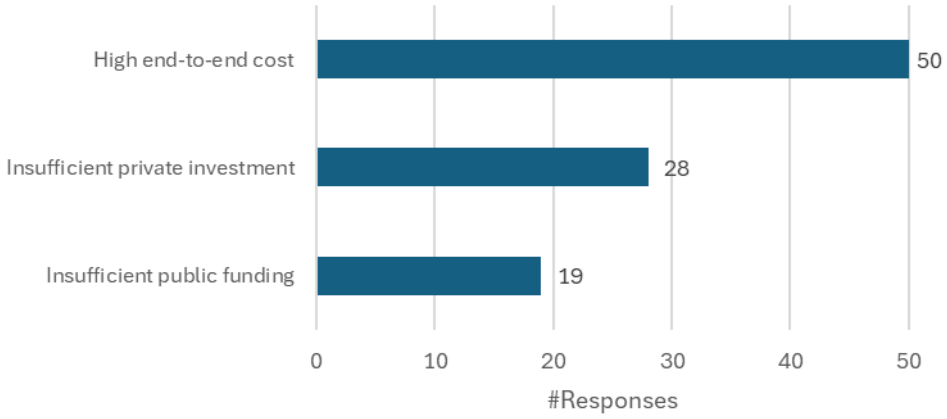
Currently, the challenges associated with the cost of innovating QCom are being addressed by public funding in Europe. The European and national funding schemes described in sections 5.4 and 5.5 (including EuroQCI) provide a good starting point to cover the risk and cost of developing QCom technologies. Nevertheless, some experts have called for larger funding programs in the past, especially to set up large-scale projects in Europe. While Euro-QCI continuously pushes the roll-out of QKD infrastructure, finding a good scope for the funding schemes in terms of how targeted (narrow vs. wide) is still considered a challenge today. Private investments remain to be limited, even though activities have been increasing in the past (for example, [364]). To push QCom development, further investments by industrial players are strongly desired in Europe.

In the upcoming years, continuously increasing the investment in European QCom infrastructure is required to further push large-scale implementation. QKD systems, which are currently being commercialized, are still expensive – the high investments involved entail a high economic risk for private actors.

As public funding is currently being spent on projects with limited time frames, which are in turn connected to strategies with limited time horizons, continuity of funding cannot simply be assumed. The focus of governments can shift over time, especially after elections. This lack of certainty represents an investment risk for those institutions and companies dependent on public funding.

The survey results further validate these observations. Approximately half of the 97 responses on the most important cost factors (multiple choice) identified high costs for establishing an end-to-end connection as the primary challenge to scaling up QCom technologies (n = 50). A smaller number pointed to insufficient private investment (n = 28) and inadequate public funding (n = 19) as limiting factors. These results indicate that economic considerations – particularly high implementation costs – remain major barriers to broader adoption.

Figure 34: Survey result for the most relevant cost factors hampering the adoption of quantum communication adoption



Knowledge factors

European QCom research is well established internationally, and broad knowledge of the required technologies (e.g., photonics) is provided by universities, research institutions, and technology companies (see also section 5.1). Expertise in enabling technologies, in particular, is considered a major asset for Europe. The knowledge needed to develop the majority of essential components for QCom technologies is available in Europe, even though in-depth knowledge is not given across the entire spectrum of approaches for QCom and related technologies. While Europe has expertise in optics (e.g., technological leadership in photonic chips), it might still lack competence in developing and producing certain types of microelectronics. Skills might not be equally available in all European countries, which could give rise to potential challenges to establishing European technology sovereignty in the future. Nevertheless, the experts rated the status quo of European knowledge in QCom as the least problematic out of the four discussed dimensions of hampering factors.

Even though this puts Europe in a good starting position, some fields still require deeper knowledge. The main parameters that will need to be addressed are robustness and speed of the respective technologies. Designing and implementing the interface between Qcom technologies and conventional technologies is another major challenge that was considered potentially inadequately addressed in the initial analysis. Even though progress has been made in the past years, only commercialized products integrated into classical networks can demonstrate that this gap has been closed sufficiently. More in-depth knowledge about the relevant security aspects and potential security risks of QCom technologies is currently being developed. Furthermore, technologies for specific QCom approaches, such as quantum repeaters, are still at low maturity levels and need scientific breakthroughs for opening a path towards future applications.

Besides overcoming these challenges in research and development, transferring knowledge to industry is required and poses a central challenge when commercializing QCom technologies. This includes training a skilled workforce and QCom specialists, which might be especially difficult, as this simultaneously requires deep tech and interdisciplinary competencies, such as quantum physics, informatics, and communication technologies. However, quantum specialists make up only a small part of the required workforce – employees from well-established fields (e.g., electronics) that are willing to work in an emerging field of technology are required along the whole value chain.

Furthermore, educating potential end users in industry (e.g., banks, medical institutions, etc.) and public institutions (e.g., ministries) about the need for secure communication, the threat posed by

developments in quantum computing and the potential solutions offered by PQC and QCom technologies has been intensified in the past[4]. Yet, this dissemination of knowledge should be further expanded throughout society to raise awareness and support technology acceptance. As quantum technologies are often described as 'spooky' or unintuitive, their concrete realizations and impacts on society might be overlooked or not anticipated by uninformed stakeholders. In the past few years, the efforts towards informing relevant stakeholders about the risk of communication systems prone to the threat of future quantum computers have been intensified. This includes educating the broader public about the potential of quantum communication. Furthermore, providing transparent information about the relevant actors, services, and products in the field is required. The funding program Quantum Future Professionals [366] by the BMFTR is one example of intensified efforts towards quantum technology education and quantum awareness.

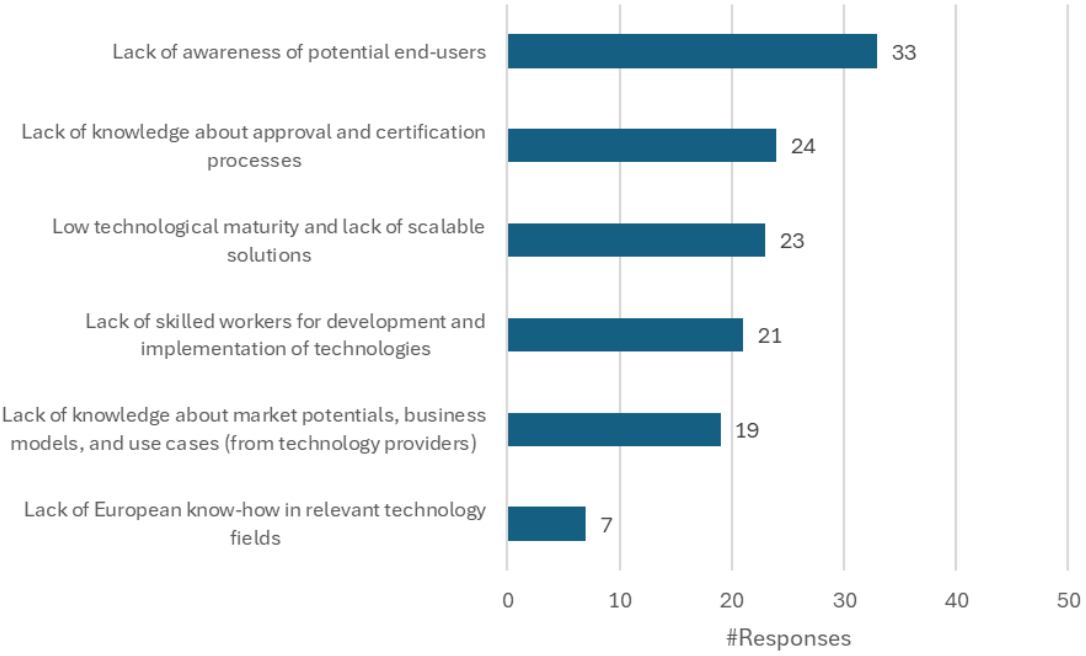
The fragmentation of end users (different requirements by different applications), activities across Europe and along the value chain has been discussed increasingly in the past few years and should be addressed by well-aligned strategies on national and European levels.

Finally, understanding the role that quantum communication can play in the future communication landscape is still an open challenge. Further insights are required into which kind of QCom technologies are needed in which applications and to what extent. A more informed idea of what European QCom value creation could look like and how potential markets will emerge is crucial to develop respective strategies.

Survey answers on knowledge-related barriers exhibited higher variability than on cost-barriers. About one quarter of the 127 responses on the most important knowledge factors (multiple choice) referred to a lack of awareness among potential end users as the most significant obstacle (n = 33). This was followed by limited knowledge of approval and certification processes (n = 24), low technological maturity and absence of scalable solutions (n = 23), insufficient skilled workforce for development and implementation (n = 21), and limited understanding of market potentials, business models, and use cases (n = 19). The least number of votes was recorded for the lack of European know-how in relevant technology fields (n = 7). These findings suggest that gaps in awareness and expertise, both among end users and within the workforce, represent key challenges to advancing QCom.

[4] For example, by targeted conferences such as seQUcom [365].

Figure 35: Survey result for the most relevant knowledge factors hampering the adoption of quantum communication adoption



Market factors

It is not yet clear in what time frame markets for QCom technologies will emerge. As governmental institutions rely on secure communication, a considerable potential market for QCom technologies exists in this area in Europe. At the same time, there are many active players in the QCom value chain, which is a good starting point for developing supplier structures for the relevant component technologies within Europe. However, market penetration is only possible if significant challenges can be overcome.

In many countries, governmental institutions and certain public organizations could only implement QCom technologies for classified communication after approval from the respective authority, generally the national (cyber)security agency (in Germany: Federal Office for Information Security [Bundesamt für Sicherheit in der Informationstechnik, BSI]). At present, no QCom products have been approved for a classified use case in a governmental institution in Germany, as – to our knowledge – no device has started an approval process yet. As the emergence of this market segment strongly depends on approvals, predicting its size is associated with great uncertainty, as it will remain fragmented by national borders.

Nevertheless, QCom is currently strongly dependent on the market that is being set up based on European public funding. Public institutions are often mentioned as potential early adopters that could play a very important role for this field of technology – more likely is the adoption in less-regulated use cases by private actors or as well-defined applications in the banking sector. Creating anchor customers is anticipated, but remains challenging. The currently limited size of this market deprives QCom technologies of the possibility to "learn on the market", i.e., use the experiences made with early generations to boost the further development of the respective technologies.

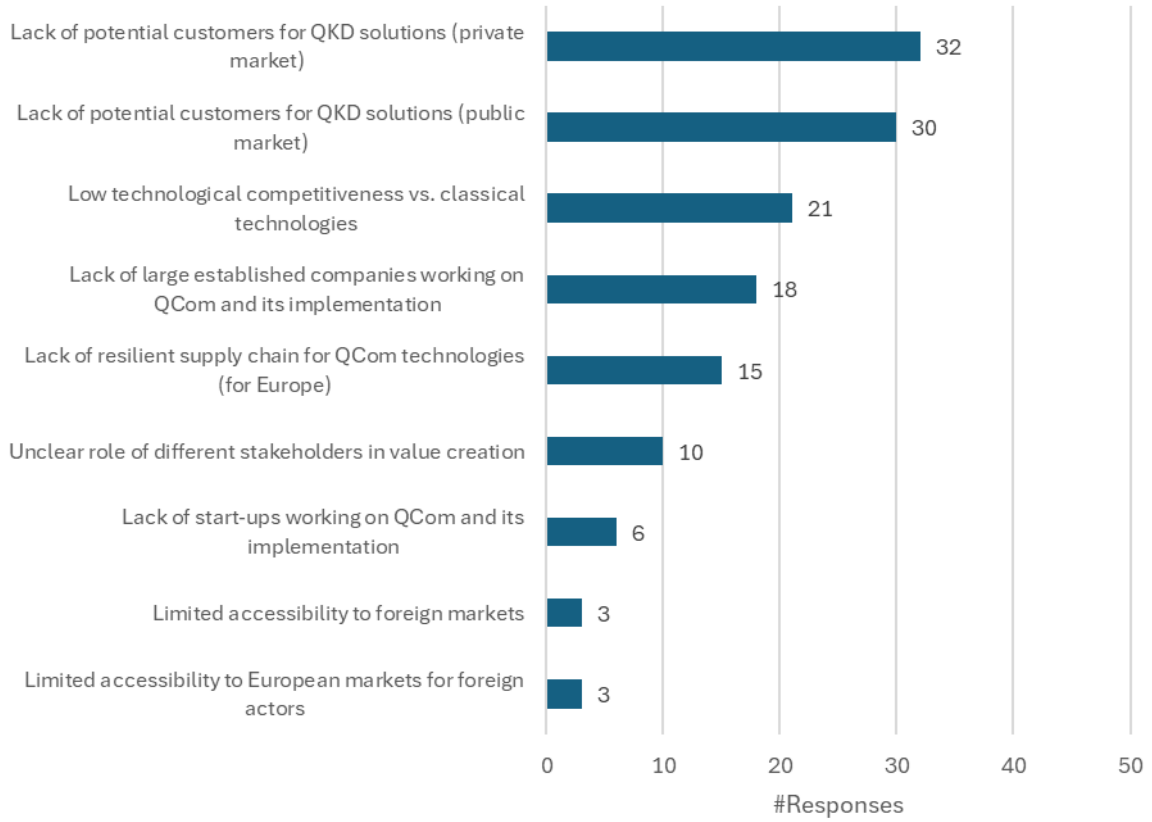
Furthermore, the role that the different stakeholders play in value creation remains unclear. This results in uncertainty regarding the skills that should be developed by the various actors and could

simultaneously hinder the adoption of the technology by end users (e.g., who will provide the system to the end user—system developers or telecommunication companies? What are the business and use cases?).

Telecommunication companies can be quite large and there may be only a few providers in some countries. If such a company develops significant market power, it could impact the concerted efforts of other stakeholders, such as European standardization activities.

Among 138 responses, nearly half (n = 62) cited the lack of (potential) customers for QKD solutions as the most significant market barrier – with similar emphasis on private (n = 32) and public market (n = 30). Other concerns included low competitiveness compared to classical technologies (n = 21), the absence of large established companies actively engaged in quantum communication (n = 18), and a lack of a resilient supply chain for quantum communication technologies in Europe (n = 15). Factors such as few start-ups (n = 6) and limited market accessibility for foreign actors (n = 3) were viewed as less critical. Overall, limited demand and industrial engagement are seen as major constraints on market development.

Figure 36: Survey Result for the Most Relevant Market Factors Hampering the Adoption of Quantum Communication Adoption



Institutional factors

As previously mentioned, the emergence of a relevant market is strongly dependent on the decisions and policies of governments and public institutions. Political will at national and European levels is required for QCom technologies in particular, as they involve critical infrastructure.

Demonstrating the required security level of QCom systems necessary to be approved for demanding use cases is a gatekeeper to large parts of the potential QCom market. Defining the procedures performed in testing laboratories for approval and certification processes could provide more

clarity for technology providers and potential end users – activities have been pushed in the past years[5] and a first protection profile for prepare-and-measure QKD systems has been developed [368]. However, proofs of security for real-world implementations and their demonstration by standardized measurement procedures remain to be developed in the near-term future. The BSI has an important role in the approval and certification of QKD systems in Germany.

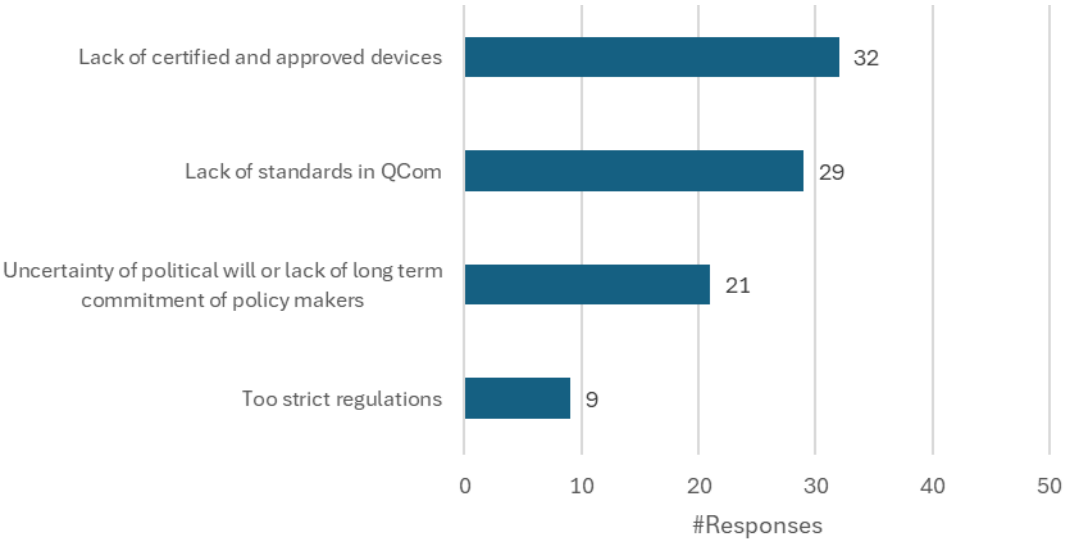
Furthermore, different countries often maintain their own certification and approval schemes for security products such as QCom systems used in government institutions. The potential denied approval for using QCom systems developed abroad for certain use cases or the implementation of regulations preventing their use in certain fields have a direct impact on market accessibility. Although domestic companies could profit from this in general, they limit the export-related value creation potential. Even for domestic companies, this could pose a challenge if the use of components of certain suppliers is prohibited.

Standards for QCom technologies (beyond the existing QKD standards, such as ETSI 011 or ETSI 003 [369, 370]) are still under development [371]. On the one hand, the current lack of standards can inhibit the development of technologies at system level and system integration. On the other hand, this makes it difficult to compare different technologies, prototypes, and products at all maturity stages. The development of more and newer standards that are being picked-up by companies is therefore an important task for the upcoming years.

The national and European public funding schemes have to comply with competition law regulations. This as well as other bureaucratic processes are challenges potentially delaying or preventing the realization of large projects.

Of 91 responses, about two-thirds highlighted the lack of certified and approved devices (n = 32) and the lack of standards in QCom (n = 29) as the most significant institutional obstacles. Additionally, uncertainty regarding political will or lack of long-term policy commitment (n = 21) was rated as critical. In contrast, overly strict regulations were seen as less obstructive (n = 9). These findings emphasize the importance of standardization, certification, and sustained policy support for widespread implementation.

Figure 37: Survey result for the most relevant institutional factors hampering the adoption of quantum communication adoption



[5] For example, QuNET+BlueCert [367].

Participants were also asked to identify the most critical roadblocks to implementing quantum networks in real-world environments. The predefined options included (multiple answers were possible): a) scalability of quantum memories, b) trusted nodes, c) robustness to environmental noise, d) integration with existing infrastructure, and e) cost and accessibility. Respondents could also provide additional input in a free-text field.

Among 172 responses from 60 participants, cost and accessibility, along with the scalability of quantum memories, were identified as the most critical barriers. High costs and limited availability of quantum hardware and expertise were cited most frequently (n = 46). Scalability challenges of quantum memories, essential for storing quantum information, were also highlighted as major obstacles (n = 40). Additional challenges included integration with existing infrastructure (n = 33), dependency on trusted intermediate nodes that limit true end-to-end security (n = 26), and sensitivity of quantum signals to loss, decoherence, and other environmental effects (n = 23). Overall, high costs, limited hardware availability, and difficulties in scaling reliable quantum memories stand out as the most critical technical and economic barriers.

6.4 Measures

Many of the above discussed challenges need to be addressed by stakeholders from science, industry, and politics to pave the way for achieving technology sovereignty in QCom. In the expert interviews, the initial list of challenges (Table 12) was used to formulate recommended measures for the respective actors. Again, the list of measures does not claim to be exhaustive. It is based on the interview results (2023) and was updated according to the workshop with the SQuaD consortium (2025).

Table 12: Challenges and measures for achieving technology sovereignty in quantum communication technologies within Europe

Dimension	Challenges	Measures
Cost factors	• High investment costs for infrastructure and QCom technologies • High risk for investments • Reliability of investments	• Continuation of public funding • Incentives for end users from industry (e.g., subsidies) • Investments in European infrastructure (e.g., testbeds)
Knowledge factors	• Understanding security aspects • Quantum repeaters • Awareness of QCom	• Education programs for stakeholders from relevant disciplines • Outreach • Promotion of technology transfer to industry
Market factors	• Initial market penetration to boost innovation dynamics • Emergence of markets beyond public institutions • Highly regulated markets • Business models	• Incentives for end users from industry • Cooperation along the value chain • Discuss and develop business models

Dimension	Challenges	Measures
Institutional factors	• Political strategies • Regulations • Proof of security • Bureaucracy	• Standardization and certification activities • Investments in infrastructure (EuroQCI) • Cooperation of authorities of European member states • Streamlined and reduced bureaucracy

Cost factors

Maintaining large and stable public funding levels over the coming decade to minimize the risks for science and industry is crucial for enabling the continuous development of a European quantum communication ecosystem. Funding schemes are still main drivers of the current innovation activities. Aligning these activities with like-minded countries could be used to create synergies.

In addition, greater involvement of industrial actors was deemed necessary. Public funding could be used to incentivize industry activities and open markets beyond public institutions. One possibility could be to introduce subsidies for end users purchasing QCom technologies.

Scaling up the production and miniaturization of QCom systems will be the next step for many start-ups and companies active in this field. This provides the opportunity to reduce production costs and offer the respective products at lower prices.

Public funding should be used to invest in the infrastructure needed to enable QCom in Europe. Currently, public funding is driving the rollout of testbeds. As secure communication infrastructure is critical for Europe and its member states, it cannot solely rely on private-sector investments. The creation of testbeds in Euro-QCI and national funding programs is a valuable starting point.

Knowledge factors

As a skilled workforce is needed to innovate and implement QCom technologies, the education programs developed in the respective funding programs can play an important role for the upcoming years. These programs should take into account the wide range of skills needed. They could specifically address experts of certain disciplines and be tailored to enable interdisciplinary cooperation. Quantum specialist will be only a part of the skilled workforce needed, experts in electronics or communication technologies are at least as essential.

Further knowledge of all the relevant security aspects of complete QCom systems, in particular the interfaces to conventional technologies, should be developed and disseminated into science and industry. On this basis, a proof of security and respective testing procedures for real-world implementations need to be developed. Additionally, the educational needs of further stakeholders of the potential QCom value chain, such as (potentially certified) testing laboratories, should be identified and respective training programs developed.

Furthermore, there should be general awareness-raising about QCom in society to attract potential future workers. This outreach should address the common misconception of quantum technologies as a poorly understood technology field and the notion that QCom is based on “spooky” effects by offering more concrete discussions and technology demonstrations. As quantum communication is still perceived as an exotic technology, this will require targeted efforts.

Industrial players should invest more into acquiring the relevant knowledge about communication security and respective potential threats, as well as about QCom in particular. This should lead to a better understanding of where actions can or should be taken. Potential end users have been identified in the past [372] and should be informed in a targeted manner about the added value offered by QCom technologies.

Market factors

As mentioned above, targeted measures to create markets for early adopters are of great interest to technology providers. These measures could include incentivizing investments for potential end users from industry, opening up sales opportunities, enabling actors to experience the technologies first-hand, offering technology providers a stage to advertise their services and creating reference technologies.

Designing application labs in which new technologies can be demonstrated and analyzed in a non-regulated environment would offer the opportunity to give visibility to QKD solutions and simultaneously identify the most pressing room for further development.

Potential business models on concrete use cases should be discussed for and with all stakeholders in the QCom value chain – their cooperation is essential for developing and implementing market-ready solutions. Networking between science, industry, and policymakers should be promoted in order to clearly communicate the different stakeholders' needs.

Institutional factors

Standardization of QKD technologies on research and commercial level is needed to align different technological pathways and to create comparability. Companies should be encouraged to get involved in standardization processes and to pick up potential outcomes. This includes the promotion of the standards that result from such processes (past and future standards). These efforts are also important in the creation of approval and certification processes for well-defined use cases and devices.

Complex bureaucratic processes in the development and roll-out of quantum communication technologies, such as for acquiring funding (e.g., European funding programs), should be revised and, where advisable, be simplified, replaced, or removed entirely. The regulatory framework should allow flexible cooperation between the relevant stakeholders in science and industry throughout Europe – this includes targeted funding schemes and the limitations that the competition law poses. The responsibilities of the political actors, especially considering the financing of the QCom infrastructure (e.g., what role do the respective ministries play?), should be clarified. The harmonization of activities by European member states should be further promoted. The close exchange among national authorities serves as a role model for cooperation across Europe. The activities within EuroQCI should be continued and extended with the goal of setting up a European QCom infrastructure. The activities towards cross-border testbeds is a suitable next step. Even though national strategies cannot be entirely replaced by European strategies in this field, a European patchwork of regulations and certificates should be prevented wherever possible.

Finally, export control has become increasingly relevant in past discussions on the impact of the regulatory framework on the development of QCom technologies. More clarity is needed to assess the potential future implications for companies active in QCom.

Connecting all the stakeholders along the value chain should be further promoted by policymakers to raise awareness of the upcoming technological developments. In addition, the support of QCom start-ups remains to be essential, as they can give new impulses to technology development and implementation.

7 Conclusions

Quantum communication represents a set of strategically important technologies to enable secure communication and applications beyond this, e.g., links between quantum computers in the future. Several technologies are already commercially available, e.g., quantum key distribution (QKD) – all technologies, however, remain active areas of research.

Quantum communication technologies can be divided into three generations: QKD using the "prepare and measure" principle, QKD using entangled photons, and quantum repeaters with entanglement swapping. QKD meets the need for "quantum-secure" communication and represents one way to exchange physically secure cryptographic keys for secure communication. In particular, QKD could be used in high-security fields (e.g., federal authorities, governments, finance sector, and military). Various versions of this technology are already commercially available. However, challenges to its widespread use include pending security proofs, the high costs of new hardware, and potential users' lack of knowledge about the dangers posed by quantum computing to established encryption methods and about the potential solutions (e.g., QKD). Beyond QKD, quantum repeaters represent an important technology. These could be used to overcome the range limitation of QKD and to reduce dependence on potentially insecure "trusted nodes", and to enable distributed quantum sensing or connect quantum computers over longer distances using entanglement distribution. Linking quantum computers in such a way could drastically increase the performance and possible applications of quantum computers.

Overall, several technologies (e.g., quantum repeaters) still require research and development to deliver market-ready products and to be able to fully exploit the potential of quantum communication. In addition, the obstacles to widespread market use must be addressed, including the lack of security proof for an implemented system, certification and approval. This requires the close cooperation of different stakeholders from research, industry, and the public sectors (authorities, policymakers). Furthermore, our new survey verified recent developments in long-distance Twin-Field QKD and quantum communication beyond QKD, such as distributed quantum computing, which will add momentum in this field, although still at the research level.

For these reasons, quantum communication has been recognized internationally as a strategically relevant field of research, and numerous countries have set up related research and funding strategies and programs. Germany and Europe play a major role here in an international comparison and are on an equal footing in terms of research and development, which is reflected in the high level of publication and patenting activities. Due to the high strategic relevance of quantum communication, considerations about technology sovereignty are playing an increasingly important role. Germany and the EU should continue to consider and discuss which goals are to be achieved and which measures need to be taken to achieve the envisaged degree of technology sovereignty.

Quantum communication is a strategically important topic, and these technologies are attracting significant interest from numerous countries and regions. Germany and Europe must consider how to provide continuous support for technology development in order to achieve the strategic goal of technology sovereignty in quantum communication that they have set themselves.

In addition, since the publication of the first monitoring report, many countries have updated or are preparing new strategies related to quantum technologies, or have released additional documents to outline specific objectives for implementing their main strategies. In many cases, these strategic documents include objectives for quantum communication. This rapid update of global strategies highlights the importance of continuous monitoring activities on this technology, enabling Germany and Europe to keep pace with the actions of other countries and to adjust their own activities in a timely manner.

8 Acknowledgements

The authors gratefully acknowledge the funding by the Federal Ministry of Research, Technology and Space – Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR), Germany.

Funding reference: 16KISQ116, 16KISQ115, 16KISQ112K

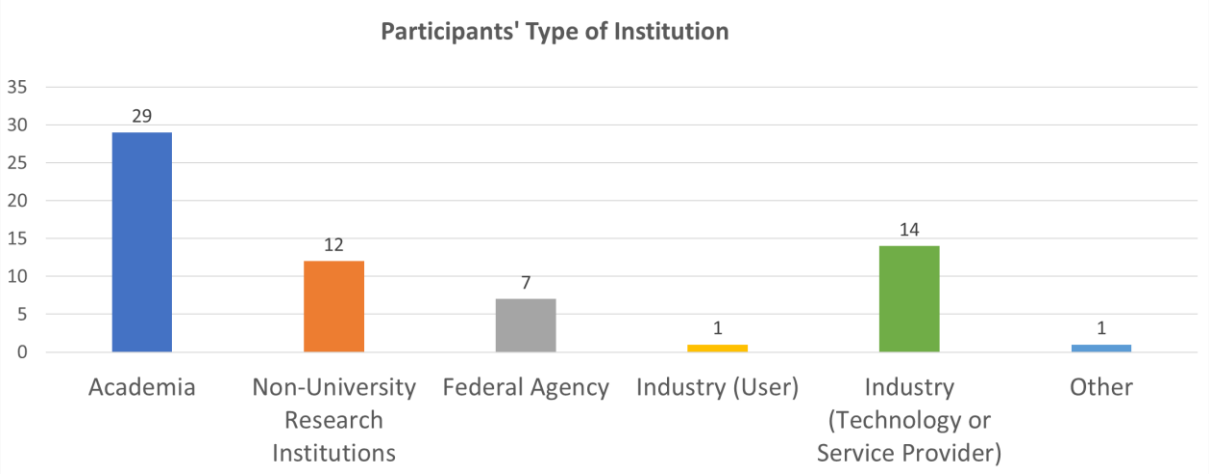
We would like to thank all the experts from academia and industry who supported us by participating in interviews and the survey. Furthermore, we would like to thank our colleagues from Fraunhofer ISI: Karin Herrmann for layout work; Paul Städter and Yuting Yang for research on market studies; Louise Antill-Blum for English language corrections; and Prof. Ulrich Schmoch for patent and publication analysis.

We would like to thank our colleagues Sebastian Koke, Nino Walenta, Thorsten A. Goebel, Ralf-Peter Braun, Tara Liebisch, and Anya Samadi for their valuable input regarding the testbed infrastructure in Germany, Elias X. Huber regarding the quantum communication R&I in China.

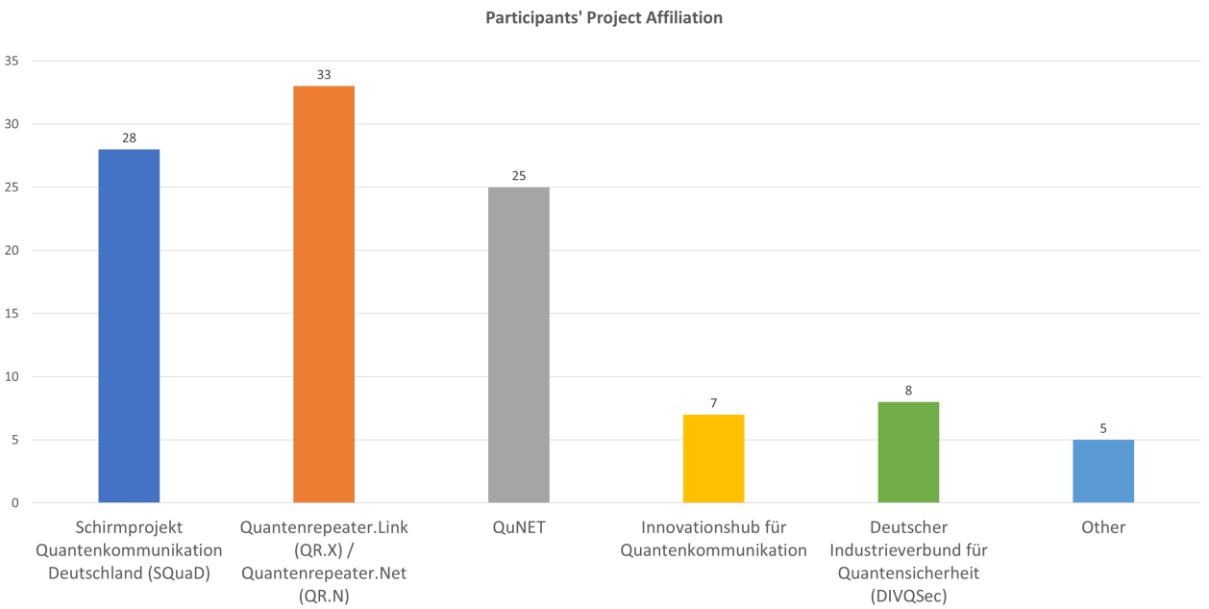
Finally, we also wish to thank all of our colleagues in the SQuaD consortium for their continuous support.

A.1 Survey - Questions and Answers

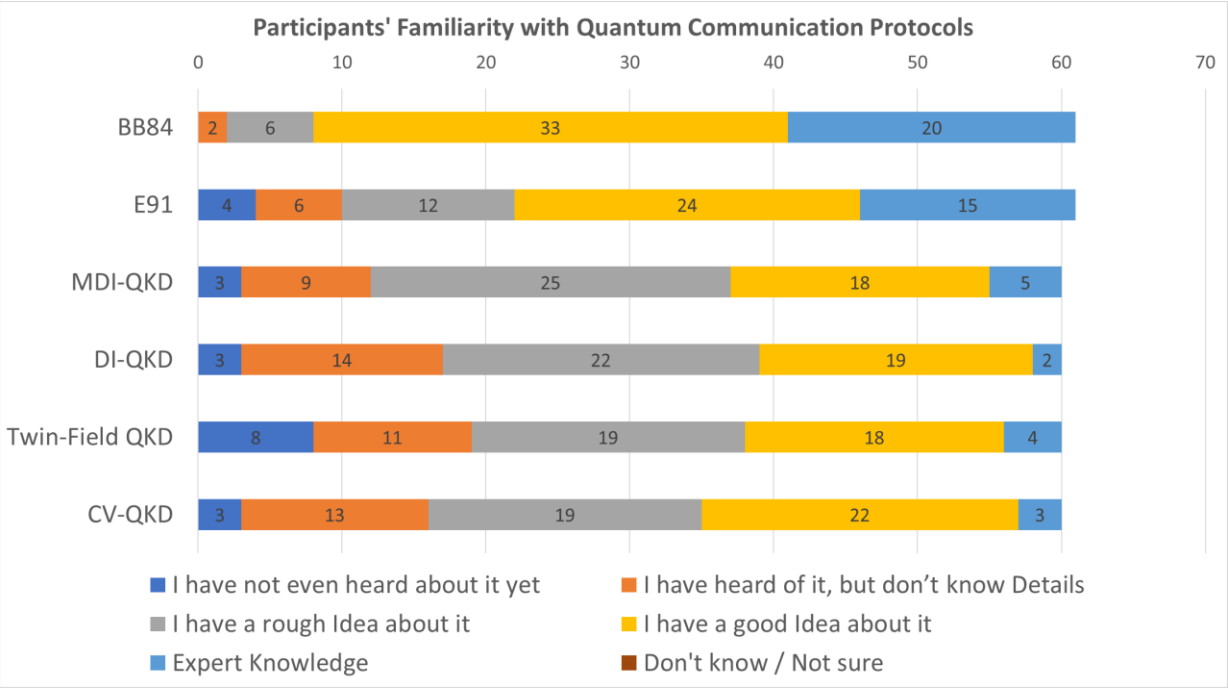
I. Introduction



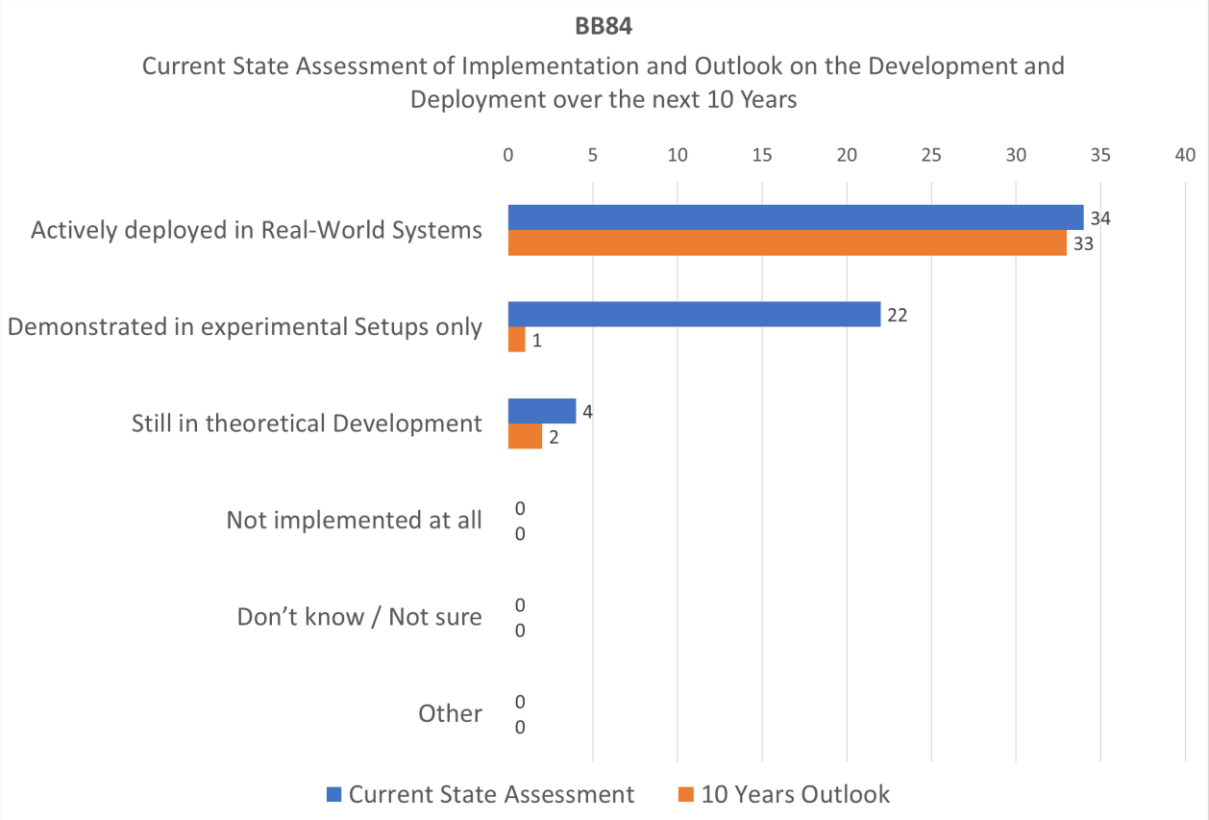
Question 1: Which Type of Institution do you work for?



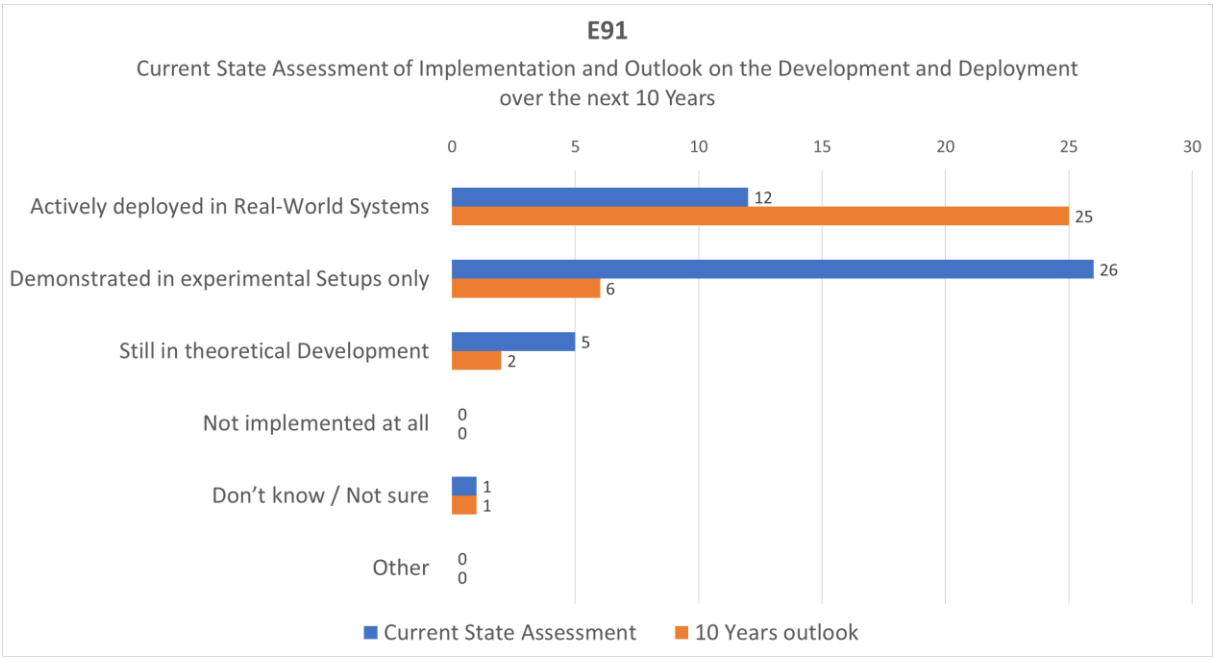
Question 2: Please indicate, if your Institution is Part of the following Projects and Initiatives.



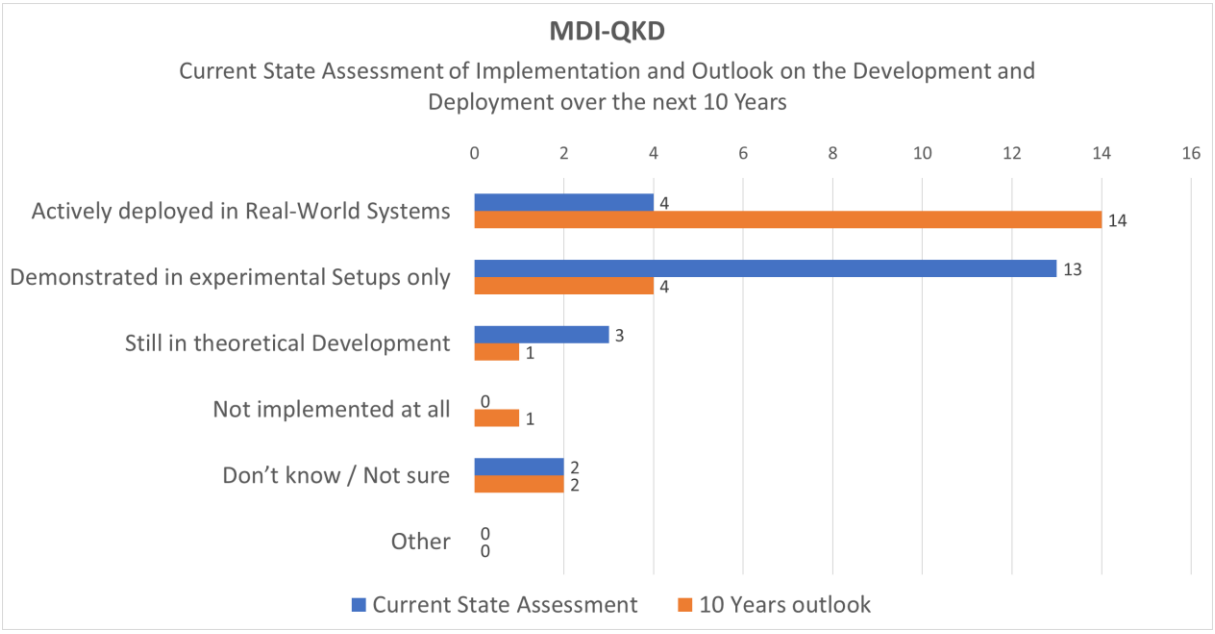
Question 3: How familiar are you with the following Quantum Communication Protocols?



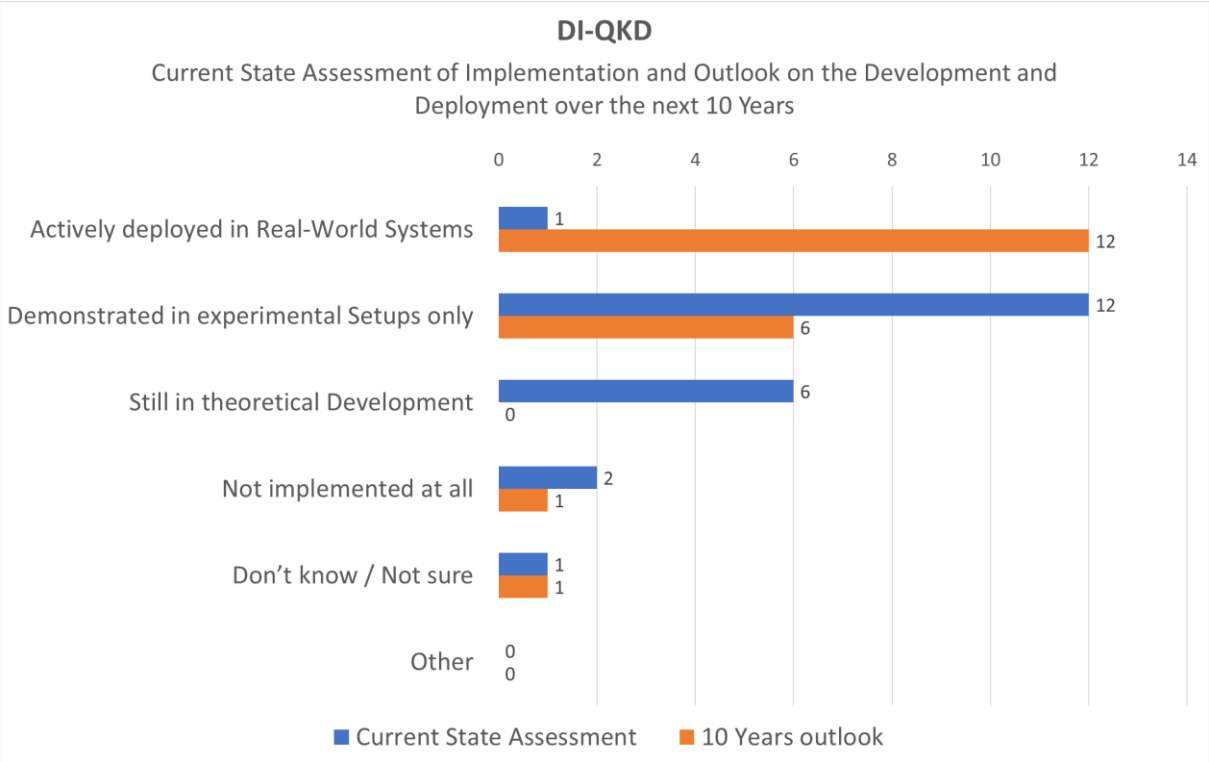
Question 4: How would you assess the current State of BB84 Implementation in Real-world Settings? And what is your Outlook on the Development and Real-world Deployment of BB84 over the next 10 years?



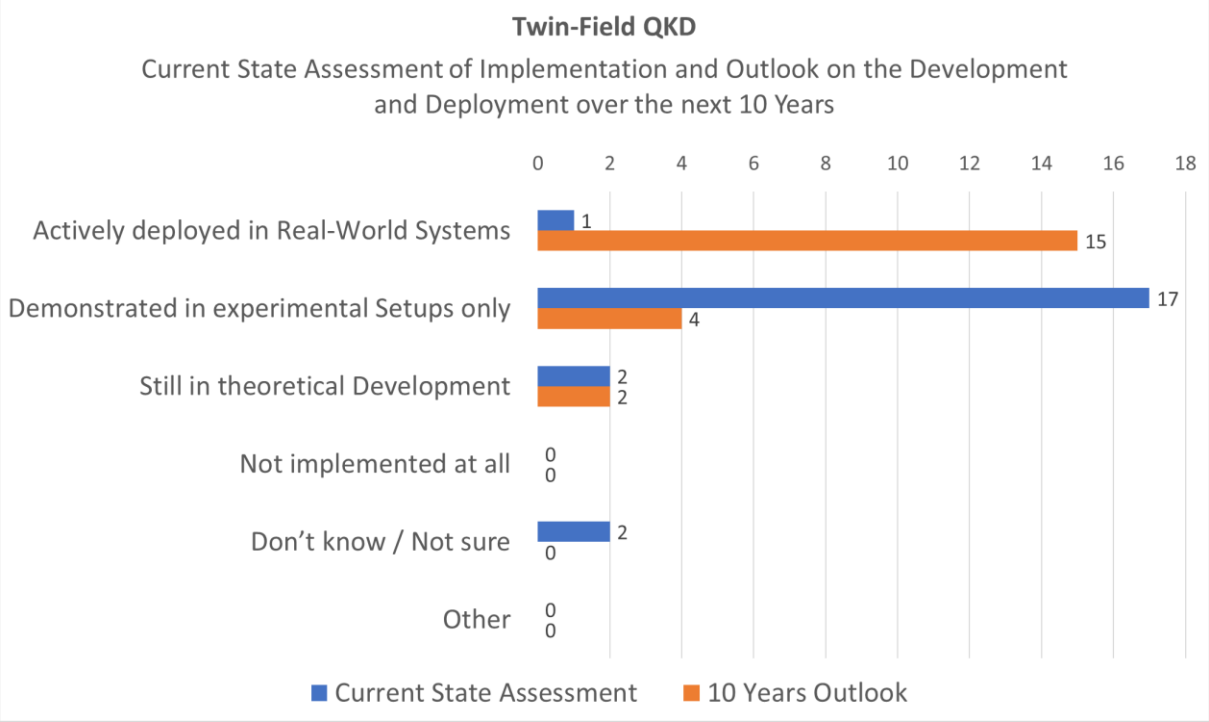
Question 5: How would you assess the current State of E91 Implementation in Real-world Settings? And what is your Outlook on the Development and Real-world Deployment of E91 over the next 10 years?



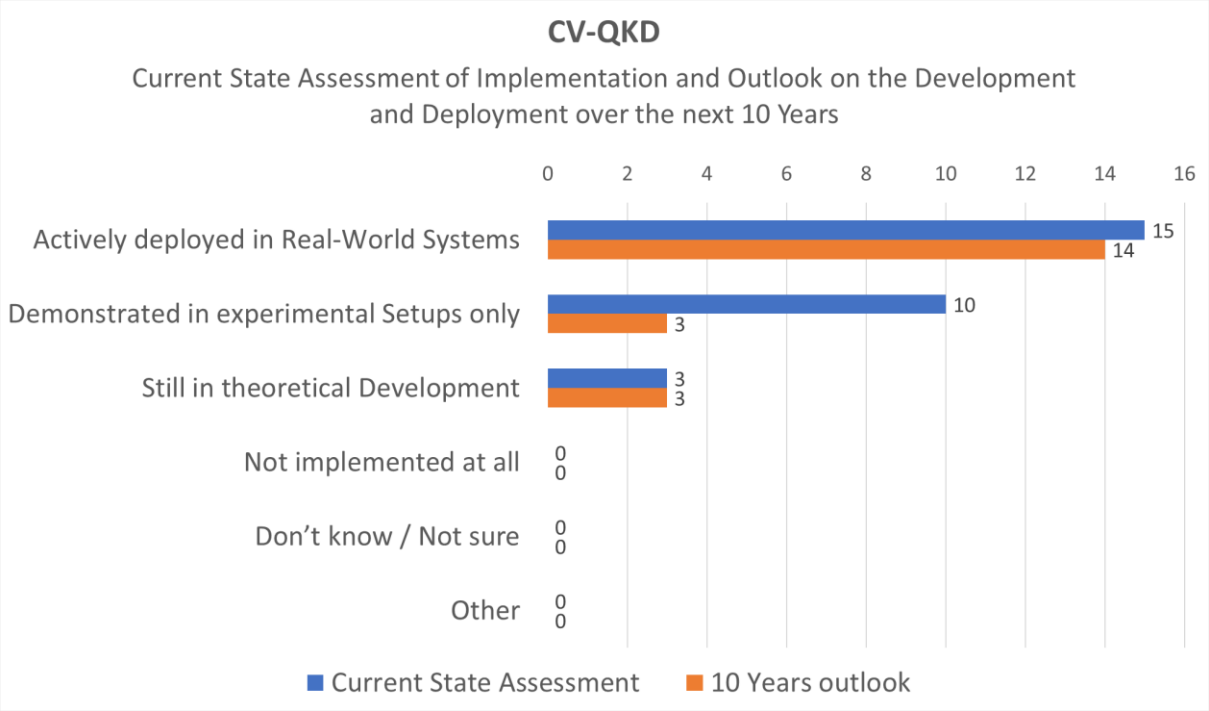
Question 6: How would you assess the current State of MDI-QKD Implementation in Real-world Settings? And what is your Outlook on the Development and Real-world Deployment of MDI-QKD over the next 10 years?



Question 7: How would you assess the current State of DI-QKD Implementation in Real-world Settings? And what is your Outlook on the Development and Real-world Deployment of DI-QKD over the next 10 years?

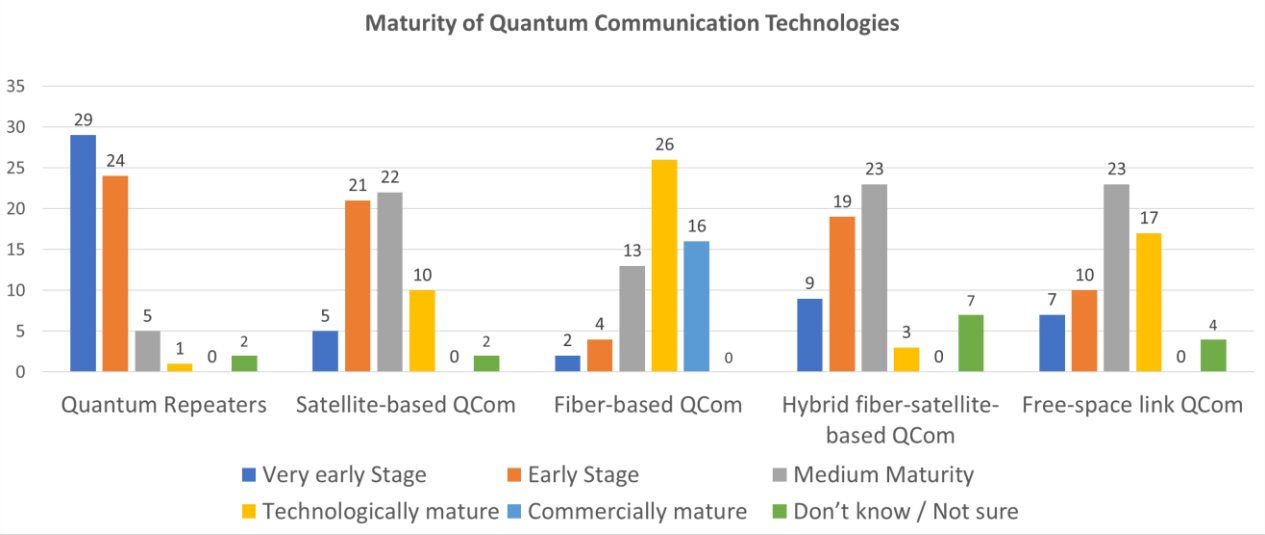


Question 8: How would you assess the current State of Twin-Field QKD Implementation in Real-world Settings? And what is your Outlook on the Development and Real-world Deployment of Twin-Field QKD over the next 10 years?

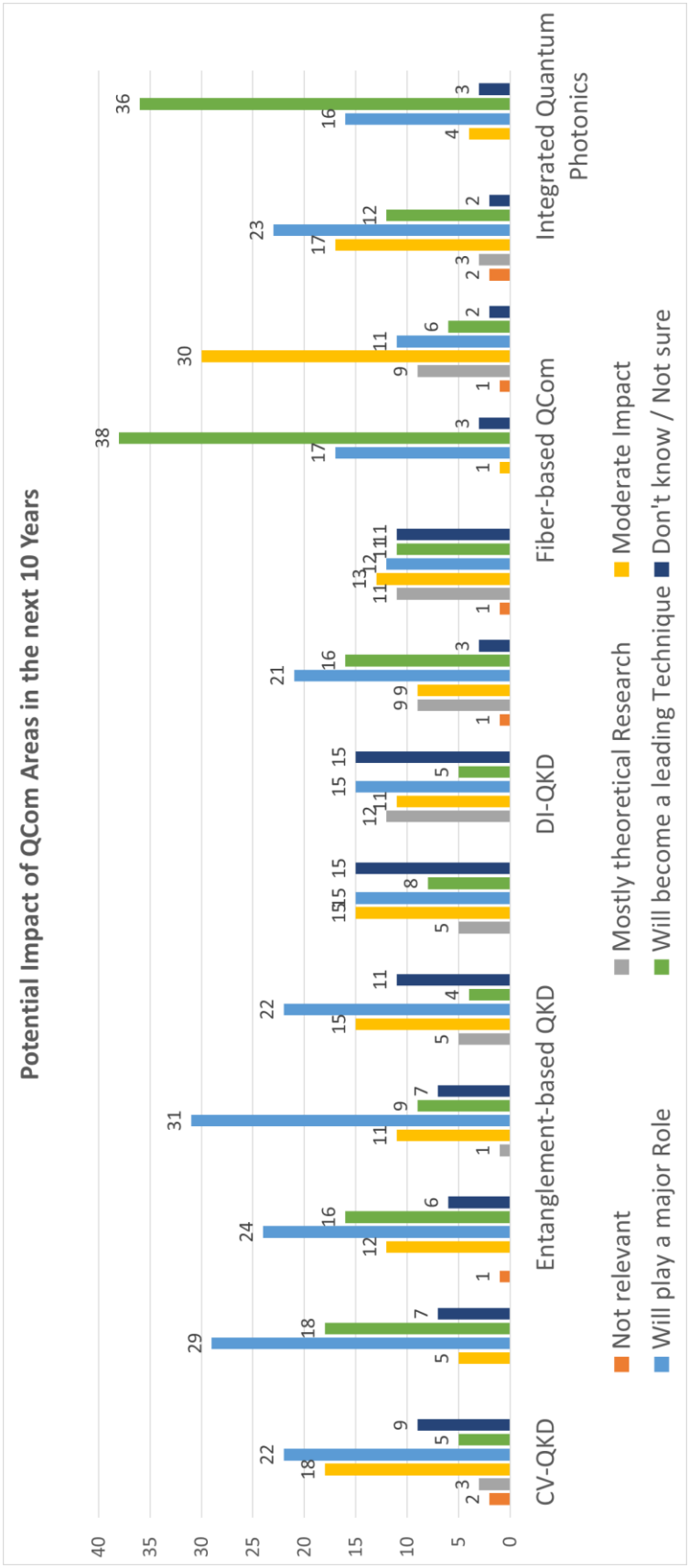


Question 9: How would you assess the current State of CV-QKD Implementation in Real-world Settings? And what is your Outlook on the Development and Real-world Deployment of CV-QKD over the next 10 years?

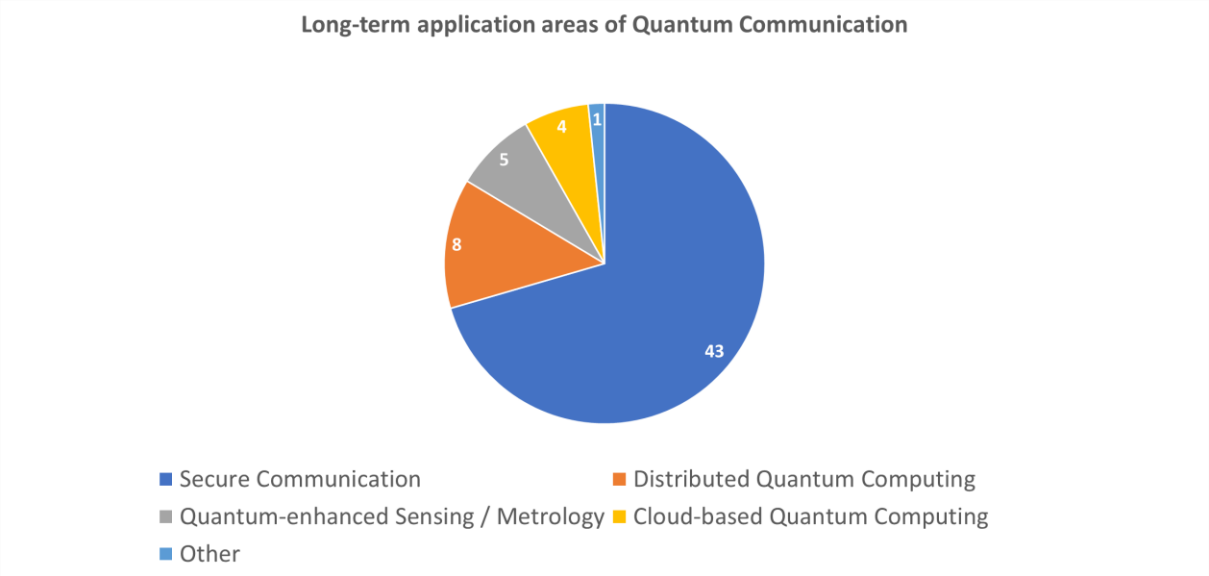
II. Quantum Communication / Quantum Technology



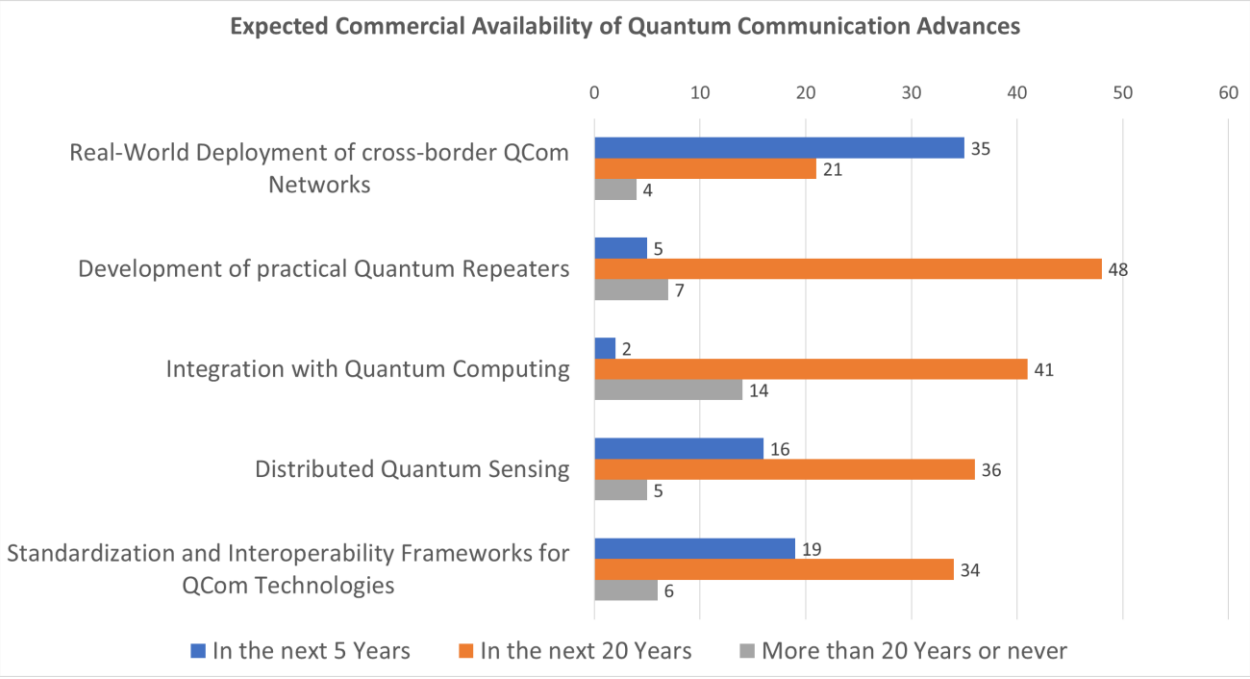
Question 10: How would you assess the Maturity of the following Quantum Communication Technologies?



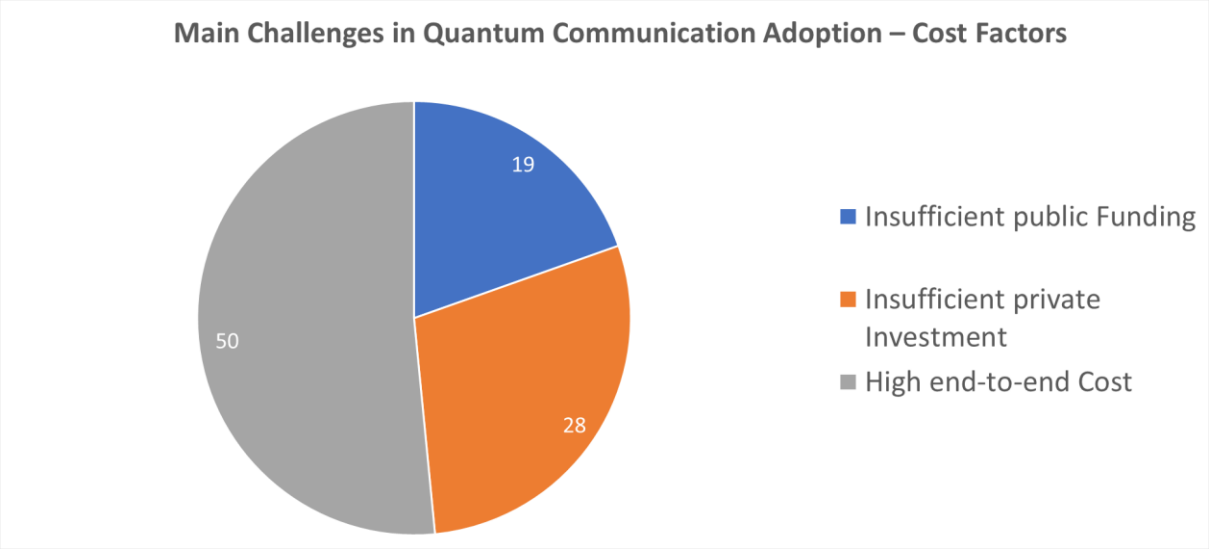
Question 11: Considering recent Research Trends, how would you assess the potential Impact of the following Areas on Quantum Communication in the next 10 Years?



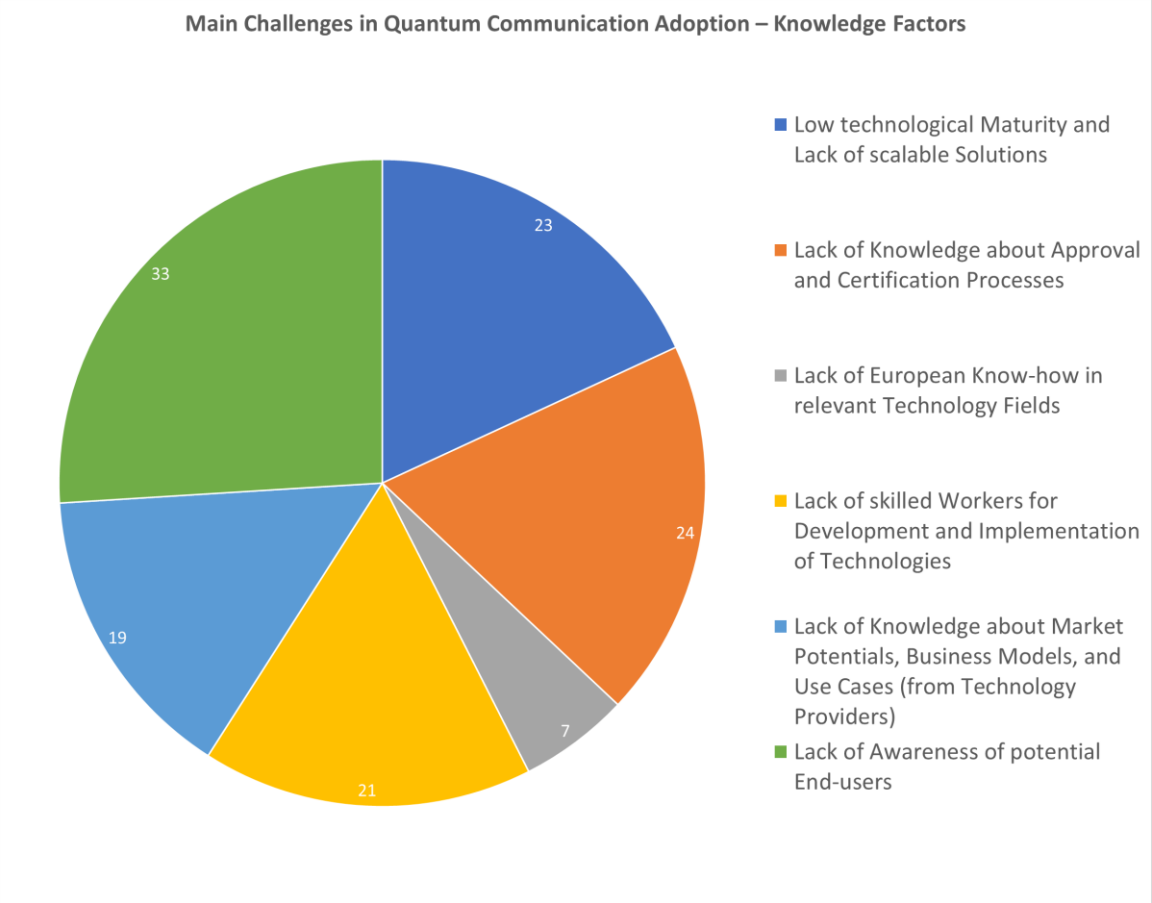
Question 12: Which Application Area do you believe will benefit the most from Quantum Communication Technologies in the long Term?



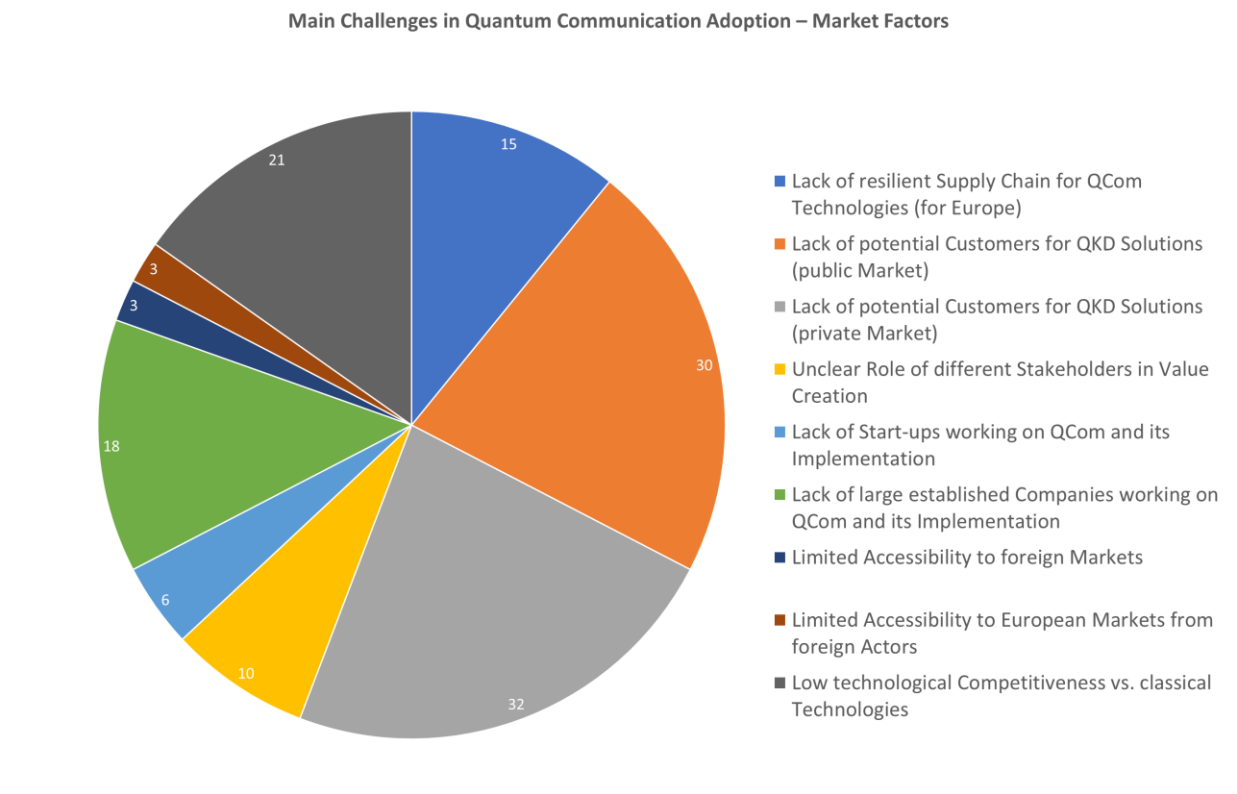
Question 13: Which of the following Advances in Quantum Communication do you expect to become commercially available beyond Lab Demonstrations in the Future?



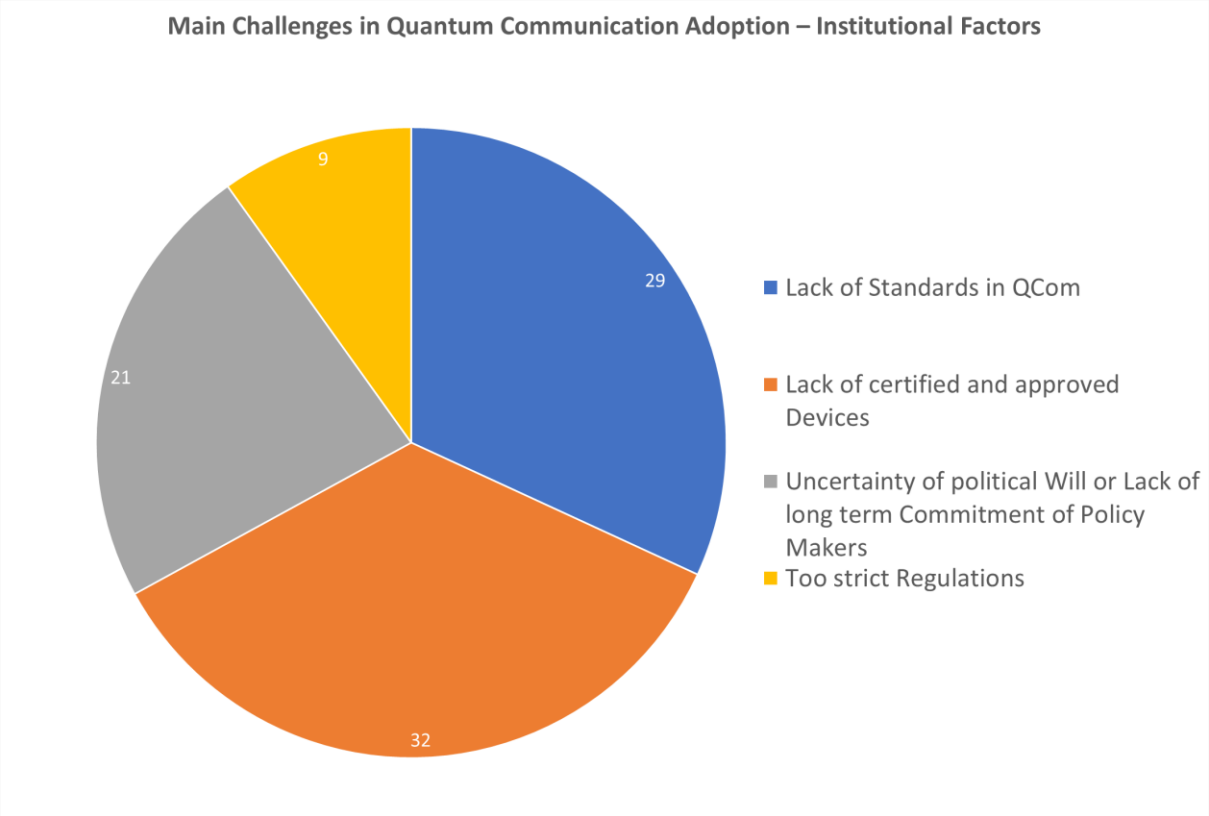
Question 14: What are the Main Challenges preventing the widespread Implementation of Quantum Communication? - Cost Factors



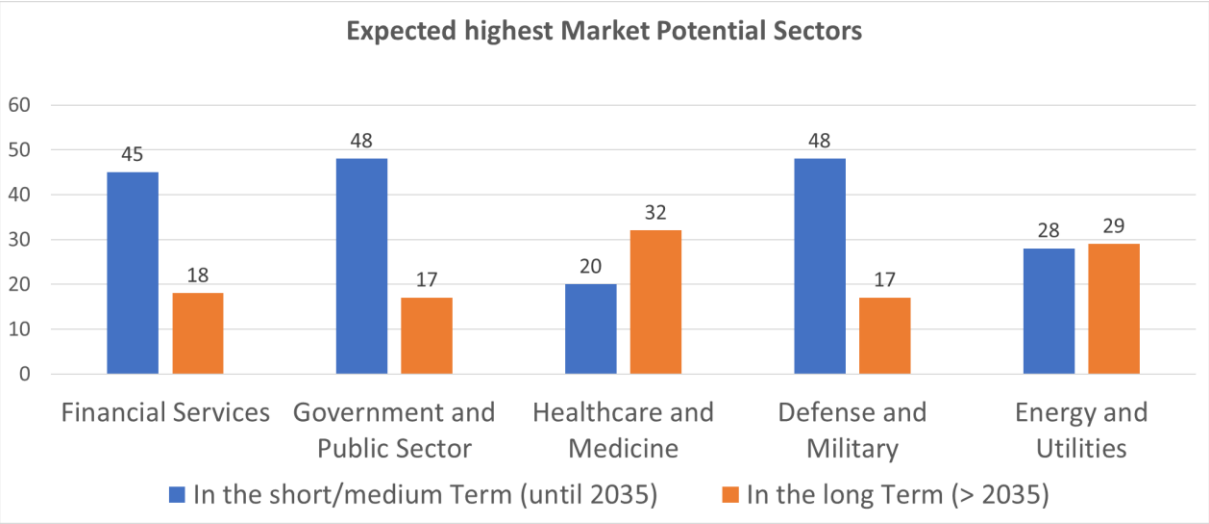
Question 15: What are the Main Challenges preventing the widespread Implementation of Quantum Communication? - Knowledge Factors



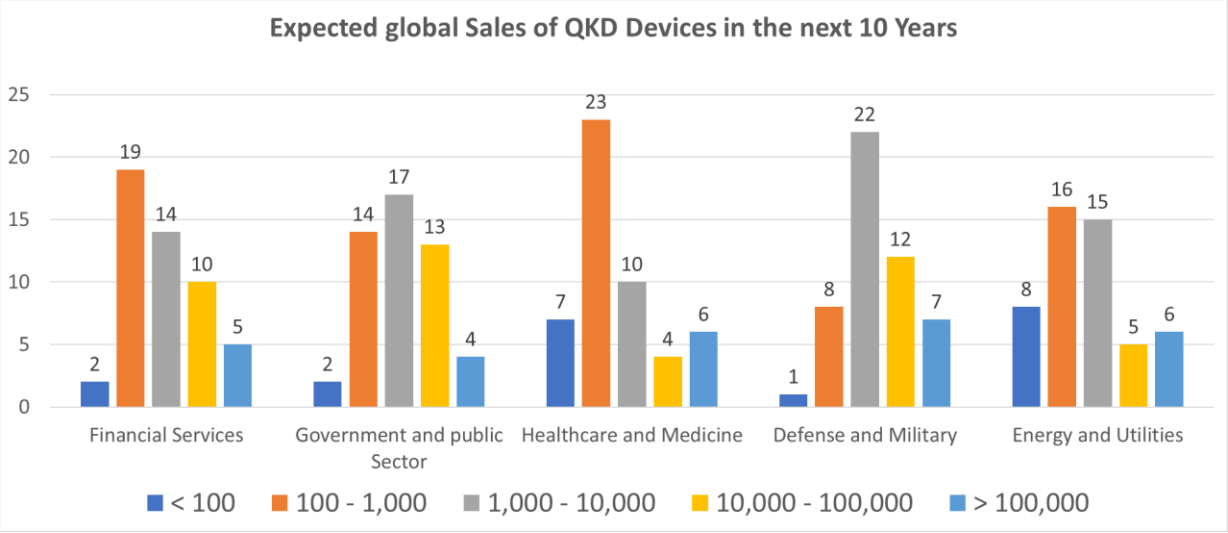
Question 16: What are the Main Challenges preventing the widespread Implementation of Quantum Communication? - Market Factors



Question 17: What are the Main Challenges preventing the widespread Implementation of Quantum Communication? - Institutional Factors

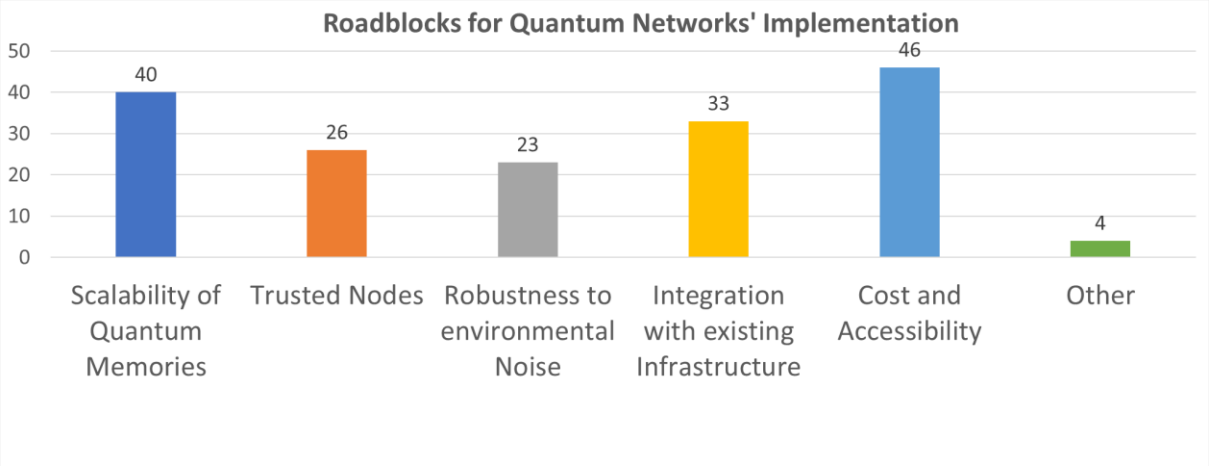


Question 18: In which Sectors do you believe Quantum Communication has large Market Potential?

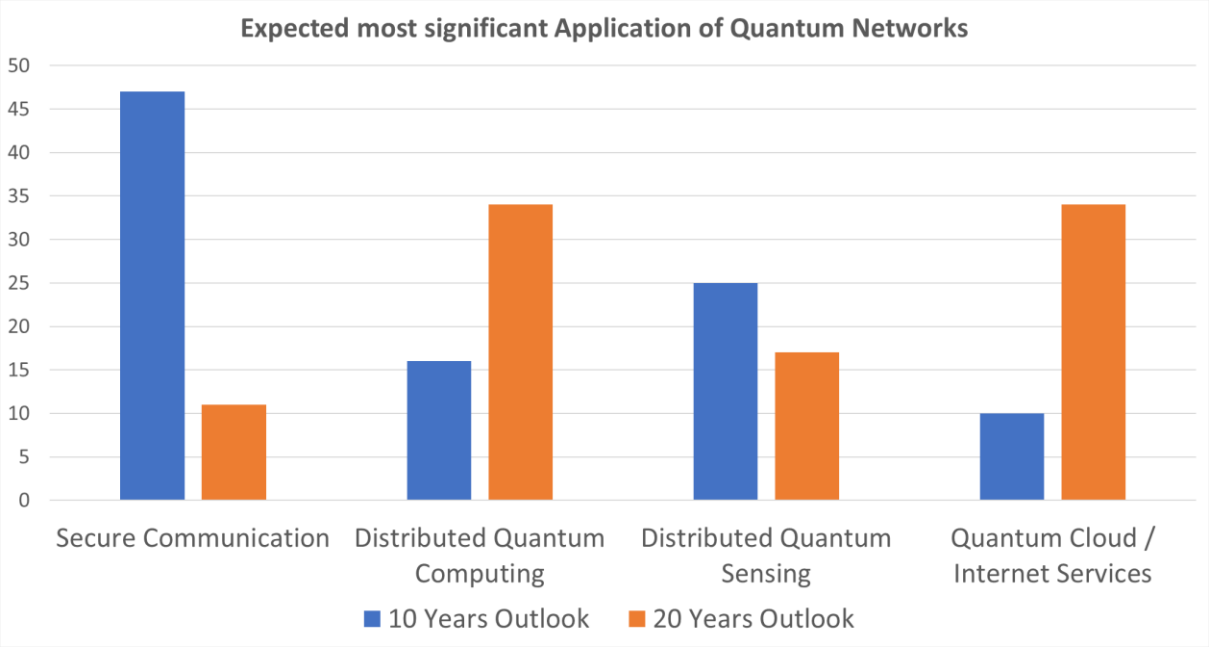


Question 19: How many QKD Devices could be sold globally in the next 10 Years in the following Markets?

III. Quantum Networks



Question 20: What do you consider the most critical Factors (Roadblocks) for implementing Quantum Networks in Real-world Environments?



Question 21: Quantum Networks enable the Transmission of Quantum Information between physically separated Nodes. If these nodes include Quantum Memories with long Coherence Times, Entanglement can be distributed across the Network. What do you believe will be the most significant Application of Quantum Networks in the Future?

References

[1] Schmaltz T, Endo C, Becher C, Schmidt J, Krieg L, Weymann L and Shirinzadeh S 2024 *Monitoring Report 1 - Quantum Communication* https://doi.org/10.24406/publica-3285

[2] Bundesministerium für Forschung, Technologie und Raumfahrt - BMFTR *Startseite — Vernetzung und Sicherheit digitaler Systeme* https://www.forschung-it-sicherheit-kommunikationssysteme.de/ (accessed 10 Dec 2025)

[3] Cordis *Projects & results | CORDIS | European Commission* https://cordis.europa.eu/projects (accessed 16 Oct 2025)

[4] National Quantum Initiative *National Quantum Coordination Office (NQCO)* https://www.quantum.gov/ (accessed 18 Oct 2025)

[5] UKRI *UK National Quantum Technologies Programme* https://uknqt.ukri.org/ (accessed 17 Oct 2025)

[6] Cabinet Office Home Page *Quantum Technology Innovation* https://www8.cao.go.jp/cstp/ryoshigijutsu/ryoshigijutsu.html (accessed 17 Oct 2025)

[7] OECD 2025 *A quantum technologies policy primer - OECD Digital Economy Papers (OECD Digital Economy Papers* No. 371*)* (Paris)

[8] subcommittee on quantum information science committee on science of the national science & technology council 2024 *NATIONAL QUANTUM INITIATIVE SUPPLEMENT TO THE PRESIDENT'S FY 2025 BUDGET*

[9] Cabinet Office *Expert Panel of Quantum Technology Innovation* https://www8.cao.go.jp/cstp/ryoshigijutsu/expert_panel.html (accessed 19 Jan 2026)

[10] Deutscher Bundestag 2025 *Antwort der Bundesregierung der Fraktion der CDU/CSU – Drucksache 20/14569 –: Aktueller Umsetzungsstand des Handlungskonzeptes Quantentechnologien der Bundesregierung* https://dserver.bundestag.de/btd/20/149/2014986.pdf

[11] Lewis A, Scudo P, Cerutti I, Travagnin M, Marcantonini C, Ascheri A, Nardo M, Di Girolamo F, Zaurino E and Martinez Cillero M 2025 *Future Directions for Quantum Technology in Europe* (Luxembourg (Luxembourg)) https://data.europa.eu/doi/10.2760/0891087

[12] Edler J *et al* 2020 *Technology sovereignty. From demand to concept* (Karlsruhe: Fraunhofer ISI) https://www.isi.fraunhofer.de/content/dam/isi/dokumente/publikationen/technology_sovereignty.pdf

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

[14] Bundesamt für Sicherheit in der Informationstechnik 2020 *Entwicklungsstand Quantencomputer* (Bundesamt für Sicherheit in der Informationstechnik) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Zusammenfassung-V_1_2.pdf?__blob=publicationFile&v=1

[15] Bundesministerium für Bildung und Forschung (BMBF, now called BMFTR) 2018 *Quantentechnologien – von den Grundlagen zum Markt: Rahmenprogramm der Bundesregierung* https://www.bmftr.bund.de/SharedDocs/Publikationen/DE/5/31432_Rahmenprogramm_Quantentechnologien.pdf?__blob=publicationFile&v=6

[16] 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)

[17] Liu Y-K and Moody D 2024 Post-quantum cryptography and the quantum future of cybersecurity **21** 40501

[18] CSRC | NIST 2022 *Announcing PQC Candidates to be Standardized, Plus Fourth Round Candidates | CSRC* https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4 (accessed 15 May 2026)

[19] NIST 2025 *NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption* https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption (accessed 7 May 2026)

[20] Bundesministerium für Forschung, Technologie und Raumfahrt - BMFTR 2025 *Hightech Agenda Deutschland* https://www.bmftr.bund.de/SharedDocs/Publikationen/DE/L/31881_Hightech_Agenda_Deutschland.pdf?__blob=publicationFile&v=14 (accessed 7 May 2026)

[21] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned *Nature* **299** 802–3

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

[23] 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)

[24] 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)

[25] Ralph T C 1999 Continuous variable quantum cryptography *Phys. Rev. A* **61** 010303(R)

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

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

[28] 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

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

[30] CORDIS - Forschungsergebnisse der EU *Development of a Global Network for Secure Communication based on Quantum Cryptography* (CORDIS - Forschungsergebnisse der EU) https://cordis.europa.eu/project/id/506813/de

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

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

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

[34] 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)

[35] 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)

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

[37] Chen H-Z *et al* 2025 Implementation of carrier-grade quantum communication networks over 10000 km *npj Quantum Inf* **11** 137

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

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

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

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

[42] 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)

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

[44] 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

[45] Dynes J F *et al* 2019 Cambridge quantum network *npj Quantum Inf* **5** 101

[46] 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

[47] European Commission *Shaping Europe's digital future: The European Quantum Communication Infrastructure (EuroQCI) Initiative* https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (accessed 26 Sep 2025)

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

[49] Chen J-P *et al* 2021 Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas *Nat. Photon.* **15** 570–5

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

[51] 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

[52] Hajomer A A E, Bruynsteen C, Derkach I, Jain N, Bomhals A, Bastiaens S, Andersen U L, Yin X and Gehring T 2024 Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receiver *Optica* **11** 1197

[53] Wang H *et al* 2025 High-rate continuous-variable quantum key distribution over 100 km fiber with composable security *Optica* **12** 1657

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

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

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

[57] Bundesministerium für Forschung, Technologie und Raumfahrt - BMFTR *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)

[58] 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

[59] Horoschenkoff P *et al* 2025 DemoQuanDT: a carrier-grade QKD network *J. Opt. Commun. Netw.* **17** 743

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

[61] Bundesministerium für Forschung, Technologie und Raumfahrt - BMFTR *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)

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

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

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

[65] 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

[66] Weedbrook C 2013 Continuous-variable quantum key distribution with entanglement in the middle *Phys. Rev. A* **87** 22308

[67] 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

[68] 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

[69] Joshi S K *et al* 2020 A trusted node-free eight-user metropolitan quantum communication network *Science advances* **6** eaba0959

[70] 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

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

[72] Alqedra M K, Huang C-T, Yeung E, Chang W-H, Haffouz S, Poole P J, Dalacu D, Elshaari A W and Zwiller V 2025 Entangled Photon Pair Generation in the Telecom O-Band from Nanowire Quantum Dots *Nano letters* **25** 10321–7

[73] Basso Basset F *et al* 2021 Quantum key distribution with entangled photons generated on demand by a quantum dot *Science advances* **7** eabe6379

[74] 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** eabe8905

[75] Hreibi A, Kniggendorf A-K, Kuhl A, Kronjäger J, Schnatz H and Kück S 2025 Entanglement-based intercity quantum key distribution: Metrology and implementation *Measurement: Sensors* **38** 101777

[76] Sena M *et al* 2025 High-fidelity quantum entanglement distribution in metropolitan fiber networks with co-propagating classical traffic *J. Opt. Commun. Netw.* **17** 1072

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

[78] 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

[79] Zhuang S-C *et al* 2025 Ultrabright Entanglement Based Quantum Key Distribution over a 404 km Optical Fiber *Physical review letters* **134** 230801

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

[81] Bundesministerium für Forschung, Technologie und Raumfahrt - BMFTR *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)

[82] 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.** 10

[83] 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

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

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

[86] 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

[87] 2021 *Souverän. Digital. Vernetzt.: Forschungsprogramm Kommunikationssysteme* https://www.bmftr.bund.de/SharedDocs/Publikationen/DE/5/31677_Souveraen_Digital_Vernetzt.html

[88] Josephine Dias and Tim C. Ralph 2017 *Quantum repeaters using continuous-variable teleportation* https://journals.aps.org/pra/abstract/10.1103/PhysRevA.95.022312 (accessed 6 Jun 2024)

[89] Seshadreesan K P, Krovi H and Guha S 2020 Continuous-variable quantum repeater based on quantum scissors and mode multiplexing *Phys. Rev. Research* **2** 13310

[90] 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

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

[92] Bundesministerium für Forschung, Technologie und Raumfahrt *Quantenrepeater.Net - QR.N* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/quantenrepeater-net-qr.n (accessed 6 Feb 2026)

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

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

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

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

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

[98] 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 *Optica Quantum* **1** 94–102

[99] 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** 20307

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

[101] 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

[102] Kucera S *et al* 2024 Demonstration of quantum network protocols over a 14-km urban fiber link *npj Quantum Inf* **10.** 88

[103] Thomas J M, Yeh F I, Chen J H, Mambretti J J, Kohlert S J, Kanter G S and Kumar P 2024 Quantum teleportation coexisting with classical communications in optical fiber *Optica* **11** 1700

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

[105] Bergerhoff M, Elshehy O, Kucera S, Kreis M and Eschner J 2024 Quantum repeater node with free-space coupled trapped ions *Phys. Rev. A* **110** 32603

[106] 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

[107] Stolk A J *et al* 2024 Metropolitan-scale heralded entanglement of solid-state qubits *Science advances* **10** eadp6442

[108] Liu J-L *et al* 2024 Creation of memory-memory entanglement in a metropolitan quantum network *Nature* **629** 579–85

[109] 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** 23086

[110] Wallnöfer J, Hahn F, Wiesner F, Walk N and Eisert J 2024 Faithfully simulating near-term quantum repeaters *PRX Quantum* **5** 10351

[111] Da Silva F F, Avis G, Slater J A and Wehner S 2024 Requirements for upgrading trusted nodes to a repeater chain over 900 km of optical fiber *Quantum Sci. Technol.* **9** 45041

[112] 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** 10202

[113] Bassoli R, Boche H, Deppe C, Ferrara R, Fitzek F H P, Janssen G and Saeedinaeeni S 2021 Quantum Communication Networks: Design and Simulation *Quantum Communication Networks* (Cham: Springer) pp 187–209

[114] 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** 45006

[115] 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)

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

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

[118] Chang X-Y, Hou P-Y, Zhang W-G, Meng X-Q, Yu Y-F, Lu Y-N, Liu Y-Q, Qi B-X, Deng D-L and Duan L-M 2025 Hybrid entanglement and bit-flip error correction in a scalable quantum network node *Nat. Phys.* **21** 583–9

[119] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 Overcoming the rate-distance limit of quantum key distribution without quantum repeaters *Nature* **557** 400–3

[120] Ma X, Zeng P and Zhou H 2018 Phase-Matching Quantum Key Distribution *Phys. Rev. X* **8** 31043

[121] Wang X-B, Yu Z-W and Hu X-L 2018 Twin-field quantum key distribution with large misalignment error *Phys. Rev. A* **98** 62323

[122] Pittaluga M, Minder M, Lucamarini M, Sanzaro M, Woodward R I, Li M-J, Yuan Z and Shields A J 2021 600-km repeater-like quantum communications with dual-band stabilization *Nat. Photon.* **15** 530–5

[123] Wang S *et al* 2022 Twin-field quantum key distribution over 830-km fibre *Nat. Photon.* **16** 154–61

[124] Zhou L *et al* 2024 Independent-optical-frequency-comb-powered 546-km field test of twin-field quantum key distribution *Phys. Rev. Applied* **22** 64057

[125] Du H, Paraiso T K, Pittaluga M, Lo Y S, Dolphin J A and Shields A J 2024 Twin-field quantum key distribution with optical injection locking and phase encoding on-chip *Optica* **11** 1385

[126] Pittaluga M *et al* 2025 Long-distance coherent quantum communications in deployed telecom networks *Nature* **640** 911–7

[127] Mandil R, Qian L and Lo H-K 2025 Long-fiber Sagnac interferometers for twin-field quantum key distribution networks *Phys. Rev. Applied* **23** 34040

[128] Zheng Y *et al* 2026 Large-scale quantum communication networks with integrated photonics *Nature* **651** 68–75

[129] Peng Q, Chen J-P, Xing T, Wang D, Wang Y, Liu Y and Huang A 2025 Practical security of twin-field quantum key distribution with optical phase-locked loop under wavelength-switching attack *npj Quantum Inf* **11.** 7

[130] Kimble H J 2008 The quantum internet *Nature* **453** 1023–30

[131] Main D, Drmota P, Nadlinger D P, Ainley E M, Agrawal A, Nichol B C, Srinivas R, Araneda G and Lucas D M 2025 Distributed quantum computing across an optical network link *Nature* **638** 383–8

[132] Saha S, Shalaev M, O'Reilly J, Goetting I, Toh G, Kalakuntla A, Yu Y and Monroe C 2025 High-fidelity remote entanglement of trapped atoms mediated by time-bin photons *Nature communications* **16** 2533

[133] Inc Photonic *et al* 2024 *Distributed Quantum Computing in Silicon*

[134] Storz S *et al* 2023 Loophole-free Bell inequality violation with superconducting circuits *Nature* **617** 265–70

[135] Song J, Yang S, Liu P, Zhang H-L, Xue G-M, Mi Z-Y, Zhang W-G, Yan F, Jin Y-R and Yu H-F 2025 Realization of High-Fidelity Perfect Entanglers between Remote Superconducting Quantum Processors *Physical review letters* **135** 50603

[136] Sekine A, Murakami R and Doi Y 2025 Microwave-to-Optical Quantum Transduction of Photons for Quantum Interconnects *Phys. Rev. B* **112** 94413

[137] Brubaker B M, Kindem J M, Urmey M D, Mittal S, Delaney R D, Burns P S, Vissers M R, Lehnert K W and Regal C A 2022 Optomechanical Ground-State Cooling in a Continuous and Efficient Electro-Optic Transducer *Phys. Rev. X* **12** 21062

[138] Sahu R, Hease W, Rueda A, Arnold G, Qiu L and Fink J M 2022 Quantum-enabled operation of a microwave-optical interface *Nature communications* **13** 1276

[139] Arnold G, Werner T, Sahu R, Kapoor L N, Qiu L and Fink J M 2025 All-optical superconducting qubit readout *Nature physics* **21** 393–400

[140] Zhao H, Chen W D, Kejriwal A and Mirhosseini M 2025 Quantum-enabled microwave-to-optical transduction via silicon nanomechanics *Nature nanotechnology* **20** 602–8

[141] Barz S, Kashefi E, Broadbent A, Fitzsimons J F, Zeilinger A and Walther P 2012 Demonstration of blind quantum computing *Science* **335** 303–8

[142] Barz S, Fitzsimons J F, Kashefi E and Walther P 2013 Experimental verification of quantum computation *Nature Phys* **9** 727–31

[143] Wei Y-C *et al* 2025 Universal distributed blind quantum computing with solid-state qubits *Science* **388** 509–13

[144] Pezzè L, Smerzi A, Oberthaler M K, Schmied R and Treutlein P 2018 Quantum metrology with nonclassical states of atomic ensembles *Rev. Mod. Phys.* **90** 35005

[145] Nichol B C, Srinivas R, Nadlinger D P, Drmota P, Main D, Araneda G, Ballance C J and Lucas D M 2022 An elementary quantum network of entangled optical atomic clocks *Nature* **609** 689–94

[146] Wu S, Bao G, Guo J, Chen J, Du W, Shi M, Yang P, Chen L and Zhang W 2023 Quantum magnetic gradiometer with entangled twin light beams *Science advances* **9** eadg1760

[147] Huxter W S, Palm M L, Davis M L, Welter P, Lambert C-H, Trassin M and Degen C L 2022 Scanning gradiometry with a single spin quantum magnetometer *Nature communications* **13** 3761

[148] Stas P-J *et al* 2026 Entanglement-assisted non-local optical interferometry in a quantum network *Nature* **651** 326–32

[149] Bennett C H and Wiesner S J 1992 Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states *Physical review letters* **69** 2881–4

[150] Wolff L H, Belzig P, Christandl M, Durhuus B and Tomamichel M 2025 Fundamental Limit on the Power of Entanglement Assistance in Quantum Communication *Physical review letters* **134** 20802

[151] Hao S, Shi H, Li W, Shapiro J H, Zhuang Q and Zhang Z 2021 Entanglement-Assisted Communication Surpassing the Ultimate Classical Capacity *Physical review letters* **126** 250501

[152] Nafria V and Djordjevic I B 2023 Entanglement assisted communication over the free-space optical link with azimuthal phase correction for atmospheric turbulence by adaptive optics *Optics express* **31** 39906–16

[153] Nafria V and Djordjevic I B 2024 Entanglement assisted free-space optical communication with two-pump-based entanglement generation outperforming classical laser communication in strong turbulence regime at 10 Gb/s *Optics express* **32** 47908–19

[154] Ren S, Yan Y, Li Y, Li C, Han D, Zhu X, Wang M and Su X 2026 Deterministic entanglement-assisted quantum communication over 20 km fiber channel *Light, science & applications* **15** 83

[155] Li Y *et al* 2025 Realizing ultrahigh capacity quantum superdense coding on quantum photonic chip *npj Quantum Inf* **11.** 49

[156] Prasad T and Grassl M 2025 Codes for entanglement-assisted classical communication *npj Quantum Inf* **11.** 13

[157] 24 Market Reports 2023 *Quantum Key Distribution (QKD) Market, Global Outlook and Forecast 2023-2030* (24 Market Reports) https://www.24marketreports.com/ict-and-media/global-quantum-key-distribution-forecast-2023-2030-957

[158] 360 ResearchReports 2022 *GLOBAL QUANTUM KEY DISTRIBUTION (QKD) MARKET RESEARCH REPORT 2022* (360 ResearchReports) https://www.360researchreports.com/global-quantum-key-distribution-qkd-market-21606092

[159] 360 ResearchReports 2023 *GLOBAL QUANTUM COMMUNICATION MARKET GROWTH (STATUS AND OUTLOOK) 2023-2029* (360 ResearchReports) https://www.360researchreports.com/global-quantum-communication-market-23051430

[160] 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) https://www.adroitmarketresearch.com/industry-reports/quantum-cryptography-market

[161] 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) https://www.adroitmarketresearch.com/industry-reports/quantum-key-distribution-qkd-market?utm_source=AS5Ad12m

[162] 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) https://www.alliedmarketresearch.com/quantum-cryptography-market-A08464

[163] ASD Reports 2023 *Quantum Cryptography Market - Global Forecast to 2028* (ASD Reports) https://www.asdreports.com/market-research-report-620758/quantum-cryptography-market-global-forecast

[164] 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) https://www.astuteanalytica.com/industry-report/quantum-secure-communication-market

[165] 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) https://www.astuteanalytica.com/industry-report/quantum-cryptography-and-network-market

[166] bcc Research 2019 *Global Market for Quantum Cryptography* (bcc Research) https://www.bccresearch.com/market-research/information-technology/global-market-of-quantum-cryptography-market-report.html

[167] Business Growth Reports 2022 *Global Quantum Communication Market Size, Status and Forecast 2022-2028* (Business Growth Reports) https://www.businessgrowthreports.com/global-quantum-communication-market-22176549

[168] Data Bridge 2021 *Global Quantum Cryptography Market – Industry Trends and Forecast to 2028* (Data Bridge) https://www.databridgemarketresearch.com/reports/global-quantum-cryptography-market

[169] Data Intelo 2022 *Quantum Secure Communication Market Research Report* (Data Intelo) https://dataintelo.com/report/global-quantum-secure-communication-market/

[170] FactMR 2021 *Quantum Cryptography Market* (FactMR) https://www.factmr.com/report/quantum-cryptography-market

[171] 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) https://www.fiormarkets.com/report/global-quantum-cryptography-market-by-component-solutions-services-376071.html

[172] Fusion Market Research 2021 *Quantum Key Distribution (QKD) Market - Global Outlook and Forecast 2021-2027* (Fusion Market Research) https://icrowdnewswire.com/quantum-key-distribution-qkd-market-size-share-value-and-competitive-landscape-2021-2027

[173] 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) https://www.globmarketreports.com/industry-reports/260457/Quantum-Key-Distribution-(QKD)-market

[174] Global Information 2023 *Global Quantum Communication Market Size, Status and Forecast 2023-2029* (Global Information) https://www.giiresearch.com/report/qyr1214605-global-quantum-communication-market-size-status.html

[175] 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) https://www.globalmarketestimates.com/market-report/global-quantum-cryptography-market

[176] GlobalInfoResearch 2023 *Global Quantum Key Distribution (QKD) Market 2023 by Company, Regions, Type and Application, Forecast to 2029* (GlobalInfoResearch) https://www.globalinforesearch.com/reports/988398/quantum-key-distribution-(qkd)

[177] HTF Market Intelligence 2022 *Quantum Communication Device Market, Global Outlook and Forecast 2022-2028* (HTF Market Intelligence) https://www.htfmarketreport.com/reports/4077519-quantum-communication-device-market

[178] IMR Reports 2023 *Global Quantum Key Distribution (QKD) Market by Solution, Services, Application, and Region - Global Forecast to 2028* (IMR Reports) https://www.imrmarketreports.com/reports/quantum-key-distribution-qkd-market/

[179] Industry ARC 2023 *Quantum Cryptography Market - Forecast(2023 - 2028)* (Industry ARC) https://www.industryarc.com/Report/15803/quantum-cryptography-market.html

[180] 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) https://industrygrowthinsights.com/report/quantum-key-distributionmarket/

[181] Industry Research 2022 *GLOBAL QUANTUM CRYPTOGRAPHY MARKET SIZE, STATUS AND FORECAST 2022* (Industry Research) https://www.industryresearch.biz/global-quantum-cryptography-market-19859179

[182] Industry Research 2022 *GLOBAL QUANTUM KEY DISTRIBUTION (QKD) MARKET RESEARCH REPORT 2022(STATUS AND OUTLOOK)* (Industry Research) https://www.industryresearch.co/global-quantum-key-distribution-qkd-market-21109807

[183] Ken Research 2021 *Global Quantum Cryptography Market Outlook: Ken Research* (Ken Research) https://www.kenresearch.com/blog/2021/11/global-quantum-cryptography-market-outlook-ken-research/

[184] 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) https://www.knowledge-sourcing.com/report/quantum-cryptography-market

[185] Market Growth Reports 2021 *Global Quantum Communication Market Size, Status and Forecast 2021-2027* (Market Growth Reports) https://www.marketgrowthreports.com/global-quantum-communication-market-17703837

[186] Market Growth Reports 2022 *Global Quantum Key Distribution (QKD) Market 2022 by Company, Regions, Type and Application, Forecast to 2028* (Market Growth Reports) https://www.marketgrowthreports.com/global-quantum-key-distribution-qkd-market-21023035

[187] Market Growth Reports 2022 *Global Quantum Key Distribution (QKD) Market Research Report 2022* (Market Growth Reports) https://www.theexpresswire.com/pressrelease/Quantum-Key-Distribution-QKD-Market-in-Size-2023-Technological-Advancements-in-Report-with-New-Forecast-2028-SWOT-Value-Chain-Analysis-till-2028-81-Report-Pages_18416199

[188] Market Growth Reports 2023 *Global Quantum Key Distribution (QKD) Industry Research Report 2023, Competitive Landscape, Market Size, Regional Status and Prospect* (Market Growth Reports) https://www.theexpresswire.com/pressrelease/Quantum-Key-Distribution-QKD-Market-2023-Growth-Trend-Share-and-Forecast-till-2030-99-Pages-Report_20398230

[189] Market Growth Reports 2023 *Global Quantum Key Distribution (QKD) Market Research Report 2023* (Market Growth Reports) https://www.marketwatch.com/press-release/2030-quantum-key-distribution-qkd-market-size-industry-report-2023-2023-05-18#:~:text=The%20global%20Quantum%20Key%20Distribution%20(QKD)%20market%20was%20valued%20at,considered%20while%20estimating%20market%20sizes.

[190] 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) https://www.marketreportsworld.com/global-quantum-communication-market-18678407

[191] Market Reports world 2021 *Global Quantum Communication Market Size, Status and Forecast 2021-2027* (Market Reports world) https://www.marketreportsworld.com/global-quantum-communication-market-17703837

[192] Market Reports world 2023 *GLOBAL QUANTUM KEY DISTRIBUTION (QKD) AND QUANTUM CRYPTOGRAPHY (QC) MARKET GROWTH (STATUS AND OUTLOOK) 2023-2029* (Market Reports world) https://www.marketreportsworld.com/global-quantum-key-distribution-qkd-and-quantum-cryptography-qc-market-22695952

[193] Market Reports world 2023 *GLOBAL QUANTUM KEY DISTRIBUTION (QKD) MARKET RESEARCH REPORT 2023* (Market Reports world) https://www.marketreportsworld.com/global-quantum-key-distribution-qkd-market-22609686

[194] 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) https://www.marketresearchfuture.com/reports/quantum-cryptography-market-4836

[195] Market Research intellext 2023 *Global Quantum Cryptography Services Market Size By Product, By Application, By Geography, Competitive Landscape And Forecast* (Market Research intellext) https://www.marketresearchintellect.com/product/global-quantum-cryptography-services-market-size-forecast/

[196] 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) https://www.marketresearchupdate.com/industry-growth/quantum-key-distribution-qkd-market-size-409367

[197] Market Research world 2022 *GLOBAL QUANTUM KEY DISTRIBUTION QKD MARKET RESEARCH REPORT 2022(STATUS AND OUTLOOK)* (Market Research world) https://www.marketreportsworld.com/global-quantum-key-distribution-qkd-market-21179346

[198] Market Research.com 2022 *Global Quantum Key Distribution (QKD) Market Size, Status and Forecast 2022-2028* (Market Research.com) https://www.marketresearch.com/QYResearch-Group-v3531/Global-Quantum-Key-Distribution-QKD-31907466/

[199] Market Research.com 2023 *Global Quantum Key Distribution QKD Market Research Report 2023(Status and Outlook)* (Market Research.com) https://www.marketresearch.com/Bosson-Research-v4252/Global-Quantum-Key-Distribution-QKD-32788747/

[200] 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) https://www.marketresearch.com/MarketsandMarkets-v3719/Quantum-Cryptography-Offering-Solutions-Services-34072311/

[201] Market Stats Ville 2022 *Quantum Secure Communication Market 2022* (Market Stats Ville) https://www.marketstatsville.com/global-quantum-secure-communication-market

[202] 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) https://www.taiwannews.com.tw/en/news/4888997

[203] 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) https://www.marketsandmarkets.com/Market-Reports/quantum-cryptography-market-45857130.html

[204] MMR 2022 *Quantum Cryptography Market – Global Industry Analysis And Forecast (2022-2029)* (MMR) https://www.maximizemarketresearch.com/market-report/global-quantum-cryptography-market-key-trends/6554/

[205] Mobility Foresights 2023 *Global Quantum Key Distribution Market 2022-2030* (Mobility Foresights) https://mobilityforesights.com/product/quantum-key-distribution-market/

[206] Mordor Intelligence 2023 *QUANTUM CRYPTOGRAPHY MARKET SIZE & SHARE ANALYSIS - GROWTH TRENDS & FORECASTS (2023 - 2028)* (Mordor Intelligence) https://www.mordorintelligence.com/industry-reports/quantum-cryptography-market

[207] Persistence Market Research 2023 *Quantum Cryptography Market* (Persistence Market Research) https://www.persistencemarketresearch.com/market-research/quantum-cryptography-market.asp

[208] 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) https://www.precisionreports.co/2022-2029-global-quantum-cryptography-professional-market-20665332

[209] 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) https://www.prof-research.com/Quantum-Key-Distribution-(QKD)-Market

[210] 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) https://www.openpr.com/news/3047518/quantum-cryptography-market-size-share-industry-forecast

[211] Reports & Markets 2021 *Global Quantum Key Distribution (QKD) Industry Market Research Report* (Reports & Markets) https://www.reportsandmarkets.com/reports/global-quantum-key-distribution-qkd-market-4269690.amp

[212] Research and Markets 2022 *Quantum Cryptography Market - Forecasts from 2021 to 2026* (Research and Markets) https://www.businesswire.com/news/home/20220301005639/en/Global-Quantum-Cryptography-Market-2021-to-2026---Growing-Applications-Across-Industry-Verticals-Enterprises-and-Government-Sectors---ResearchAndMarkets.com

[213] 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) https://www.researchnester.com/reports/quantum-cryptography-market/1901

[214] Research Reportsworld 2022 *GLOBAL QUANTUM COMMUNICATION MARKET SIZE, STATUS AND FORECAST 2022-2028* (Research Reportsworld) https://www.researchreports-world.com/global-quantum-communication-market-20511649

[215] Research Reportsworld 2022 *GLOBAL QUANTUM KEY DISTRIBUTION (QKD) MARKET GROWTH (STATUS AND OUTLOOK) 2022-2028* (Research Reportsworld) https://www.researchreportsworld.com/global-quantum-key-distribution-qkd-market-21662339

[216] 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) https://www.supplydemandmarketresearch.com/global-quantum-key-distribution-qkd-market-1660196

[217] technavio 2021 *Quantum Cryptography Solutions Market by End-user and Geographic Landscape - Forecast and Analysis 2021-2025* (technavio) https://www.technavio.com/report/quantum-cryptography-solutions-market-industry-analysis

[218] 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) https://www.techsciresearch.com/report/global-quantum-cryptography-market/1512.html

[219] Tramsparency Market Research 2019 *Quantum Key Distribution Market* (Tramsparency Market Research) https://www.transparencymarketresearch.com/quantum-key-distribution-market.html

[220] 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) https://www.verifiedmarket-research.com/download-sample/?rid=6854

[221] 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) https://www.verifiedmarketreports.com/product/global-quantum-key-distribution-qkd-market-2019-by-company-regions-type-and-application-forecast-to-2024/

[222] Visiongain 2021 *Quantum Cryptography Market Report 2021-2031* (Visiongain) https://www.reportlinker.com/p06195544/Quantum-Cryptography-Market-Report-2031.html

[223] we market research 2022 *Global Quantum Secure Communication Market* (we market research) https://www.newstrail.com/quantum-secure-communication-market-size-2022/

[224] Congnitive Markt Research 2023 *Quantum Communication Market Report 2024 (Global Edition)* (Congnitive Markt Research) https://www.cognitivemarketresearch.com/quantum-communication-market-report

[225] Credence Research 2023 *Quantum Cryptography Market By Component Type (Quantum Key Distribution (QKD) Systems, Quantum Cryptographic Communication Devices, Quantum Cryptographic Software, Quantum Cryptographic Services); By Application (Secure Communocation, Data Encryption, Network Security, Financial Services, Government and Defense); By End User(Government and Defense, Financial Institutions, Healthcare, Telecommunications, Enterprises); By Deployment Mode(Cloud-based, On-Premisses, Hybrid); By User Cases; By Regulatory Compliance and Standards; By Region- Growth, Future Prospects& Competitive Analysis, 2022-2030* (Credence Research) https://www.credenceresearch.com/report/quantum-cryptography-market

[226] Exactitude Consultancy 2023 *Quantum Cryptography Market by Component (Solution, Service), Organization Size (Small and Medium Enterprise, Large Enterprise), Application (Network Security, Application Security, Network Security), Industry (IT and Telecommunications, BFSI, Healthcare and Life Sciences, Healthcare). , Automotive, Retail, Government & Defense, Other) and Region, Global Trends and Projections from 2023 to 2030* (Exactitude Consultancy) https://exactitudeconsultancy.com/de/reports/33431/quantum-cryptography-market/

[227] Future Market Insights 2023 *Quantum Cryptography Market Outlook from (2023 to 2033)* (Future Market Insights) https://www.futuremarketinsights.com/reports/quantum-cryptography-market

[228] KBV Research 2023 *Global Quantum Cryptography Market Size, Share & Industry Trends Analysis Report By Vertical, By Security Type (Network Security and Application Security), By Offering, By Regional Outlook and Forecast, 2023 - 2030* (KBV Research) https://www.kbvresearch.com/quantum-cryptography-market/

[229] QYResearch 2023 *Quantum Communication - Global Market Insights and Sales Trends 2024* (QYResearch) https://www.qyresearch.com/reports/1767888/quantum-communication

[230] Value Market Research 2023 *Global Quantum Cryptography Market Report By Offering (Solutions, Services), By Security Type (Network Security, Application Security), By Vertical (Government, Defense, BFSI, Healthcare, Retail, eCommerce) And By Regions - Industry Trends, Size, Share, Growth, Estimation and Forecast, 2023-2032* (Value Market Research) https://www.valuemarketresearch.com/report/quantum-cryptography-market

[231] Verifed Market reports 2023 *Global Quantum Communication Market By Type (Hardware, Software), By Application (Government, Military and Defense), By Geographic Scope And Forecas* (Verifed Market reports) https://www.verifiedmarketreports.com/product/quantum-communication-market/

[232] Allied Market Research 2024 *Quantum Cryptography Market Size, Share, Competitive Landscape and Trend Analysis Report by Component, by Security Type, by Industry Vertical and by Organizational Size : Global Opportunity Analysis and Industry Forecast, 2023-2032* (Allied Market Research) https://www.alliedmarketresearch.com/quantum-cryptography-market-A08464

[233] ASD Reports 2024 *Quantum Communication Market Report 2024-2034* (ASD Reports) https://www.asdreports.com/market-research-report-666653/quantum-communication-market-report

[234] Business Research Insights 2024 *Quantum Communication Market Size, Share, Growth, and Industry Analysis, (Hardware, Software and Services), By Application (Government, Military And Defense, Telecommunication, BFSI, Enterprise And Industrial), Regional Insights, and Forecast To 2032* (Business Research Insights) https://www.businessresearchinsights.com/market-reports/quantum-communication-market-113933

[235] Business Research Insights 2024 *Quantum Key Distribution (QKD) Market Size, Share, Growth, And Industry Analysis, By Type (Type I, Type II), By Application (Financial, Government, Military & Defense, Others), Regional Insights, and Forecast From 2024 To 2031* (Business Research Insights) https://www.businessresearchinsights.com/market-reports/quantum-key-distribution-qkd-market-106645

[236] Congnitive Markt Research 2024 *Quantum Cryptography Market Report 2024 (Global Edition)* (Congnitive Markt Research) https://www.cognitivemarketresearch.com/quantum-cryptography-market-report?gad_source=1

[237] Congnitive Markt Research 2024 *Quantum Key Distribution-QKD Market Report 2024 (Global Edition)* (Congnitive Markt Research) https://www.cognitivemarketresearch.com/quantum-key-distribution-qkd-market-report

[238] Credence Research 2024 *Quantum Key Distribution Market By Type (Multiplexed Systems, Long Distance System); By Application (Telecom and Data Center, Financial Services Companies, Government & Defence, Healthcare, Others); By Region - Growth, Share, Opportunities & Competitive Analysis, 2024 - 2032* (Credence Research) https://www.credenceresearch.com/report/quantum-key-distribution-market

[239] Fortune Business Insights 2024 *Quantum Cryptography Market Size, Share & Industry Analysis, By Type (Quantum Key Distribution, Quantum Random Number Generation , and Others), bY Security Type(Appilications Security, and Network Security), By Industry(BFSI, Cloud & Datacenter, Government, Energy / Ulilities, Healthcare, Automotive, and Others(Gaming, Retail &Consumer Goods, and Others)), and Regional Forrecast, 2024-2032* (Fortune Business Insights) https://www.fortunebusinessinsights.com/industry-reports/quantum-cryptography-market-100211

[240] GlobalInfoResearch 2024 *Global Quantum Key Distribution (QKD) Device Market 2024 by Company, Regions, Type and Application, Forecast to 2030* (GlobalInfoResearch) https://www.globalinforesearch.com/reports/2366734/quantum-key-distribution--qkd--device

[241] Grand View Research 2024 *Quantum Cryptography Market Size, Share & Trends Analysis Report By Type (Hardware, Software, Services), By End-use, By Application, By Region, And Segment Forecasts, 2024 - 2030* (Grand View Research) https://www.grandviewresearch.com/industry-analysis/quantum-cryptography-market-report

[242] IDTechEx Research 2024 *Quantum Communication Markt 2024-2034: Technology, Trends, Players, Foecasts* (IDTechEx Research) https://www.idtechex.com/en/research-report/quantum-communication-market-2024-2034-technology-trends-players-forecasts/984

[243] Industry ARC 2024 *Quantum Cryptography Market - Forecast(2023 - 2028)* (Industry ARC) https://www.industryarc.com/Report/15803/quantum-cryptography-market.html

[244] Innovative Market Research 2024 *Global Quantum Key Distribution (QKD) Market Size Analysis [2024-2032] | 121 Pages Modern Report* (Innovative Market Research) https://www.linkedin.com/pulse/global-quantum-key-distribution-qkd-market-size-u6eye/

[245] Market Digitals 2024 *Quantum Communication Market projected to reach USD 2.48 Billion by 2030, growing at a CAGR of 20.2% during the forecast period of 2023-2030 - says MarketDigits in its latest study* (Market Digitals) https://www.globenewswire.com/en/news-release/2024/01/23/2814308/0/en/Quantum-Communication-Market-projected-to-reach-USD-2-48-Billion-by-2030-growing-at-a-CAGR-of-20-2-during-the-forecast-period-of-2023-2030-says-MarketDigits-in-its-latest-study.html

[246] Market Research Future 2024 *Quantum Cryptography Market Research Report Information By Service (Support and Maintenance, Deployment and Integration, and Consulting), by Application (Database Encryption, Application Security, and Network Security), By Component (Hardware and Software) And By Region (North America, Europe, Asia-Pacific, And Rest Of The World) –Market Forecast Till 2032* (Market Research Future) https://www.marketresearch-future.com/reports/quantum-cryptography-market-4836

[247] Market Research Future 2024 *Quantum Communication Market Research Report Information By Product Type (Hardware, Service), By Application (National Defense, Aerospace, Finance, Other), And By Region (North America, Europe, Asia-Pacific, And Rest Of The World) –Market Forecast Till 2032* (Market Research Future) https://www.marketresearchfuture.com/reports/quantum-communication-market-12240

[248] Market Research Intellect 2024 *China Quantum Key Distribution Qkd Market Size Forecast* (Market Research Intellect) https://www.marketresearchintellect.com/product/china-quantum-key-distribution-qkd-market-size-forecast/

[249] Markets and Markets 2024 *Quantum Communication Market by Solution (Quantum Detectors,Quantum Key Distribution(QKD), Quantum Random Number Generator(QRNG), Quantum-safe Cryptography),QKD Transmission Type(Fiber-based and Free-space/ Satellite-based)-Global Forecast to 2030* (Markets and Markets) https://www.marketsandmarkets.com/Market-Reports/quantum-communication-market-143942501.html

[250] Markrt us 2024 *Global Quantum Cryptography Market By Component (Hardware, Software), By Application (Network Security, Database Encryption, Application Security), By End-User (Government and Defense, BFSI, Healthcare, IT and Telecommunication, Aerospace and Defense, Other End-users), By Region And Key Companies - Industry Segment Outlook, Market Assessment, Competition Scenario, Trends And Forecast 2024-2033* (Markrt us) https://market.us/report/quantum-cryptography-market/

[251] MMR 2024 *Quantum Cryptography Market – Global Industry Analysis And Forecast (2024-2030)* (MMR) https://www.maximizemarketresearch.com/market-report/global-quantum-cryptography-market-key-trends/6554/

[252] Mordor Intelligence 2024 *Quantum Cryptography Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029)* (Mordor Intelligence) https://www.mordorintelligence.com/industry-reports/quantum-cryptography-market

[253] OpenPR 2024 *Quantum Communication Global Market Report 2024 by The Business Research Company | Toshiba Corporation, ID Quantique SA, Nu Quantum Ltd., QuintessenceLabs Pty. Ltd., MagiQ Technologies Inc., SpeQtral Pte Ltd., Arqit Quantum Inc., QuantumCTek Co. Ltd* (OpenPR) Quantum Communication Global Market Report 2024 by The Business (openpr.com)

[254] Polaris Market Researhc 2024 *Quantum Cryptography Market Size Worth $ 11,336 Million By 2032 | CAGR: 41.10%* (Polaris Market Researhc) https://www.polarismarket-research.com/press-releases/quantum-cryptography-market

[255] PR newswire 2024 *Quantum Cryptography (QC) Market worth $7.59 billion by 2030 - Exclusive Report by MarketsandMarkets* (PR newswire) https://www.prnewswire.com/news-releases/quantum-cryptography-qc-market-worth-7-59-billion-by-2030---exclusive-report-by-marketsandmarkets-302271161.html

[256] Precision Business Insights 2024 *Quantum Communication Market Size, Share, Growth, Trends, and Global Industry Analysis: By Transmission Type (Fibre-Based, Free-Space/Satellite-Based), Deployment Mode (On-Premises, Cloud), Organization Size (Small and Medium-Sized*

Enterprises, Large Enterprises), End User (Banking, Financial Services, & Insurance, Healthcare, Aerospace, It & Telecommunication, Government & Defense, Others) and Region Forecast 2019-2030 (Precision Business Insights) https://www.precisionbusinessinsights.com/market-reports/quantum-communication-market

[257] Research and Market 2024 *Quantum Communication Market Report 2024-2034* (Research and Market) https://www.researchandmarkets.com/reports/5979701/quantum-communication-market-report

[258] Research and Market 2024 *Global Quantum Cryptography Market Report 2024* (Research and Market) https://www.researchandmarkets.com/reports/5983851/global-quantum-cryptography-market-report

[259] Research and Markets 2024 *Quantum Key Distribution (QKD) Market Opportunities 2024: The Quantum-Safe Path to the Quantum Internet* (Research and Markets) https://www.researchandmarkets.com/reports/5981952/quantum-key-distribution-qkd-market

[260] Research and Markets 2024 *Quantum Cryptography Market Report 2024-2034* (Research and Markets) https://www.researchandmarkets.com/reports/5960264/quantum-cryptography-market-report

[261] Research and Markets 2024 *Quantum Key Distribution (QKD) Market Opportunities Report 2024: Security Objections to QKD in the US may be Fading Away* (Research and Markets) https://www.globenewswire.com/news-release/2024/07/08/2909473/0/en/Quantum-Key-Distribution-QKD-Market-Opportunities-Report-2024-Security-Objections-to-QKD-in-the-US-may-be-Fading-Away.html

[262] Research Nester 2024 *Quantum Key Distribution (QKD) Market Size & Share,by Component (Solution, Services); Type (Multiplexed Systems, Long Distance System); End Use (Telecom & Data center, Financial Services Companies, Government, Defense, Healthcare, Transport, Retail)-Global Supply& Demand Analysis, Growth Forecasts, Statistics Report 2024-2036* (Research Nester) https://www.researchnester.com/reports/quantum-key-distribution-market/5812

[263] Research Nester 2024 *Quantum Communication Market Size & Share, by Product Type (Hardware, Service); Security Service (Application Security, Network Security); Application (National Defense, Aerospace, BFSI, Government, Telecommunication, Enterprise, Industrial) - Global Supply & Demand Analysis, Growth Forecasts, Statistics Report 2025-2037* (Research Nester) https://www.researchnester.com/reports/quantum-communication-market/5747

[264] straits research 2024 *Quantum Cryptography Market Size, Share & Trends Analysis Report By Components (Hardware, Software, Services), By Type (Quantum Key Distribution (QKD), Quantum Random Number Generation (QRNG), Others), By Service (Support and Maintenance, Deployment and Integration, Consulting), By Security Type (Database Encryption, Application Security, Network Security), By Industry (BFSI, Cloud and Datacentre, Government, Energy and Utilities, Healthcare, Automotive, Others) and By Region(North America, Europe, APAC, Middle East and Africa, LATAM) Forecasts, 2025-2033* (straits research) https://straitsresearch.com/report/quantum-cryptography-market

[265] Verifed Market reports 2024 *Global Quantum Communication Market By Type (Hardware, Software), By Application (Government, Military and Defense), By Geographic Scope And Forecast* (Verifed Market reports) https://www.verifiedmarketreports.com/product/quantum-communication-market/

[266] Verifed Market reports 2024 *Global Quantum Key Distribution (QKD) Market By Type (Rigid 1-2Sided, Standard Multilayer), By Application (Financial, Government), By Geographic Scope*

And Forecast (Verifed Market reports) https://www.verifiedmarketreports.com/product/global-quantum-key-distribution-qkd-market-2019-by-company-regions-type-and-application-forecast-to-2024/

[267] Visiongain 2024 *Quantum Cryptography Market Report 2024-2034* (Visiongain) https://www.visiongain.com/report/quantum-cryptography-market-2024/

[268] Visiongain 2024 *Quantum Communication Market Report 2024-2034* (Visiongain) https://www.visiongain.com/report/quantum-communication-market-2024/

[269] Business Research Insights 2025 *Quantum Communication Market Size, Share, Growth, and Industry Analysis, (Hardware, Software and Services), By Application (Government, Military And Defense, Telecommunication, BFSI, Enterprise And Industrial), Regional Insights and Forecast From 2025 To 2033 Source: https://www.businessresearchinsights.com/market-reports/quantum-communication-market-113933* (Business Research Insights) https://www.businessresearchinsights.com/market-reports/quantum-communication-market-113933

[270] Business Research Insights 2025 *Quantum Key Distribution (QKD) Market Size, Share, Growth, And Industry Analysis, By Type (Type I, Type II), By Application (Financial, Government, Military & Defense, Others), Regional Insights and Forecast From 2025 To 2033* (Business Research Insights) https://www.businessresearchinsights.com/market-reports/quantum-key-distribution-qkd-market-106645

[271] Business Research Insights 2025 *Quantum Communication Market Size, Share, Growth, and Industry Analysis, (Hardware, Software and Services), By Application (Government, Military And Defense, Telecommunication, BFSI, Enterprise And Industrial), Regional Insights and Forecast From 2025 To 2033* (Business Research Insights) https://www.businessresearchinsights.com/market-reports/quantum-communication-market-113933

[272] Business Research Insights 2025 *Quantum Key Distribution (QKD) Market Size, Share, Growth, And Industry Analysis, By Type (Type I, Type II), By Application (Financial, Government, Military & Defense, Others), Regional Insights and Forecast From 2025 To 2033* (Business Research Insights) https://www.businessresearchinsights.com/market-reports/quantum-key-distribution-qkd-market-106645

[273] Cognitive Market Research 2025 *Quantum Key Distribution-QKD Market Report 2025 (Global Edition)* (Cognitive Market Research) https://www.cognitivemarketresearch.com/quantum-key-distribution-qkd-market-report#:~:text=Cognitive%20Market%20Research%20has%20recently%20published%20the%207th,majorly%20two%20types%20of%20information%20qualitative%20and%20quantitative.

[274] Coherent Market Insights 2025 *Quantum Key Distribution Market Analysis & Forecast: 2025–2032* (Coherent Market Insights) https://www.coherentmarketinsights.com/market-insight/quantum-key-distribution-market-5971

[275] Coherent Market Insights 2025 *Quantum Cryptography Market Report 2025 (Global Edition)* (Coherent Market Insights) https://www.cognitivemarketresearch.com/quantum-cryptography-market-report

[276] Fortune Business Insights 2025 *Quantum Cryptography Market Size, Share & Industry Analysis, By Type (Quantum Key Distribution, Quantum Random Number Generation, and Others), By Security Type (Application Security, Network Security, Database Security, and Cloud Security), By Industry (BFSI, Government, Energy & Utilities, Healthcare, Automotive, and Others), and Regional Forecast, 2024 – 2032* (Fortune Business Insights) https://www.fortunebusinessinsights.com/industry-reports/quantum-cryptography-market-100211

[277] Future Market Insights 2025 *Quantum Cryptography Market Insights - Growth & Forecast 2025 to 2035* (Future Market Insights) https://www.futuremarketinsights.com/reports/quantum-cryptography-market

[278] GII research 2025 *Quantum Cryptography Market: Global Industry Analysis, Size, Share, Growth, Trends, and Forecast, 2025 - 2032* (GII research) https://www.giiresearch.com/report/pmrs1701677-quantum-cryptography-market-global-industry.html

[279] Global Growth Insights 2025 *Quantum Cryptography Market Size, Share, Growth, and Industry Analysis, By Types (Solutions, Services, Hardware), Applications (Financial, Government, Military & Defense, Others) and Regional Insights and Forecast to 2033* (Global Growth Insights) https://www.globalgrowthinsights.com/market-reports/quantum-cryptography-market-108162

[280] Market Research Future 2025 *Quantum Communication Market Research Report Information By Product Type (Hardware, Service), By Application (National Defense, Aerospace, Finance, Other), And By Region (North America, Europe, Asia-Pacific, And Rest Of The World) – Market Forecast Till 2034. Source: https://www.marketresearchfuture.com/reports/quantum-communication-market-12240* (Market Research Future) https://www.marketresearchfuture.com/reports/quantum-communication-market-12240

[281] Markets and Markets 2025 *Quantum Key Distribution Market by Offering (Solution and Services), Type (Multiplexed QKD Systems and Long-Distance QKD Systems), Application (Network Security, Data Encryption, Secure Communication) – Global Forecast to 2030* (Markets and Markets) https://www.marketsandmarkets.com/Market-Reports/quantum-key-distribution-qkd-market-80654677.html

[282] Markrt us 2025 *Global Quantum Communication Market Size, Share, Statistics Analysis Report By Offering (Solutions (Quantum Communication Components (Photon Sources, Quantum Memory, Quantum Detectors, Quantum Modulators and Transceivers, Quantum Repeaters), Quantum Key Distribution (QKD) Solutions, Quantum Random Number Generator (QRNG), Quantum-Safe Cryptographic Solutions), Services), By Transmission Medium (Fiber-Based QKD, Free-Space/Satellite-Based QKD), By Enterprise Size (Large Enterprises, Small & Medium Enterprises (SMEs)), By Vertical (BFSI, Government & Defense, Healthcare, Aerospace, IT & Telecom, Energy & Utilities, Others), Region and Companies - Industry Segment Outlook, Market Assessment, Competition Scenario, Trends and Forecast 2025-2034* (Markrt us) https://market.us/report/quantum-communication-market/

[283] Mckinsey Digital 2025 *Quantum communication growth drivers: Cybersecurity and quantum computing* (Mckinsey Digital) https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-communication-growth-drivers-cybersecurity-and-quantum-computing#/

[284] Predence Research 2025 *Quantum Communication Market Size, Share, and Trends 2025 to 2034* (Predence Research) https://www.precedenceresearch.com/quantum-communication-market

[285] QY research 2025 *Global Quantum Cryptography Market Research Report 2025* (QY research) https://www.qyresearch.com/reports/3472734/quantum-cryptography

[286] Research and Market 2025 *Quantum Communication Market Report 2025* (Research and Market) https://www.researchandmarkets.com/reports/5983855/quantum-communication-market-report

[287] Research and Markets 2025 *Quantum Cryptography Market Report 2025* (Research and Markets) https://www.researchandmarkets.com/reports/5983851/quantum-cryptography-market-report

[288] Research Nester 2025 *Quantum Key Distribution (QKD) Market Size, by Component (Solution, Services), Type (Multiplexed Systems, Long Distance System), End Use (Telecom & Data Center, Financial Services Companies, Government, Defense, Healthcare, Transport, Retail) – Growth Trends, Regional Share, Competitive Intelligence, Forecast Report 2025–2037* (Research Nester) https://www.researchnester.com/reports/quantum-key-distribution-market/5812

[289] straits research 2025 *Quantum Communication Market Size, Share & Trends Analysis Report By Component (Solutions, Services), By Enterprise Size (Large Enterprises, Small and Medium Enterprises (SMEs)), By Transmission Type (Fiber Based, Satellite based), By Industry Vertical (BFSI, Government & Defence, Healthcare, Aerospace, IT & Telecom, Others) and By Region(North America, Europe, APAC, Middle East and Africa, LATAM) Forecasts, 2025-2033* (straits research) https://straitsresearch.com/report/quantum-communication-market

[290] The Business Research Company 2025 *Quantum Cryptography Global Market Report 2025 – By Type (Quantum Key Distribution, Quantum Random Number Generation, Other Types), By Component (Solutions, Services), By Applications (Network Security, Application Security, Database Security), By End-Users (Information Technology and Telecommunications, Banking, Financial Services, and Insurance, Government and Defense, Healthcare, Other End-Users) – Market Size, Trends, and Global Forecast 2025–2034* (The Business Research Company) https://www.thebusinessresearchcompany.com/report/quantum-cryptography-global-market-report

[291] Verifed Market reports 2025 *Global Quantum Communication Market Size By Technology Type (Quantum Key Distribution (QKD), Quantum Repeaters), By Application Sector (Government and Defense, Banking and Finance), By End-User Type (Large Enterprises, Small and Medium-Sized Enterprises (SMEs)), By Delivery Mode (On-Premises Solutions, Cloud-Based Solutions), By Component Type (Hardware Components, Software Components), By Geographic Scope And Forecast* (Verifed Market reports) https://www.verifiedmarketreports.com/product/quantum-communication-market/#:~:text=According%20to%20a%20report%20by%20the%20National%20Institute,rate%20%28CAGR%29%20of%2029.6%25%20from%202021%20to%202026.

[292] Bundesministerium für Forschung, Technologie und Raumfahrt *Research and Innovation - BMFTR's Data Portal* https://www.datenportal.bmftr.bund.de/portal/en/research.html (accessed 7 Jan 2026)

[293] Eurostat *Statistics Explained - R&D expenditure* https://ec.europa.eu/eurostat/statistics-explained/index.php?title=R%26D_expenditure (accessed 7 Jan 2026)

[294] Bundesregierung 2025 *Antwort der Bundesregierung der Fraktion der CDU/CSU: Aktueller Umsetzungsstand des Handlungskonzeptes Quantentechnologien der Bundesregierung (BT-Drs. 20/14986)* https://dserver.bundestag.de/btd/20/149/2014986.pdf

[295] muquanet 2026 *Quantenkommunikationsinfrastruktur* https://www.unibw.de/muquanet/projekte/quantenkommunikationsinfrastruktur (accessed 20 Mar 2026)

[296] muquanet 2026 *Hochintegrierte QKD-Komponenten* https://www.unibw.de/muquanet/projekte/hochintegrierte-qkd-komponenten (accessed 20 Mar 2026)

[297] muquanet 2026 *Quantensichere Verschlüsselung (OSI-Layer 2)* https://www.unibw.de/muquanet/news/quantensichere-verschluesselung-auf-layer-2 (accessed 20 Mar 2026)

[298] QU-PILOT 2026 *Homepage - QU-PILOT* https://qu-pilot.eu/ (accessed 20 Mar 2026)

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

[300] Bundesministerium für Bildung und Forschung (BMBF, now called BMFTR) 2023 *Handlungskonzept Quantentechnologien der Bundesregierung* https://www.bmftr.bund.de/SharedDocs/Downloads/DE/230426-handlungskonzept-quantentechnologien.pdf?__blob=publicationFile&v=4

[301] Bundesministerium für Forschung, Technologie und Raumfahrt - BMFTR 2026 *Homepage - 18 Milliarden Euro für die Hightech Agenda Deutschland* https://www.bmftr.bund.de/SharedDocs/Kurzmeldungen/DE/2025/09/260925-haushalt-26-1-lesung.html (accessed 16 Jan 2026)

[302] Bundesministerium für Bildung und Forschung (BMBF, now called BMFTR) 2022 *Forschungsprogramm Quantensysteme* https://www.bmftr.bund.de/SharedDocs/Publikationen/DE/5/31714_Forschungsprogramm_Quantensysteme.pdf?__blob=publicationFile&v=5

[303] Fraunhofer Institute for Applied Optics and Precision Engineering IOF 2022 *First successful exchange of quantum keys between Erfurt and Jena via optical fiber: Fiber link over 75 kilometers enables new QKD experiments* https://www.iof.fraunhofer.de/en/pressrelease/2022/quantum-keys-exchange-successful.html (accessed 15 May 2024)

[304] Bundesministerium für Forschung, Technologie und Raumfahrt - BMFTR 2026 *Technologie-Roadmap Quantentechnologie: Version 1.0 – Stand Mai 2026* https://hightech-agenda-deutschland.de/roadmaps/quantentechnologien/ (accessed 22 May 2026)

[305] 2026 *QUBE II — Kommunikationstechnologien und Cybersicherheit* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qube-2 (accessed 16 Jan 2026)

[306] Fraunhofer Institute for Applied Optics and Precision Engineering IOF 2026 *QuNET initiative: One step closer to highly secure quantum communication* https://www.iof.fraunhofer.de/en/pressrelease/2023/QuNET-Keyexperiment-2023.html (accessed 10 Jun 2026)

[307] QuNET 2025 *Start - QuNET* https://qunet-initiative.de/ (accessed 16 Jan 2026)

[308] Fraunhofer Institute for Applied Optics and Precision Engineering IOF 2025 *Foundation for the future quantum network: quantum channels tested in flight* https://www.iof.fraunhofer.de/en/pressrelease/2025/QuNET-key-experiment-3-Quantum-channels-tested-in-flight.html (accessed 22 May 2026)

[309] 2026 *QUBE — Kommunikationstechnologien und Cybersicherheit* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qube (accessed 16 Jan 2026)

[310] 2026 *QUBE-II erfolgreich gestartet* https://www.telematik-zentrum.de/news/2026-05-04/ (accessed 10 Jun 2026)

[311] 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)

[312] The European Quantum Flagship 2024 *Strategic Research and Industry Agenda SRIA 2030: Roadmap and Quantum Ambitions over this Decade*

[313] European Commission 2025 *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Quantum Europe Strategy: Quantum Europe in a Changing World* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0363

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

[315] 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)

[316] Parker E *et al* 2022 *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology* https://www.rand.org/pubs/research_reports/RRA869-1.html

[317] Huber E X 2025 How China plans to turn quantum into a future industry *China ∩ Quantum*

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

[319] Aleksandr Khmelev *et al* 2024 Eurasian-scale experimental satellite-based quantum key distribution with detector efficiency mismatch analysis *Opt. Express* **32** 11964–78

[320] Li Y *et al* 2025 Microsatellite-based real-time quantum key distribution *Nature* **640** 47–54

[321] 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)

[322] The government of People's Republic of China 2025 *工业和信息化部办公厅关于组织开展2025年未来产业创新任务揭榜挂帅工作的通知_国务院部门文件_中国政府网* https://www.gov.cn/zhengce/zhengceku/202501/content_6999416.htm (accessed 16 Jan 2026)

[323] Xin L 2024 China's 'father of quantum' says global secure communications just 3 years away *South China Morning Post*

[324] Huber E X 2025 "Pan megagroup" - An update on recent achievements and the future of quantum networks *China ∩ Quantum*

[325] DARPA *QuANET: Quantum-Augmented Network | DARPA* https://www.darpa.mil/research/programs/quantum-augmented-network (accessed 16 Jan 2026)

[326] U.S. Senate Committee on Commerce, Science, & Transportation 2024 *Cantwell, Young, Durbin, Daines Introduce National Quantum Initiative Reauthorization Act* https://www.commerce.senate.gov/2024/12/cantwell-young-durbin-daines-introduce-national-quantum-initiative-reauthorization-act (accessed 16 Jan 2026)

[327] DICK DURBIN U.S. Senator for Illinois 2024 *Durbin Advocates For His Bipartisan Quantum Computing Legislation In Energy & Natural Resources Committee Hearing* https://www.durbin.senate.gov/newsroom/press-releases/durbin-advocates-for-his-bipartisan-quantum-computing-legislation-in-energy-and-natural-resources-committee-hearing (accessed 16 Jan 2026)

[328] U.S. Congress 2025 *S.1344 - 119th Congress (2025-2026): Quantum Sandbox for Near-Term Applications Act of 2025* https://www.congress.gov/bill/119th-congress/senate-bill/1344/text (accessed 16 Jan 2026)

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

[330] 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)*

[331] University of Cambridge 2025 *Researchers demonstrate the UK's first long-distance ultra-secure communication over a quantum network* https://www.cam.ac.uk/research/news/researchers-demonstrate-the-uks-first-long-distance-ultra-secure-communication-over-a-quantum (accessed 16 Jan 2026)

[332] Department for Science, Innovation & Technology 2023 *National Quantum Strategy Missions* https://www.gov.uk/government/publications/national-quantum-strategy/national-quantum-strategy-missions (accessed 16 Jan 2026)

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

[334] Secretariat of Science, Technology and Innovation Policy, Cabinet Office 2023 *Strategy of Quantum Future Industry Development Summary* https://www8.cao.go.jp/cstp/english/strategy_r08.pdf

[335] Ministry of Science and ICT 2025 *과기정통부, 2025 년 양자과학기술 및 산업육성을 위해 1,980 억 원 투자*

[336] 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)

[337] ID Quantique 2025 *Clavis XG Series QKD obtains National Security Certification* https://www.idquantique.com/clavis-xg-series-qkd-obtains-national-security-certification/ (accessed 16 Jan 2026)

[338] 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)

[339] Government of Canada 2025 *National Quantum Strategy Roadmap QUANTUM COMMUNICATION AND POST-QUANTUM CRYPTOGRAPHY* https://ised-isde.canada.ca/site/national-quantum-strategy/en/national-quantum-strategy-roadmap-quantum-communication-and-post-quantum-cryptography

[340] 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)

[341] 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

[342] 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)

[343] IITM CDOT SAMGNYA TECHNOLOGIES 2026 *IITM CDOT SAMGNYA TECHNOLOGIES* https://www.samgnya.in/ (accessed 16 Jan 2026)

[344] Indian Ministry of Defense 2024 *CONTRACT SIGNING OF ARMY iDEX PROJECT* https://www.pib.gov.in/PressReleasePage.aspx?PRID=2060379&reg=3&lang=2 (accessed 16 Jan 2026)

[345] Advanced Television 2022 *Eagle-1 could start new fleet for SES* https://www.advanced-television.com/2022/09/26/eagle-1-could-start-new-fleet-for-ses/ (accessed 16 Jan 2026)

[346] Lewis B 2025 *Scientists test quantum mechanics in outer space* https://www.aps.org/ap-snews/2025/04/quantum-mechanics-in-outer-space

[347] CQT - Centre for Quantum Technologies 2025 *New SpeQtre satellite to communicate with CQT ground station - CQT - Centre for Quantum Technologies* https://www.cqt.sg/high-light/new-speqtre-satellite-to-communicate-with-cqt-ground-station/ (accessed 10 Jun 2026)

[348] The Government of the UK 2018 UK and Singapore come together to launch £10m quantum space programme *GOV.UK*

[349] JAXA 2024 *令和６年度 宇宙戦略基金事業 公募要領* https://fund.jaxa.jp/content/uploads/ko-boyoryo_10.pdf

[350] Chinmaya Academy for Civil Services 2026 *Quantum Computing Using Satellites by 2030* https://currentaffairs.chinmayaias.com/quantum-computing-using-satellites-by-2030/ (accessed 16 Jan 2026)

[351] 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)

[352] Deutsche Telekom 2023 *Deutsche Telekom opens quantum research lab* https://www.tele-kom.com/en/media/media-information/archive/deutsche-telekom-opens-quantum-research-lab-1047874

[353] Blaum K, Kaufmann P, Kronjäger J, Kück S, Liebisch T C, Meschede D, Naegele-Jackson S, Schiller S and Schnatz H 2025 *The QTF-Backbone: Proposal for a Nationwide Optical Fibre Backbone in Germany for Quantum Technology and Time and Frequency Metrology*

[354] Schirmprojekt Quantenkommunikation Deutschland 2026 *Testbed-Karte zur Quantenkommunikation in Deutschland* https://www.squad-germany.de/testbeds/ (accessed 12 Jun 2026)

[355] Bundesministerium für Forschung, Technologie und Raumfahrt - BMFTR *Technologische Souveränität* https://www.bmftr.bund.de/DE/Forschung/Schluesseltechnologien/TechnologischeSouveraenitaet/technologischesouveraen (accessed 29 May 2026)

[356] 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

[357] Bundesministerium für Bildung und Forschung (BMBF, now called BMFTR) 2021 *Technologisch souverän die -Zukunft gestalten: BMBF-Impulspapier zur technologischen Souveränität* https://www.bmftr.bund.de/SharedDocs/Publikationen/DE/5/24032_Impulspapier_zur_technologischen_Souveraenitaet.pdf?__blob=publicationFile&v=5

[358] 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)

[359] Bundesamt für Sicherheit in der Informationstechnik *Kryptografie quantensicher gestalten: Grundlagen, Entwicklungen, Empfehlungen* (Bundesamt für Sicherheit in der Informationstechnik) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf?__blob=publicationFile&v=5

[360] French Cybersecurity Agency, Federal Office for Information Security, Netherlands National Communications Security Agency and Swedish National Communications Security Authority, Swedish Armed Forces 2024 *Position Paper on Quantum Key Distribution*

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4

[361] VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V 2025 *VDE Positionspapier Quantentechnologien* https://www.vde.com/resource/blob/2408772/62f57c8a3aea54570768f2e2b4132bce/quanten-download-data.pdf

[362] Schmaltz T, Endo C, Eßwein R, Groth J, Gruber S, Kroll H, Vogelsang M M, Neuhäusler P and Weymann L 2025 *Quantentechnologien und Quanten-Ökosysteme (*7-2025*)* (Expertenkommission Forschung und Innovation (EFI) - Commission of Experts for Research and Innovation, Berlin) https://ideas.repec.org/p/zbw/efisdi/312418.html

[363] Federal Office for Information Security 2022 *General information on KRITIS - What are Critical Infrastructures?* https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis.html (accessed 15 May 2024)

[364] 2026 *Erste Group setzt neue Maßstäbe in der Quantenverschlüsselung* https://www.erstegroup.com/de/news-media/presseaussendungen/2026/02/23/erste-group-setzt-neue-massstaebe-in-der-quantenverschluesselung (accessed 20 Mar 2026)

[365] seQUcom *Securing Enterprise Communications* https://sequcom.de/

[366] 2026 *Quantum Future Professionals* https://www.quantensysteme.info/foerdermassnahmen/details/q/quantum_future_professionals (accessed 20 Mar 2026)

[367] 2026 *QuNET+BlueCert — Kommunikationstechnologien und Cybersicherheit* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qunet-bluecert (accessed 20 Mar 2026)

[368] ETSI 2024 GS QKD 016 - V2.1.1 - Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules

[369] ETSI 2016 GS QKD 011 - V1.1.1 - Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems

[370] ETSI GR QKD 003 2018 *Quantum Key Distribution (QKD); Components and Internal Interfaces (*V2.1.1*)* (ETSI)

[371] CEN-CENELEC Focus Group on Quantum Technologies 2023 *Standardization Roadmap on Quantum Technologies: Release 1* https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf

[372] Schmaltz T *et al* 2025 *Application Perspectives in Quantum Communication* https://doi.org/10.24406/publica-4734