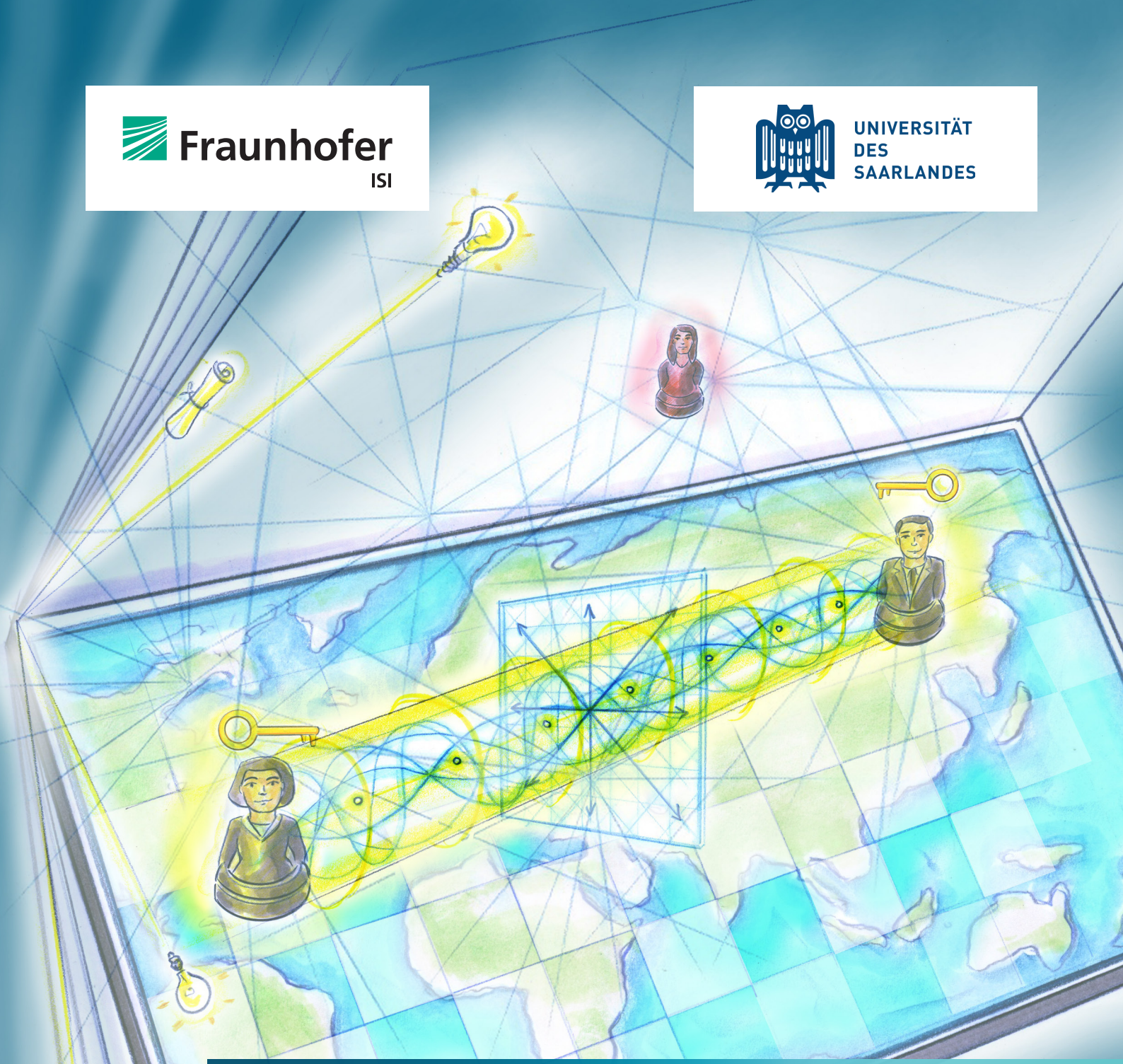
Fraunhofer ISI

UNIVERSITÄT DES SAARLANDES



July 2024

Monitoring Report 1 Quantum Communication

Publishing notes

Monitoring Report 1 – Quantum Communication

Project coordination

Fraunhofer-Institut für System- und Innovationsforschung ISI

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

Universität des Saarlandes

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

Responsible for content

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

Compiled on behalf of

Umbrella Project for Quantum Communication in Germany (Schirmprojekt Quantenkommunikation Deutschland – SQuaD), funded by the Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung – BMBF)

SPONSORED BY THE
Federal Ministry of Education and Research

Picture credits

Cover page: Heyko Stöber, Hohenstein

Published

July 2024

DOI

doi:10.24406/publica-3285

License

Notes

Contents

Executive Summary

Secure communication represents a cornerstone of free societies and is essential for the reliable operation of critical infrastructures. Cryptographic methods are crucial to ensure this. However, developments in quantum computing mean that the encryption protocols used today might be able to be decrypted in the foreseeable future, which is why "quantum-secure" ways of encrypting communication are urgently needed. The emerging technology of quantum key distribution (QKD), which enables physically secure communication based on quantum mechanical principles, and technologies able to transport or exchange quantum states over longer distances are grouped together using the term quantum communication. This report provides an overview of the technologies and technology generations of quantum communication, analyzes developments in the fields of research, industrialization, test infrastructure and the market, and discusses the relevance of technology sovereignty in quantum communication.

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 & 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 & measure QKD is already a market-ready technology for secure communication. However, its widespread use is being hampered by high costs, pending proofs of security, certification and approval.

Second generation - quantum key distribution with photonic entanglement sources:
Quantum entanglement, a special form of linking between quantum mechanical particles, 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 & 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, 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 repeaters 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.

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 almost 2000 in 2022. The majority of these were from China (33% share of publications), closely followed by the EU (29%, 7% from Germany) and the USA (16%). A citation analysis reveals that, on average, publications from the EU are cited 23 times, more frequently than publications from the other regions/countries analyzed. This suggests a high relevance of European publications.

Patenting activities in the field of quantum communication have also increased greatly in the past few years and there were more than 200 transnational patent applications in 2021. The majority of recent patent applications have come from the EU (35% share of patents), followed by the USA (29%) and China (15%). Technology enterprises, large telecommunications providers, and research institutions/organizations show the highest patent activity. Even though most patent applications are from industry (approx. 70%), the technology continues to be strongly driven by research organizations (approx. 30%).

Analyzing numerous market studies 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 represents a global turnover of EUR 1.7 billion in 2023, which could increase to EUR 5.8 billion 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 62 projects in the field of quantum communication funded by the BMBF, and 57 projects funded by the EU Framework Programme Horizon 2020 (H2020), as well as 21 projects funded under Horizon Europe (HE). The majority of these projects focus on QKD (especially BMBF and HE), light sources (BMBF, H2020 and HE), and quantum networks (especially H2020).

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 and have established R&D programs. Numerous countries have developed strategies and are making significant investments in quantum communication. China, USA, UK, Japan, and South Korea should be mentioned in particular.

To provide an *overview of existing test infrastructure*, this report includes a map of the so-called *testbeds* for quantum communication in Germany and gives a brief description of each. The construction of (test) infrastructure is hugely important for the industrialization and widespread application of quantum communication.

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 valid 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 potentials of quantum communication technologies was frequently emphasized, which goes 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 are seen in the high investment costs for infrastructure and quantum communication technologies as well as in the further development of systems and technologies. Wider market implementation also faces challenges, especially with regard to the lack of awareness about security risks in communication, potential users' perception of quantum communication, the development of markets and business models in the private sector, the strong regulation of some markets (especially in the public sector), and security proofs.

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, dismantling obstacles 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 (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. An update of this report is planned. A combination of methods (section 2) was applied to obtain a detailed picture.

The state of research in quantum communication is discussed within a qualitative analysis (section 3). Different software and hardware approaches to quantum communication are introduced, and the potential evolution of technology generations is highlighted.

The quantitative analysis (section 4) 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 5). Based on expert interviews, a discussion of the skills 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 6) and an outlook on potential further activities is provided.

2 Methods

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:

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

Citation analyses were carried out using the QCom-related publications from 2019. We chose this year as it allows sufficient time for citation but is still relatively recent.

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

Meta-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 68 relevant market reports with publishing dates from 2019 to July 2023. 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 BMBF 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. [1] 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. [2] The search methodology for the EU database included a first round of filtering using the keywords "communication" and "quantum" in the title or abstract of the 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) in FY 2019-2023 [3]
- UK: National Quantum Technology Programme (NQTP) in 2014-2023 [4]
- JP: Quantum Technology and Innovation Strategy published in 2020 [5]

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 "Quantum Technologien (2018)" and "Vernetzung und Sicherheit digitaler Systeme (2017)"

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. [6] Therefore, our analysis only provides a rough estimate of China's investment.[1]

We calculated the total funding for quantum technologies based on the respective main initiatives (the NQI report for the US, the NQTP for the UK and the Quantum Technology Innovation Strategy for Japan). In the case of the EU, although our project monitoring data include projects funded by thematically open initiatives (e.g., European Research Council), here, we only considered projects under the Quantum Flagship to compare the intensity of QCom in the quantum-specific strategy. In addition, two Specific Grant Agreement (SGA) projects (Qu-Test and Qu-Pilot) were excluded from QCom funding because they focus on quantum technologies in general and it was not possible to differentiate their contribution to QCom topics.[2] For the total investment in Germany, in addition to the two BMBF framework programs mentioned above, we included the COVID recovery plan for quantum technologies (EUR 2 billion).

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. EuroQCI was excluded for the EU due to missing time series data.

Data for the US were derived from the NQI Annual Budget Report 2023, which provides the actual budget for FY2019-2021, the estimated budget for FY2022, and the proposed budget for FY2023. In Japan, budget planning is usually based on a single year, and our data mostly reflect the actual

[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 Mckinsey&Co. 2023) [7] with the averaged ratio of QCom funding to QT funding in other analyzed countries.

[2] Following our analysis, we learnt that Qu-Test is also of strategic importance for QCom. This project will be taken into account accordingly in the update of this report.

annual allocation to projects and programs. When annual budget data were 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.

Technology Sovereignty

The discussion of aspects of technology sovereignty in quantum communication was based on five interviews with experts from science, industry, and politics. The interviewees were introduced to the concept of technological sovereignty as developed by Fraunhofer ISI. [8] 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. [9]

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 is particularly known for breaking down large natural numbers into their prime factors more efficiently than conventional computers, and demonstrates the much faster ability of quantum computers to tackle mathematical problems previously considered extremely difficult to solve and therefore used in classical 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)" [10], 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 in the early 2030s. 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)" [11], which was launched by the German Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung, BMBF) 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 encryption 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. Examples are algorithms based on elliptical curves or lattice-based protocols. [12] As this does not require any special hardware, it offers a short-term option for protecting key transmission against quantum attacks. In this context, the US National Institute of Standards and Technology (NIST) has been investigating the vulnerability of numerous proposed methods in a multi-stage process since 2017. Only one algorithm for public key cryptography and three algorithms for digital signatures made it to the fourth round in 2022: the CRYSTALS-Kyber key-purification method and the CRYSTALS-Dilithium, Falcon and SPHINCS+ signature methods. In addition, the three code-based key agreement methods Classic McEliece, BIKE and HQC as well as other signature methods are currently being tested with the aim of standardizing a selection of methods whose security is guaranteed by as many different mathematical problems as possible. [13] PQC methods will not be discussed further in the remainder of this report, such that the focus is on QKD as a cryptographic method.

Today, quantum cryptography is considered a key technology for the security of digital infrastructures in our society and can be described as the most technologically advanced of the quantum technology pillars mentioned above. 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, such that no new communication infrastructure is required. 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 & 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 & 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 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.

a) 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.
b) No-cloning theorem: According to the quantum mechanical no-cloning theorem by William Wootters and Wojciech Zurek (1982), 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. [13] 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. However, the BSI's most important argument is that 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. [14]

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. [14] 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 & 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. [15]

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 [16] and converted into a practicable protocol [17] 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. [18] 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 [19] and the more complicated theoretical security analysis. [15] 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:

c) 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.

d) 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 Industry

QKD demonstrations and testbeds

Although comparatively new, QKD that is based on the prepare & 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. [20] 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. [21] 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. [22] 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. [23] 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. [24] 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. [25] 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. [15] 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. [26]

The Beijing-Shanghai Backbone Network (BSBN), which began operations in August 2017, is currently the most far-reaching and advanced QKD network. It is the world's first quantum-secure long-range communication link, was 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. [27] 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. [28] 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 [29], the BNL is a government experimental facility that provides infrastructure and capabilities to help develop the quantum ecosystem. [30] 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. [31] In June 2022, Amazon also announced the "AWS Center for Quantum Networking" at industrial level, whose task is to develop new hardware, software and applications for quantum networks. [32] 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. [33] 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. [34, 35] In addition, Toshiba UK and BT 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. [36] 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 new space-based secure communications system. [37]

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). [13]

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. The maximum distance that has been achieved to date for a direct connection using optical fiber is 1000 km. Twin-field QKD was used here, in which the interference of two different phase-stable optical fields is used to exchange quantum information between the communication partners. [38] 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. [38–40] A CV-QKD system with 16 symbols achieved key rates of 49 Mbps over 25 km to 2 Mbps over 80 km of fiber optic cable. [41] An overview of current performance parameters (with a focus on CV-QK) is provided by Zhang et al. (2023). [42]

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. [34, 35] 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 BMBF-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. [43] 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 BMBF. 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. [44] There are also individual BMBF-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. [45, 46] 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 is 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. [47] Another project worth mentioning is "Anwendungsorientierte Demonstration von Quantenkommunikation in Deutschland, DemoQuanDT (Application-oriented demonstration of quantum communication in Germany)", which focuses 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 will be set up in a real-world fiber network between Bonn and Berlin, which will be used for research purposes and is set to become the longest quantum network in Germany. This will make use of existing fiber optics and regular operating points. [48] In addition, the BMBF-funded "6G-Quantum Security (6G-QuaS)" project targets the development of a hybrid wired industrial network. Here, the quantum information is to be stored continuously in the phase and amplitude of the light. This should result in significantly lower latency times and greater resilience to attacks while maintaining the same level of security. [49] The BMBF-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)" aims to further develop existing CV-QKD approaches based on coherent optical transmission technology. In this context, the objectives are 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. [50] Also worth mentioning is the joint project "Quantum Internet of Things (QUIET)", which focuses on the development of a communication network and the connection of quantum sensors using distributed quantum states and conventional transmission. This should significantly increase the performance and security of the network. [51]

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 & 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, [52] and Charles H. Bennett, Gilles Brassard and N. David Mermin 1992, BBM92, [53]) 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. The difference to the BB84 protocol is that not only two non-orthogonal 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 nonlinear 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. [54]

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, [55] but have so far only been implemented in a few demonstration experiments. [56]

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, multiparty 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. [57, 58] This can be implemented technically using a spectrally broadband source of photon pairs, which are divided into different frequency channels using wavelength demultiplexing. [59] In such multiparty 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 Industry

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. [60] While SPDC-based probabilistic entangle-

ment sources have been used in many demonstration experiments to date, the use of semiconductor quantum dot entanglement sources is still limited to initial experiments over short distances. [61, 62]

In context of the second QKD generation, the "Quantum Communications Hub" in the UK (in its second funding period since 2019) aims to develop secure quantum communication over all distance scales and to integrate QKD into existing networks for secure communication. The hub's fiber link extends from Bristol via London to Cambridge/Ipswich and has metro networks at the endpoints. Among other goals, the project is investigating 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. [63]

QKD performance parameters

Currently, entanglement-based QKD via optical fibers enables bridging a range of around 100 to 250 km. Examples are a range of approx. 50 km using a deployed fiber optic cable, a range of approx. 96 km using submarine fiber optic cables or underwater communication cables and a range of approx. 248 km using transnational point-to-point connections. [64–66]

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. So far, the highest key rate of second-generation entanglement-based QKD was 110 bit/s over a distance of 10 km of optical fiber. [67]

QKD research projects

Several national and international research projects have emerged that build on the advances described above. For example, the project "IT-Sicherheit durch verschränkungsbasierten Quantenschlüsselaustausch (Quantum-based Security Promise, Q-Sec-Pro)" aims 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 aim is to investigate and implement a QKD protocol and suitable hardware and software. This will not only make an important contribution to the development of a German quantum communication industry, but will also secure Germany's technological sovereignty. [68] Similar efforts are being made in the BMBF-funded "Q-Fiber" project that aims 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 is to implement and research novel light conducting cables for the transmission and low-cost detection of light quanta within existing IT infrastructure. [69]

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 non-local 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. [70] 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. [71] 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 [72] and rubidium atoms [73] 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.

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. [74] 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 BMBF's 2021 research program for "Kommunikationssysteme: Souverän. Digital. Vernetzt. (Communication Systems: Sovereign. Digital. Connected.)" [75] 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. [76–78] 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 Industry

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 BMBF-funded program “Digital. Sicher. Souverän. (Digital. Secure. Sovereign.)” and ensure technological sovereignty in tap-proof communication over long distances. Against this background, the ongoing "Quantum.Repeater.Link (QR.X)" project, e.g., has set the goal of exploring the distribution and storage of entanglement as a resource for quantum communication and quantum networks. To this end, optimized components and modularized devices are developed, fiber testbeds outside the lab environment are deployed and an elementary quantum repeater link is to be demonstrated under realistic field conditions. [79]

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 a necessary prerequisite 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 these demonstrations to short distances of up to two nodes. For example, it was possible to demonstrate the distribution of entanglement between quantum memories via optical fiber links over distances between approx. 500 m and 35 km. [80–84] 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). [85, 86] 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. [87–89] 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. [90, 91] The most advanced demonstration of a more complex quantum network consisting of three nodes was achieved using the NV centers in diamond. This experiment 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. [92] 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. [93–96] 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. [95, 97] The use of new entanglement-assisted protocols for classical communication can improve communication performance and prevent attacks on IT infrastructures. [98] Please refer to Azuma et al. [99] 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 "Quantum Repeater.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 [86] and the generation of entanglement between spatially separated qubits. [82] 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. [100] In addition, a number of research networks already exist. In academia, the "Chicago Quantum Exchange", [29] the "Brookhaven National Laboratory Quantum Network Facility (BNL)" [30] and the Center for Quantum Networks [31] should be mentioned here. In industry, the "AWS Center for Quantum Networking" [32], among others, has started developing quantum repeater components. 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" [101], 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. [102]

All these national and international efforts show that quantum repeaters are currently the subject of intensive research worldwide. As they 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.

5 Quantitative Analyses

5.1 Publication Analysis

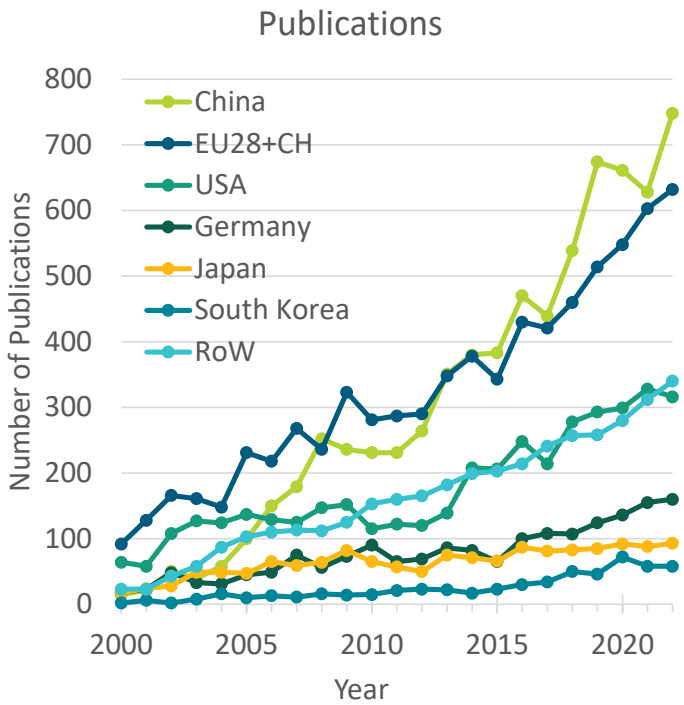
Scientific publications document the scientific progress in a certain field of technology. Analyzing how these develop can capture trends in scientific activities as well as the most important active players in a field.

We considered all peer-reviewed publications listed in Web of Science (WoS) for the period from 2000 to 2022 and used a keyword-based search strategy (for details see section 2).

Publication dynamics

The number of publications related to quantum communication has increased significantly and continuously over the last 20 years (Figure 1). While in 2000, approx. 200 publications were published globally on quantum communication, this number had risen to almost 2000 in 2022. 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 Japan, South Korea (both shown in (Figure 1), Canada, India, Russia, Australia, and Singapore (all bundled under "rest of world - RoW" in (Figure 1)).

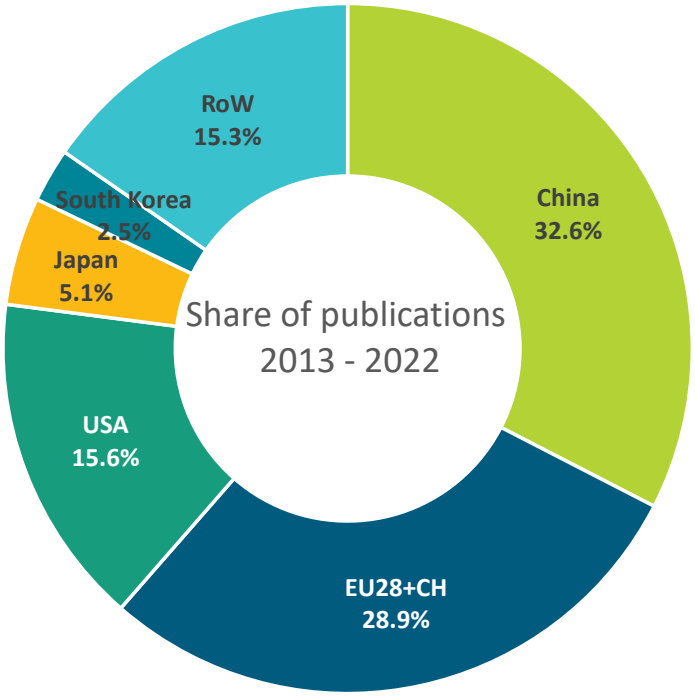
Figure 1: Peer-reviewed publications related to quantum communication of the countries with the highest number of publications from 2000 to 2022.



Country comparison

To compare the publication activities in different countries/regions, we summed up the number of publications in the last ten years of the period analyzed (2013-2022, Figure 2). China shows the highest publication activity in this time with a patent share of 33 percent, followed by the EU with 29 percent and the USA with 16 percent. Germany contributes 7 percent of the overall EU activities.

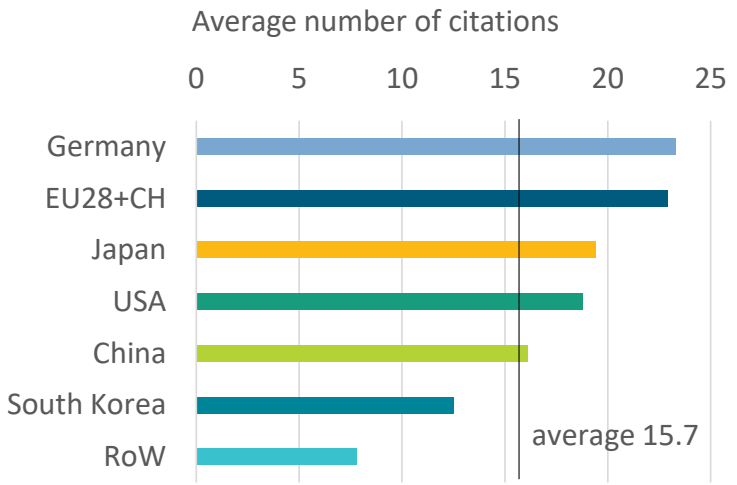
Figure 2: Share of QCom-related publications of the countries with the highest number of publications (and the EU) in the last 10 years of the period analyzed (2013-2022).



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 2019 in the different countries (Figure 3). Publications from the EU were cited on average 23 times (same for Germany), those from Japan and the USA 19 times, from China 16 times, from South Korea 13 times and all other countries 8 times. The global average was 16 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 3: Average number of citations of QCom-related publications from different countries (and the EU) from publications of the year 2019 (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 in the last two years of the period analyzed. 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., University of Science and Technology of China). 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 (10), followed by Europe (4, from France, Germany and Spain) and the USA (3).

Table 1: Institutions with the highest number of QCom-related publications in the years 2021-2022 (top-20):

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

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

To analyze European activities in QCom publishing, we listed the European institutions with at least 20 QCom-related publications in the last two years of the period analyzed (Table 2). In total, 34 institutions from the EU (EU28 + CH) published at least 20 papers in scientific journals. The largest number of institutions with a minimum of 20 publications are from France and the UK, followed by Germany, Spain, Italy, Austria, and Switzerland. 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 are below the 20-publication threshold chosen here. All institutions from Germany with at least 10 QCom-related publications in the years 2021-2022 are listed in Table 3.

Table 2: Institutions from EU28(+CH) with at least 20 QCom-related publications in the years 2021-2022:

Institution (country)	Number of patent applications (2021-22)
Centre National de la Recherche Scientifique (FR)	98
Udice French Research Universities (FR)	80
Max Planck Society (DE)	52
Universitat Politecnica de Catalunya (ES)	44
Austrian Academy of Sciences (AT)	41
University of Cambridge (UK)	40

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

Table 3: Institutions from Germany with at least 10 QCom-related publications in the years 2021-2022:

Institution (country)	Number of patent applications (2021-22)
Max Planck Society (DE)	52
Technical University of Munich (DE)	35
Helmholtz Association (DE)	28
Fraunhofer Gesellschaft (DE)	24
Munich Center for Quantum Science and Technology (DE)	19
Technical University of Berlin (DE)	15
Ruhr University Bochum (DE)	14
University of Munich (DE)	14
Heinrich Heine University Düsseldorf (DE)	12
German Aerospace Center - DLR (DE)	11
Ulm University (DE)	11
University of Siegen (DE)	11
University of Stuttgart (DE)	11
Free University of Berlin (DE)	10
Friedrich Schiller University Jena (DE)	10
Ruprecht Karl University of Heidelberg (DE)	10
Technical University of Darmstadt (DE)	10
Technische Universität Dresden (DE)	10

5.2 Patent Analysis

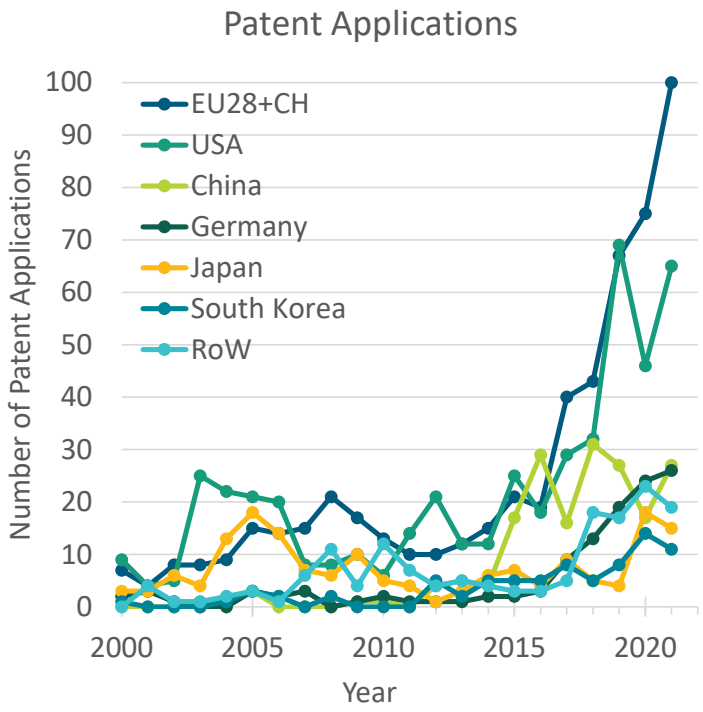
Patents often indicate commercial interest in a field of technology. Analyzing the development of patenting activities is one way to assess commercial interest trends as well as the active players in this field.

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.

Patent dynamics

Figure 4 shows the number of QCom-related patent applications between 2000 and 2021 from different countries (and the EU). Overall, a strong increase in patenting activity (from less than 20 in 2000 to more than 200 in 2021) can be observed, especially since 2014. The highest number of patent applications are from the EU (EU28 and CH), followed by the USA, and China. Other countries with relevant patenting activity include Japan, South Korea (both shown in Figure 4), Canada, Russia, Singapore, Australia, and India (all bundled under "rest of world - RoW" in Figure 4).

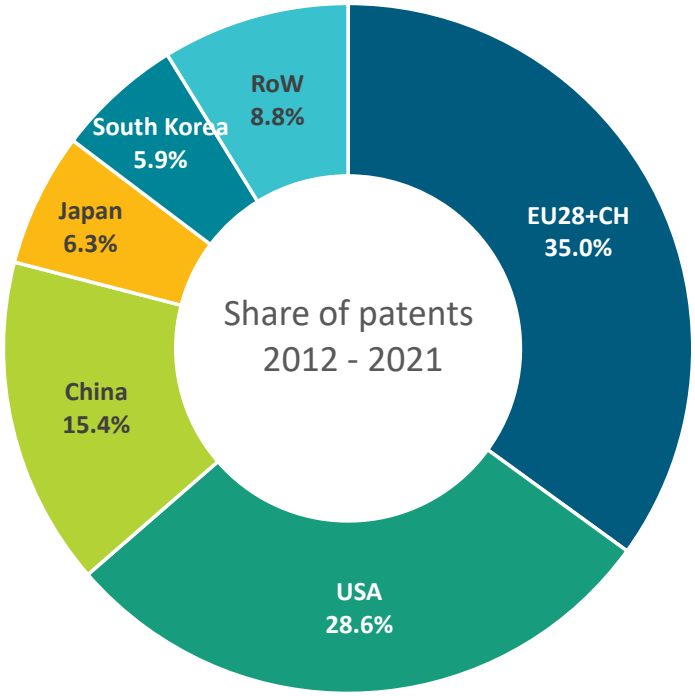
Figure 4: QCom-related transnational patent applications of the countries with the most patent applications (and the EU) from 2000 to 2021.



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 (2012-2021, Figure 5). The EU shows the highest patenting activity with a patent share of 35 percent, followed by the USA with 29 percent, and China with 15 percent. Germany contributes 9 percent of the total patent applications.

Figure 5: Share of QCom-related transnational patent applications of the countries with the most patent applications (and the EU) in the last 10 years of the period analyzed (2012-2021).



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 importing such technologies might be prohibited by national authorities. This might be reflected by greater interest in national patents rather than transnational patents.

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 2018-21 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 Intel, Arquit, Huawei, LG Electronics, Toshiba, and QuantumCTek), large telecommunications providers (including Deutsche Telekom and British Telecom) and research institutions/organizations (including MIT, Fraunhofer, Delft University of Technology, and South China Normal University). 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 technology development and thus do not appear in such analyses or not as prominently.

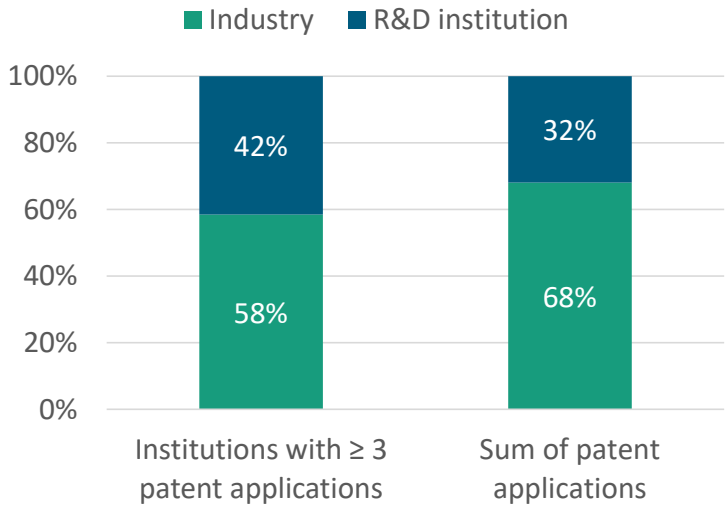
Table 4: Institutions with the highest number of QCom-related, transnational patent applications in the years 2018-2021 (top-20):

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

More than 40 percent of the institutions with at least three QCom-related patent applications between 2018 and 2021 are research institutions (Figure 6), 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.

[3] Note that the patents are assigned at company level and not at the level of the parent company.

Figure 6: **Shares of industry and research institutions with ≥ 3 QCom-related patent applications between 2018 and 21 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 three QCom-related patent applications in the last four years of the period analyzed (Table 5). Again, technology companies (including Arqit, Ericsson, ID Quantique, Terra Quantum, Thales, and Nokia) and large telecommunications providers (including Deutsche Telekom and British Telecom) are well-represented. However, in Europe more than globally, the QCom-related patenting activities are driven by research institutions/organizations (including Fraunhofer, Delft University of Technology, Netherlands Organization for Applied Scientific Research - TNO, Austrian Academy of Sciences, Centre National de la Recherche Scientifique - CNRS, CEA, Fundació Institut de Ciències Fotòniques - ICFO, and Max Planck Society). More than half of the institutions with at least three QCom-related patent applications are research institutions/organizations. These are, however, only responsible for one third of the patent applications (three or more QCom-patents). This implies that, in Europe, 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.

Table 5: **Institutions from EU28(+CH) with at least three QCom-related, transnational patent applications between 2018 and 2021:**

Institution (country)	Number of patent applications (2018-21)
Arqit (UK)	20
Huawei Technologies Düsseldorf (DE)	20
British Telecom (UK)	14
Ericsson (SE)	12
Fraunhofer (DE)	11
Delft University of Technology (NL)	10
ID Quantique (CH)	9

Institution (country)	Number of patent applications (2018-21)
Terra Quantum (CH)	6
Thales (FR)	6
Netherlands Organization for Applied Scientific Research (NL)	5
Austrian Academy of Sciences (AT)	5
Centre National de la Recherche Scientifique (FR)	4
CEA (FR)	4
Element Six (UK)	4
Fundació Institut de Ciències Fotòniques (ES)	4
Max Planck Society (DE)	4
Austrian Institute of Technology GmbH (AT)	3
Nokia Technologies Oy (FI)	3
University of Geneva (CH)	3
University of Warsaw (PL)	3
University of York (UK)	3
VTT Technical Research Centre of Finland Ltd (FI)	3

5.3 Meta-Market Report Analysis

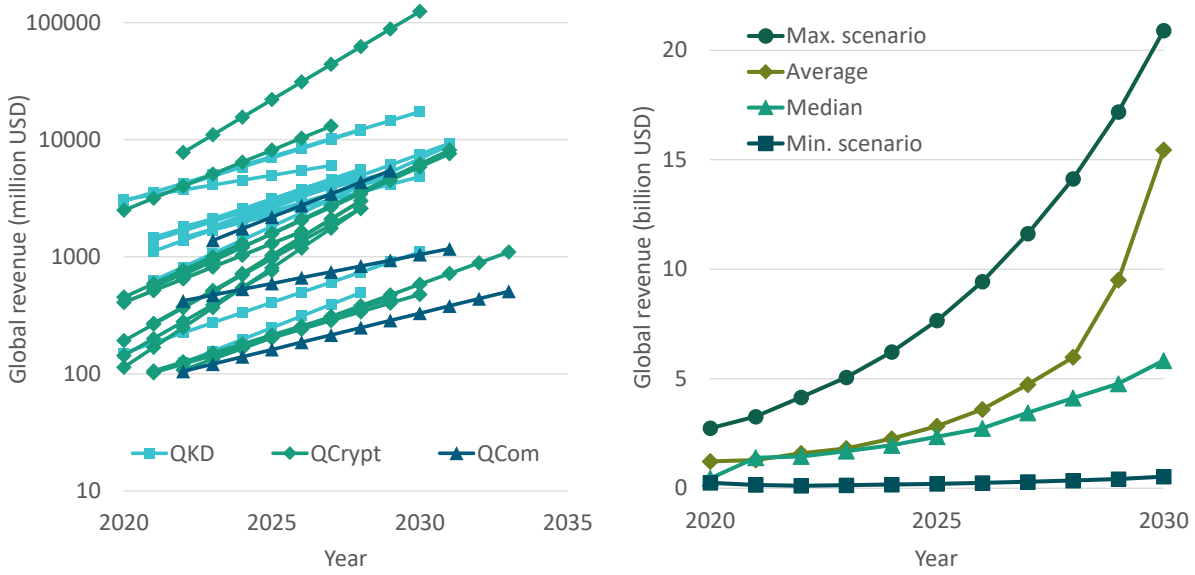
Assessing the global market size of an emerging field of technology is very challenging. Unlike established markets that are often dominated by large players and closely followed by trade associations, activities in emerging markets are typically driven by small companies, startups and R&D institutions. 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 studies is typically cost-intensive, which limits the possibilities of comparative analyses. However, many market study 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 68 market reports [103–170] published between 2019 and July 2023 on quantum communication, quantum cryptography, and quantum key distribution.

Market size and forecast trends

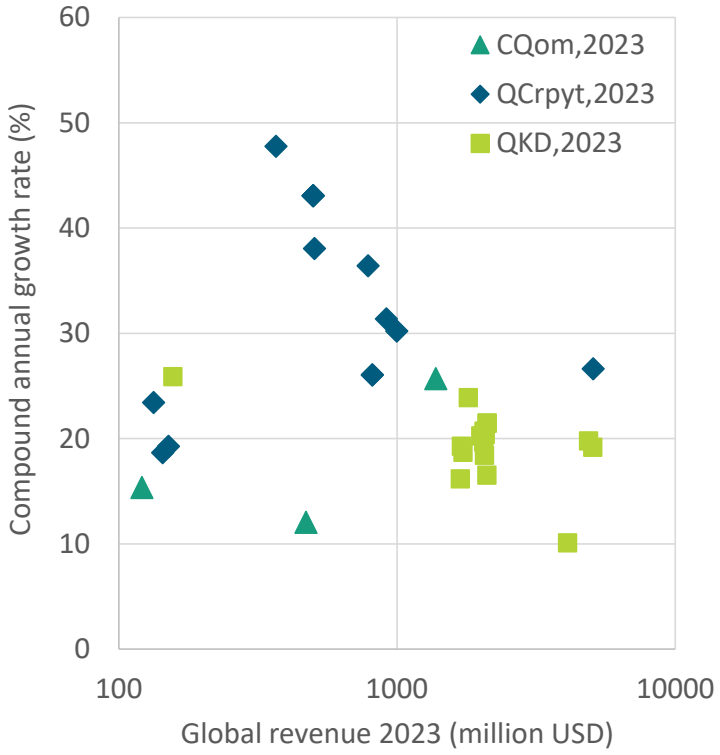
According to the analyzed market reports, global revenue in the markets for quantum communication, quantum cryptography and quantum key distribution is expected to grow significantly in the coming years (Figure 7). Compound annual growth rates (CAGR) of between 12 and 41 percent are predicted, although 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 120 million and 11 billion USD in 2023 and between 330 million and 124 billion in 2030 (left-hand graph in Figure 7). 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 7). The median calculation results in global revenue values of 1.7 billion in 2023 that increase to 5.8 billion in 2030. The future development is more likely to be somewhere between the highest and lowest predictions, possibly close to the mean or median curve.

Figure 7: **Revenue data from the 68 analyzed reports on the global quantum communication market between 2020 and 2035 (left) and results of our calculations (right).**



The analyzed market reports 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 8).

Figure 8: **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 68 studies leads to a ranking of the company names mentioned (Table 6). This analysis does not indicate which company is the 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.

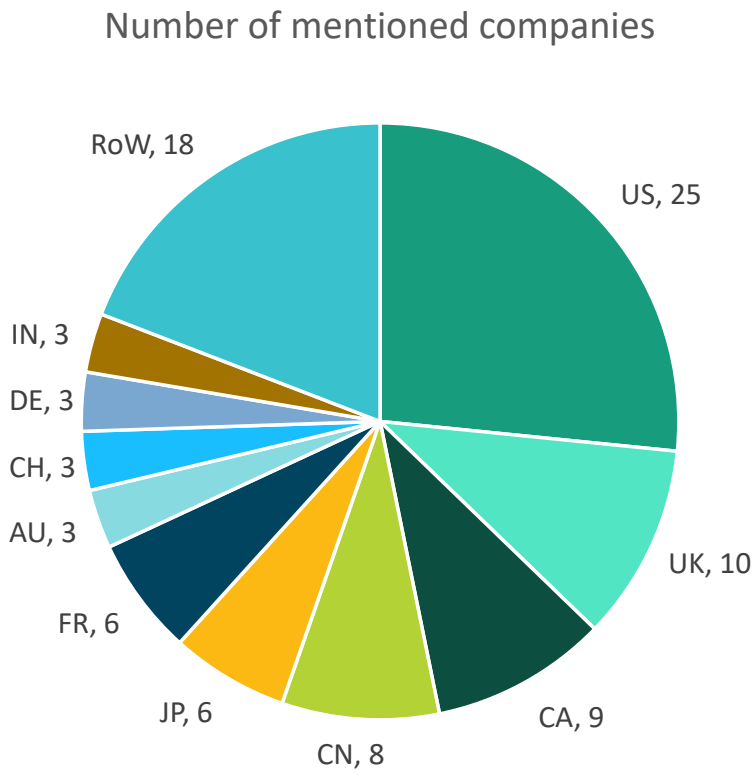
Table 6: **Companies with the highest number of mentions in market reports on QKD, QCom and QCrypt (top-20):**

Company/Institution (country)	Number of mentions
MagiQ Technologies (US)	65
Quintessence Labs (AU)	60
ID Quantique (CH)	60
Toshiba (JP)	58

Company/Institution (country)	Number of mentions
Qasky (CN)	51
QuantumCTek (CN)	48
SeQureNet (FR)	29
Qubitekk (US)	28
Crypta Labs (UK)	25
NuCrypt (US)	24
IBM (US)	21
PQ Solutions (UK)	21
NEC (JP)	21
Qudoor (CN)	19
Infineon (DE)	18
Quantum Xchange (US)	15
HP (US)	14
Qutools (DE)	14
ISARA (CA)	14
Mitsubishi (JP)	13

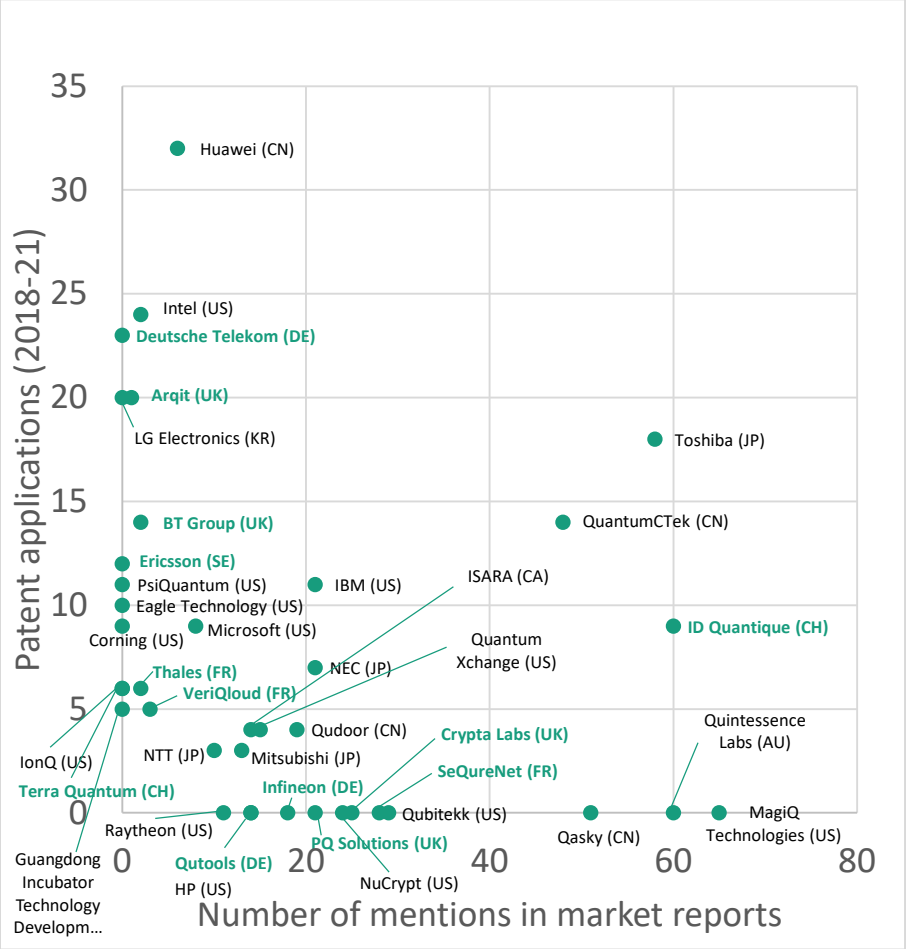
When analyzing the country of origin of the mentioned companies, the highest number come from the USA (25), the UK (10), and Canada (9), followed by China (8), Japan (6), and France (6) (Figure 9). The domination of companies from English-speaking countries again indicates the bias toward English-language companies.

Figure 9: Number of companies mentioned in the analyzed market reports by country of origin.



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 10 compares the number of mentions with the patenting activity of the relevant companies. It is surprising that the top five patent applicants Huawei, Intel, Deutsche Telekom, LG Electronics, 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 and Qasky did not show up in our patent analysis. Toshiba, QuantumCTek and ID Quantique are the companies with both significant patenting activity and frequent mentions in the market reports.

Figure 10: **Comparison of the number of patent applications and the number of mentions in market reports of companies with a minimum of 10 mentions or a minimum of 5 patent applications (European companies are high-lighted in green).**



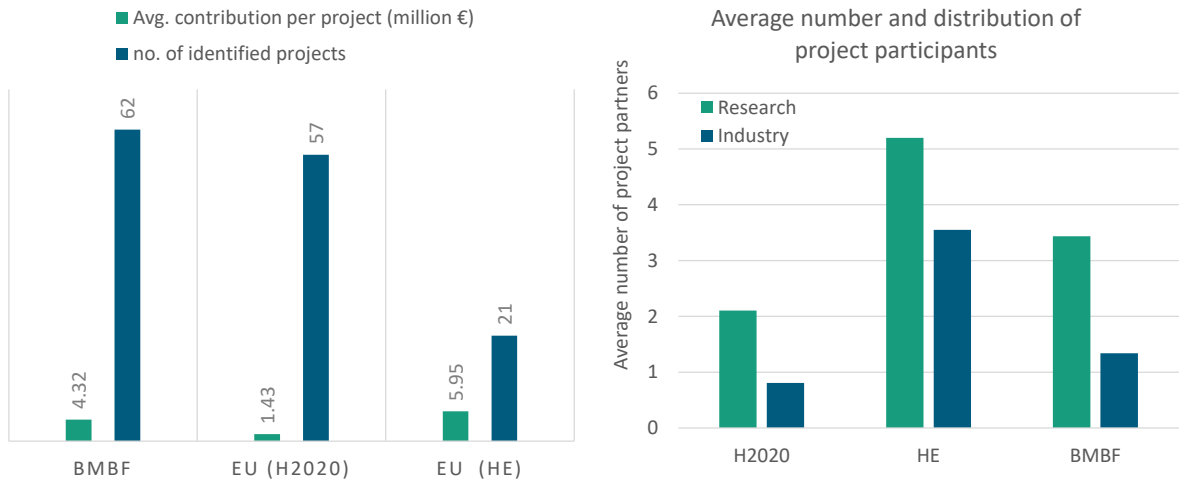
5.4 Project Monitoring

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 polices in a country or region. Accordingly, we investigated recent projects funded in the area of 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 the area of 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 in technologically advanced countries at the global level. The total expenditure on R&D in Germany in 2021 was reported to be about EUR 113 billion, which is more than 3 percent of the country's gross domestic product (GDP). [171] The German federal government provided EUR 22 billion of this, of which EUR 12 billion was allocated by the Federal Ministry of Education and Research (BMBF). BMBF 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. For this reason, BMBF-funded projects in the area of 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 2021, the EU's total R&D expenditure was reported to be about EUR 328 billion, corresponding to 2.27 percent of the Union's GDP. [172] We analyzed the major EU research and innovation funding programs, i.e., Horizon 2020 and Horizon Europe, for their projects in the field of quantum communication.

Figure 11: Number and average funding per project of identified BMBF and EU projects (left). Average number of project partners from industry and research institutions (right).



We identified 62 projects funded by the BMBF in the area of quantum communication as well as 57 projects and 21 projects funded by the EU framework programs Horizon 2020 (H2020) and Horizon Europe (HE), respectively (Figure 11, left). The identified BMBF projects have start times ranging from 2017 to mid-2023 and end times ranging from 2019 to 2026. The average BMBF contribution per project is about EUR 4.32 million. EU projects funded under H2020 (2014-2020), started in the period 2015-2021 and will end by 2026, with an average EU spending on each project of EUR 1.43 million. The HE phase (2021-2027) includes only the projects funded for the calls

launched in 2021 and 2022. These projects started in 2022 or 2023 and will end by 2027 with an average EU contribution per project of EUR 5.95 million. For both BMBF and HE, there may be additional projects funded in 2023 after the cutoff day of our analysis (July 2023).

Project participants in both the BMBF and EU programs are more often from universities and research and technology organizations as shown in Figure 11 (right). On average, there has been one industry participant in the projects funded by BMBF and H2020. For the short duration since the start of the HE program, a higher number of participants are reported for each project including more than three partners from industry on average.

Figure 12: Distribution of projects and estimated funding per year.

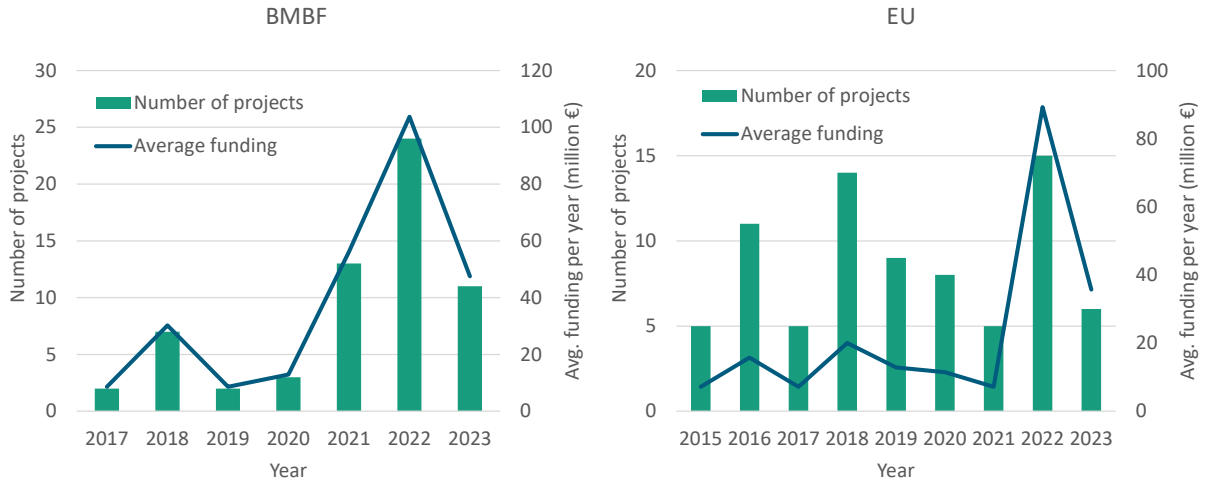
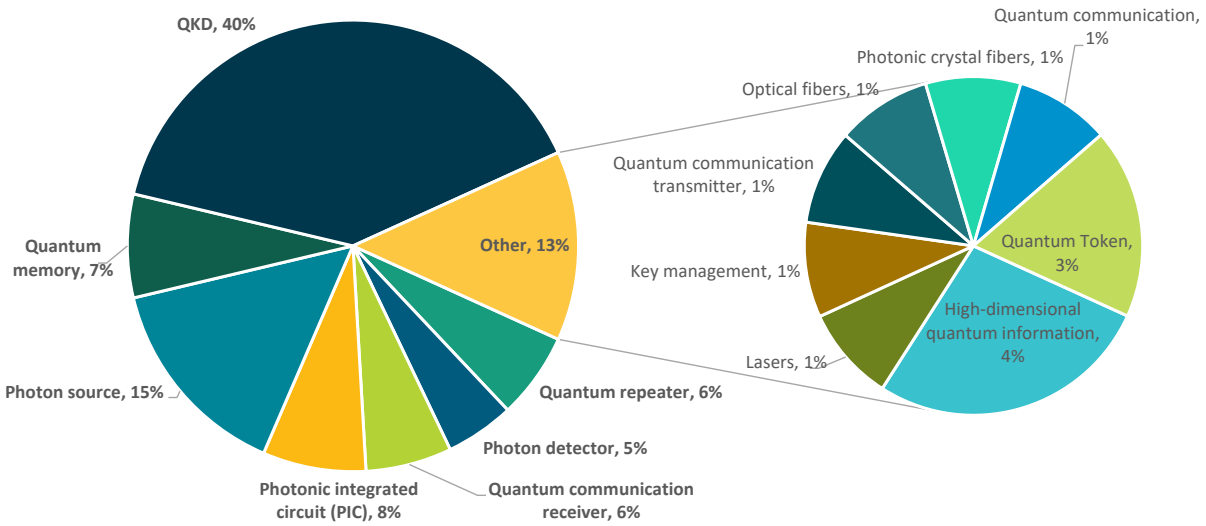


Figure 12Figure 11 shows the number of projects funded and an estimation of the allocated budget based on the average funding per project since 2015 and 2017. It can be seen that the number of projects funded by the BMBF and accordingly the annual investment have increased since 2021. A similar pattern can be observed for the start of the HE program with an increase in the number of projects in 2022 and a strongly growing average project budget in comparison with H2020. The reduction in the number of projects and average funding in 2023 is mainly due to the reported values comprising only the first half of the year. The trend of increased investment in R&I activities in quantum communication was expected to continue throughout 2023.

An analysis was also performed on the topics of the quantum communication projects funded in Germany and the EU. Figure 13 shows the distribution of topics addressed by the identified BMBF projects. Most projects focus on one topic, while a small number of projects address two topics according to the reported objectives and approaches.

Figure 13: Distribution of topics in the 62 identified projects funded by the BMBF.



As the figure indicates, a large proportion (40%) of projects deal with QKD subjects. The most relevant sub-topics here include QKD networks (44% of QKD projects), free-space QKD (25% of QKD projects), general QKD (22% of QKD projects), and QKD post-processing. Photon sources, photonic integrated circuits (PIC), quantum memory, quantum repeaters, and photon detectors account for about 15 to 5 percent of the identified projects. Topics such as high dimensional quantum information, quantum tokens, general concepts of quantum communication, key management systems, etc. are addressed by a small number of projects (4 to 1%).

Figure 14 shows the distribution of subjects among the identified EU projects funded under H2020. As the figure illustrates, quantum network, photon sources and QKD together constitute more than half of the subjects addressed by H2020 projects. The second group of subjects covers quantum memory, protocols and certification, theoretical subjects, quantum random number generators (QRNG), quantum repeaters, photon detectors, and quantum optics. There are also a few projects dealing with general quantum communication concepts, transceivers for quantum communication (excluding photon sources and detectors), quantum systems on chips, and the quantum internet. It should be noted that a smaller number of projects does not necessarily indicate the lower significance of the topic. For example, the quantum internet is a topic with high strategic priority for the EU. The corresponding project indicated among others in Figure 14 refers to the Quantum Internet Alliance [173], which is a large-scale initiative with H2020 funding of about EUR 10 million.

Figure 14: Distribution of topics in the 57 identified projects funded by Horizon 2020.

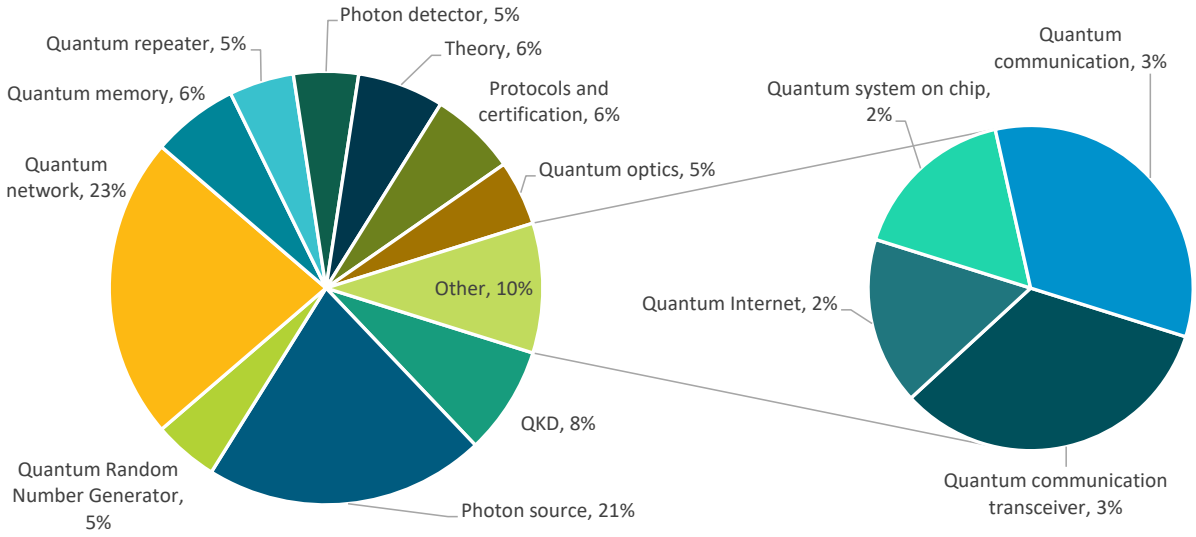
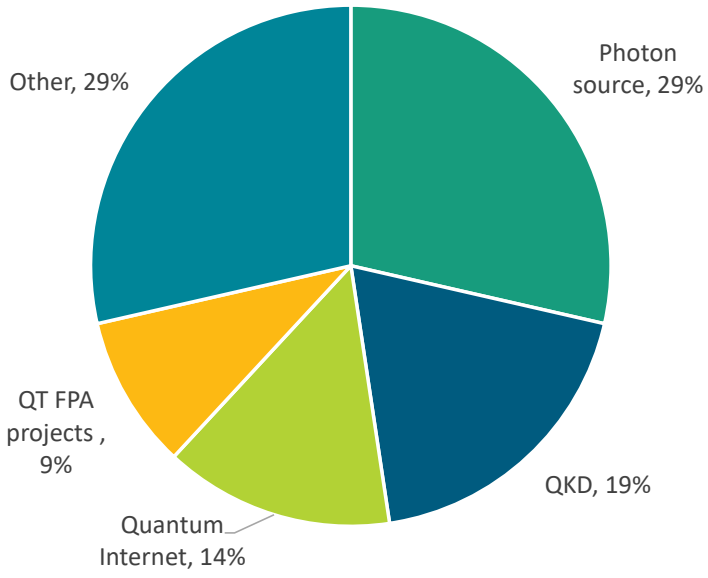


Figure 15 shows the subjects addressed in the identified projects funded by HE (calls 2021-2022). As the figure shows, photon sources, QKD and the quantum internet constitute over 60 percent of topics. There are also two funded projects based on the Framework Partnership Agreement (FPA) model for pilot line production and testing of quantum technologies including quantum communication. Among others, these projects include a photonics-pilot-line, photonic integrated circuits (PICs), entangled photon sources, and QRNGs. [174] Other topics account for about 30 percent and include QRNG, quantum modems, quantum systems on chips, quantum memory, and optical fibers, each addressed by one project.

Figure 15: Distribution of topics in the 21 identified projects funded by Horizon Europe.



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.[4]

Germany: QCom R&D activities in Germany are currently funded by two framework programs of the Federal Ministry of Education and Research (BMBF): "Quantum Technologien" and "Vernetzung und Sicherheit digitaler Systeme". "Quantum Technologien" was launched in 2018, following the announcement by BMBF that EUR 650 million would be allocated to quantum technologies. The program covers various quantum technologies, including quantum computing and simulation, quantum-based measurement techniques, basic technologies for quantum systems, as well as quantum communications (QCom). The "Vernetzung und Sicherheit digitaler Systeme" program focuses on three main topics: IT-security, communication systems, and living in a digitalized world. QCom is considered a key technology for enhancing IT-security.

Although our comparative 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 EUR 11 million to the Fraunhofer IOF to build a quantum communications infrastructure. [175] In addition to the existing programs, the BMBF released a new strategic document "Action Concept Quantum Technologies" [176] in April 2023, announcing funding of approx. EUR 2.18 billion for quantum technologies from 2023 to 2026.

Strategic Goals for QCom in Germany: Under the framework of "Quantum Technologien", the focus is to support the transition from science-led quantum research to novel applications. The new Action Concept also describes the long-term goal of establishing advanced technologies with a wide range of applications in 2036. In "Vision 2036" of the Action Concept, QCom is mentioned as a means of providing additional security for sensitive data.

The strategic document also mentions the following milestones by 2026 for QCom:

- Establishment of the first tap-proof, i.e., quantum-encrypted, communications test links between selected government sites.
- Realization of a nationwide fiber optic backbone for quantum communications and time and frequency distribution.
- Demonstration of first quantum repeater test links.
- Launch of first test satellites for QKD.

European Union: For the EU, QCom is funded by the Horizon 2020/Horizon Europe programs (focusing on R&D) and EuroQCI [37] (focusing on infrastructure and technology deployment). For detailed information on the projects within the Horizon program, please refer to section 5.4.

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

- EUR 154 million under the Digital Europe Programme, which includes industrial projects, national projects and a coordination and support action to link them all. [177]
- EUR 90 million 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. [178]

[4] In this section, the calculations assumed 1 EUR = 0.86 GBP, 156.25 JPY, 1.11 USD, 1.46 CAD, 91.17 INR and 7.77 CNY

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

Strategic Goals for QCom in the EU: The long-term vision of the EU is the development of a quantum internet throughout Europe. To achieve this goal, the Quantum Flagship and EuroQCI initiatives have been launched.

The Quantum Flagship distributes funding under Horizon 2020 and Horizon Europe. Its priorities are outlined in a Strategic Research Agenda, which sets short-term (3 years) and medium/long-term (6-10 years) goals for each technology area, including QCom.

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 late 2024.

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. USD 337 million 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. [179]

In addition to this, the National Laboratory of Quantum Information Science was launched in 2017 with an initial investment of CNY 7 billion (approx. EUR 900 million). There are also plans to invest a further CNY 100 billion (approx. EUR 13 billion) over five years, [180] which accounts for most of the estimated total investment in quantum technologies (QT) in China.

During the 14th Five-Year-Plan period (2021-2025), quantum research in China will be further supported through "Major Projects" under the Innovation 2030 program. However, as of August 2023, its funding guidelines have not been made publicly available, and the details are not clear.

Provincial governments in China also play an important role in R&D funding. For example, the new Anhui Quantum Science Industry Development Fund, established in 2017, has announced plans to devote CNY 10 billion in funding to quantum computing, communications and metrology. [180]

While the exact total amount of public funding in China is still 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 USD 100 million within China's Strategic Priority Programme on Space Science [181] as part of the Quantum Experiments at Space Scale (QUESS) project. Another important achievement is the establishment of a quantum communication network, comprising a 2,000 km fiber-optic link between different cities (Shanghai, Hefei, Ji-nan and Beijing) and a 2,600 km satellite link between two observatories.

Strategic Goals for QCom in China: Quantum technology is included as one of the prioritized frontier technologies in the 14th Five-Year Plan in China [182], although a QCom-specific strategic objective is not mentioned directly in the plan.

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. [183]

United States: In December 2018, the National Quantum Initiative (NQI) Act was passed to accelerate quantum R&D to ensure the economic and national security of the US. Initially, over USD 1.2 billion were pledged over five years, but according to the latest budget report, the strategy was already expected to allocate approximately USD 2 billion by FY2023 along with about USD 1.7 billion of the budget for baseline R&D activities in quantum technologies in relevant agencies. [184]

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). In 2023, at the mid-point of the 10-year initiative, the House Science Committee heard testimony on ideas for expanding the NQI. One discussed option was to involve additional agencies, particularly the National Aeronautics and Space Administration (NASA), in order to catch up with China in developing quantum communication satellites. [185]

The NQI categorizes its activities into five different component areas, one of which is "Quantum Networks and Communications (QNET)". We focused on QNET to identify QCom-relevant programs and projects. The NQI budget report discloses that approx. 10 percent of the R&D budget for Quantum Information Science (QIS) was spent on QNET.[5] Examples of the NQI instruments for QNET R&D are:

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

Strategic Goals for QCom in the US: 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: [186]

- 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. [187]

United Kingdom: The UK National Quantum Technologies Programme (NQTP) was launched in 2014, representing a GBP 1 billion partnership between government, academia and industry. QCom-related projects and programs were identified on the NQTP website, providing insights into its research focus. [4] These include the Quantum Communication Hub (2014-2024 with GBP 49.8 million), a quantum satellite project with Singapore (with GBP 10 million), and 26 projects supported by the Industrial Strategy Challenge Fund.

Furthermore, in 2023, the UK government published its new strategy for the period 2024-2033 with plans to invest more than GBP 2.5 billion 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. [188]

[5] The published budget data include both funding under the NQI and base funding; it is unclear how much QNET research is conducted under the NQI. Therefore, funding under the NQI was estimated by multiplying the QNET research budget by the ratio of the NQI funding for all the quantum topics for each year. Roughly half of the total quantum research budget is spent under the NQI.

Strategic Goals for QCom in the UK: The new 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.").

However, neither the UK NQTP nor the new strategy includes a specific objective for QCom issues. The new strategy states that the focus is on realizing the potential of QCom for secure communications, where clear benefits can be demonstrated, and the opportunities provided by QCom to network quantum computers, share information, and address data storage challenges.

Japan: The Japanese government released its Quantum Technology Innovation Strategy in 2020 (FY2019[6]) 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 FY2023.

The majority of public funding for QCom in Japan, approximately 73 percent, is allocated to projects led by the Ministry of Internal Affairs and Communications (MIC). Since FY2018, the MIC has supported 7 projects focusing on various areas 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.

Another important 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. [189]

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

South Korea: In 2023, South Korea unveiled its first comprehensive quantum strategy, pledging more than 3 trillion won (approx. EUR 2.1 billion) in public-private co-investment by 2035 to establish itself as a global hub of the quantum economy. In terms of QCom, the strategy aims to develop a 100 km-scale quantum network in the 2030s and promote intercity experimentation. [190]

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

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. [191] The project requires a total of 82 billion won (approx. EUR 58 million), with 54.1 billion won for the first phase and 28.6 billion won for the second phase. The final goal of the project is to develop a network covering up to 2,000 km. [192]

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. [193]

Prior to releasing this strategy, Canada had already invested over CAD 1 billion (approx. EUR 680 million) 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 over CAD 30 million for the design and implementation phases of the QEYSSat mission. [194] The satellite is scheduled for launch in 2024/2025 and will connect ground stations more than 400 km apart using BB84 and BBM92 protocols. [195]

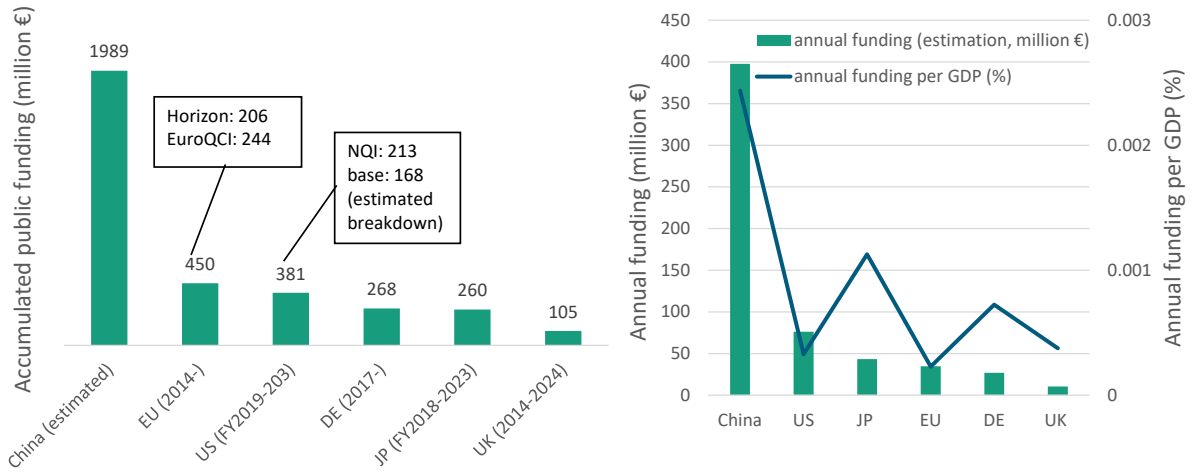
India: In April 2023, the Union Cabinet of India approved the National Quantum Mission with a total cost of INR 60 billion (approx. EUR 677 million) from 2023/24 to 2030/31. The expected deliverables of the Mission include satellite-based secure quantum communications between ground stations over a range 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 also plans to establish four thematic hubs in top academic and national R&D institutes, with one of the hubs focusing on quantum communications. [196]

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 16 compares the total amount of funding allocated in 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 16: Accumulated amount of public funding in QCom, announced up to August 2023 (left) and total annual amount of public funding in QCom (bar graph) and per GDP (line graph) (right).



Based on our estimation[7], China appears to be, by far, the most active country in funding QCom research, followed by the US, and the EU. In the case of the EU, funding under the EuroQCI contributes more to the total funding than the Horizon programs. Germany and Japan are at a similar level in terms of QCom, although Germany is estimated to invest much more in QT in general (EUR 3.5 billion in Germany compared to 1.6 billion in Japan[8]). The UK's investment is lower than that of the other analyzed countries, but may be underestimated due to the lower availability of information.

Due to the different time horizons of the funding programs in the analyzed countries, a slightly distorted picture might result from comparing overall funding volumes. Therefore, we calculated the annual funding (bar graph on the right-hand side of Figure 16) by dividing the cumulative funding by the period of the relevant strategy. China leads in this comparison as well, followed by the US, Japan, Germany, and the UK. In the case of Germany, the end of the funding program is unclear so the period from 2017 (start of the first regarded project) to 2026 (end of the latest project) was used. Since new projects could start after 2023, the annual funding for Germany is necessarily underestimated.

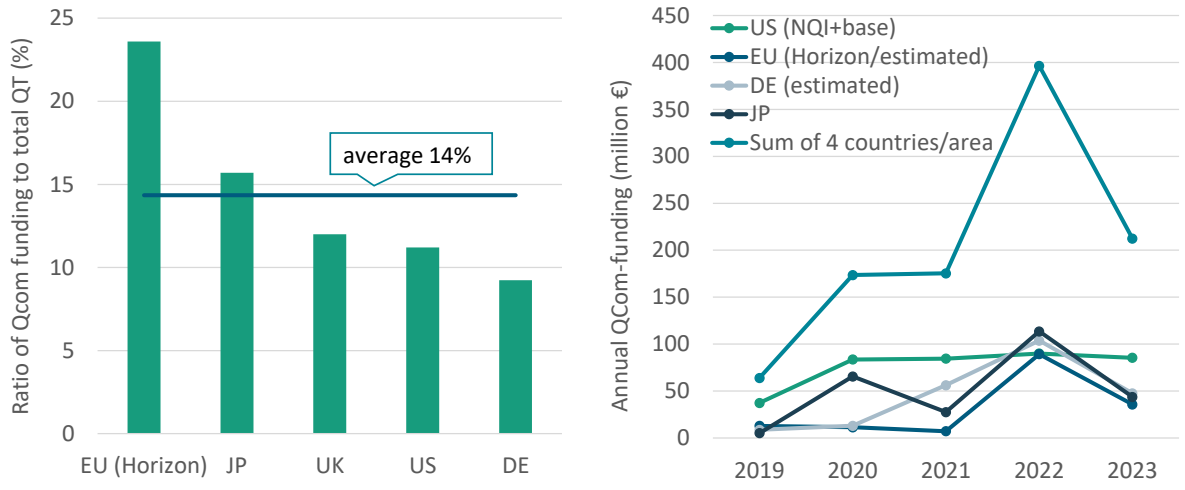
To enable a fair comparison of the amounts of QCom funding despite the different size and financial basis, we related the annual QCom funding to the gross domestic product (GDP) of the country (line graph on the right-hand side of Figure 16). Figure 16 (right) shows that while China still stands out, the figures for Germany and Japan move closer to China and even 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 be closer to that of Japan's.

[7] Note that our analysis only provides a rough estimate of China's funding by multiplying the announced government investment in quantum technologies (McKinsey&Co. 2023) [7] and the averaged QCom ratio to the total QT funding (Figure 17, left).

[8] Total amount of funding refers to the CIFAR report (2021) and the data collected in our analysis

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.

Figure 17: 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 (2019-2023) (right).



According to Figure 17 (left), the EU appears to focus nearly a quarter of its QT funding on QCom (23.6%). In particular, two SGA projects under the Framework Partnership Agreement (Quantum Secure Networks Partnership and Quantum Internet Alliance) make a significant contribution. SGA projects often have larger budgets than other projects, and two of the seven SGAs under the Quantum Flagship are related to QCom research, resulting in the relatively high QCom share of EU funding.

After the EU, Japan has the next highest ratio (15.7%). The UK, US, and Germany show a similar level of concentration on QCom, with around 10 percent of total funding. These countries allocate more funding to quantum computing than to QCom.

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 17 (right) shows the general development of funding over these five years in the US, EU, Germany, and Japan.

Overall, all four have increased their funding for QCom since 2019. Looking at the sum of the funding for three countries and the EU, the figure in 2023 is more than three times the figure in 2019. While the US has consistently spent around EUR 90-100 million since the inception of the NQI (EUR 50-60 million each year), funding in the EU, 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. The decrease in contributions in 2023 is mainly

caused by the reported values comprising only the first half of the year and the trend of increased investment is expected to continue after 2023 (see the project monitoring section for details). In the case of Germany, this expectation is also supported by the new strategy, which already plans to allocate more than EUR 2 billion to QT between 2023 and 2026 (see the next subsection for details).

The sudden jumps in Japanese funding in FY2020 and FY2022 are primarily attributed to one-year funding from the supplementary budget, which is reserved for urgent needs. In particular, the establishment of the Quantum Security Research Hub (with approx. EUR 51 million) and the two testbed projects (with approx. EUR 89 million) by the Ministry of Internal Affairs and Communications (MIC) have contributed significantly to these increases. At the same time, the MIC has recently increased its budget for longer-term (five-year) projects, and therefore public funding in Japan is expected to remain at a higher level after the FY 2023, at least compared to the FY 2019.

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 and our estimate of the QCom ratio.
- 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 state funding, such as 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. [7]

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 and deployment of new and standardized QKD-components. Several funded projects pursue the development of testbeds as a crucial part or ultimate goal. Prominent examples are the EU- and BMBF-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 QR.X-consortium as well as in projects funded by the so called Länder-Initiativen or beyond as for instance the Munich Quantum Network (MuQuaNet).

Testbeds allow for operating and evaluating devices in real world test 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 optical amplifiers and scattering of co-propagating classical channels. 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 BMBF-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 18). [197]

Figure 18: **Initial 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 consists 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 (2024).

On the map - so far - there are 14 testbeds listed, that are distributed over Germany. The testbeds are in Berlin, Thuringia, Lower-Saxony, Saxony, Saarland, and North-Rhine Westphalia. 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, the Berlin Quantum Communication Testbed is shown that consists of fibers and a free space link. In the bottom right, the MuQuaNet is shown. The specifications of the fiber testbeds can be found in Table 7. 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 limit for possible fiber-based optical transmission of QKD signals without trusted nodes or quantum repeaters that are currently researched and not yet available. 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 intra city links and therefore close to the conditions of later applications. Intra-city and intercity dark fibers are rented from commercial providers. As can be seen from Table 7, 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.X project that focuses on the development of quantum repeaters. 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 reference as well as classical communication signals. Here, first experiments test high-repetition rate QKD with semiconductor quantum dot single photon sources. 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.

One network that may prove valuable for the development of QKD is the R&D SASER network, which emerged from the BMBF-funded SASER project of the same name. As part of the project, a Germany-wide fiber network was established and continuously developed with the aim of supporting tests of optical fiber communication technologies. The R&D SASER network, which has its origins in the research and development of classic communication technologies, was not originally designed for QKD applications. Within Berlin, the SASER test network has a star-like network architecture with the central node at Deutsche Telekom Winterfeldstraße (WFD) and includes dark fibers to various locations such as Fraunhofer HHI, Humboldt University and various other locations with a total length of more than 500 km. The fully interconnected network architecture includes at least 12 nodes and allows both dense wavelength division multiplexing (DWDM) and wavelength-independent optical switching, which enables the transmission of quantum channels.

Apart from QKD transmission testbeds, there are also testbeds focusing on individual key components of QKD devices that are not listed in the testbed map, yet. At PTB, for instance, there are testbeds for 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.

Table 7: Overview of the QKD link 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).

Name	State	Type	Length	Wavelength	Status
Saarbrücken QCom Fiber Testbed	Saarland	fiber	14 km	O-band (1310 nm) to C-band (1550 nm)	operational
Jena – Erfurt Fiber Link	Thuringia	fiber	76 km	C-band (1550 nm)	operational
Campus Network Beutenberg	Thuringia	fiber	<1 km	O-band (1310 nm), C-band (1550 nm)	operational
Berlin Quantum Communication Testbed	Berlin	fiber	up to 26 km	dark fiber	operational
Niedersachsen Quantum Link	Lower-Saxony	fiber	78 km	C-band (1530-1565 nm)	operational
PhoQSNet	North-Rhine-Westphalia	fiber	9 km	O-band (1310 nm), C-band (1550 nm)	planned
Dresden QCom Fiber Testbed	Saxony	fiber	up to 20 km	O-band (1310 nm), C-band (1550 nm)	operational
Dresden QCom Fiber Testbed (in-house)	Saxony	fiber	200 m	810 nm, O-band (1310 nm) to C-band (1550 nm)	operational
Munich Quantum Network (MuQuaNet)	Bavaria	fiber and FSO	<1 km < 23 km	800 nm, C-band (1550 nm)	partially operational
tubLAN Q.0	Berlin	fiber and FSO	<1 km	780-950 m, O-band, C-band	planned
Free-space Link Jena	Thuringia	FSO	1.7 km	500 nm - 2 µm	operational
FSO testbed Oberpfaffenhofen	Bavaria	FSO	7 km	VIS, 589, 850, 1064, 1550 nm	operational
Optical Ground Station Oberpfaffenhofen	Bavaria	OGS	n/a	VIS, 589, 850, 1064, 1550 nm	operational
Optical Ground Station Jena	Thuringia	OGS	n/a	n/a	planned

6 Technology Sovereignty Considerations

According to the German government's Action Plan for Quantum Technologies ("Handlungskonzept Quantentechnologien"), Germany is striving for technology sovereignty in quantum communication technologies in collaboration with its European partners. [176] Technology sovereignty, however, involves many facets and aspects that we want to discuss in this chapter 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. [8] Building on this and on experts' opinions, 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. These key technologies include next-generation electronics, communication technologies, AI and software, data technologies, quantum computers, technologies needed to realize the circular economy or enable material innovations, batteries for electric vehicles and stationary storage systems, hydrogen technologies, and immunization technologies. [198] 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 recent 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". [199] 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 8).

Table 8: 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
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 traditional algorithms (e.g., AES-256) 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 Education and Research (BMBF) has specifically formulated the goal of achieving technology sovereignty in quantum communication and even aims for the global leadership in communication technologies. [200] In cooperation with other ministries, it has published an Action Plan for Quantum Technologies to coordinate responsibilities. Other actors from science, industry and politics have already formulated their perspectives of the potential measures to be taken. [201, 202]

However, which skills are to be maintained or developed within Europe is still open to discussion and might depend on whether stakeholders are from science, industry, politics or society. The following discussion aims to give an overview of these different perspectives. As it is based on several expert interviews, as described in section 2, it 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 experts interviewed 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 security of the communication channels used is therefore part of a nation's critical infrastructure. [203]

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, perfect PQC could make quantum communication approaches obsolete. However, there is currently no proof (or counter-proof) that PQC algorithms can resist quantum 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 decryptions based on fundamental physics 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 interviewed experts. 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 technology fields with potentially even larger markets (e.g., the 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 9: 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. [9] 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 discussed hampering factors is not exhaustive.

Table 10: 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 (public institutions) – End users from industry
Institutional factors	What are the relevant framework conditions (political, regulatory, societal, environmental, etc.)?	+ Commitment of authorities – Approvals and certifications

Cost factors

Currently, the challenges to do with the cost of innovating QCom are adequately 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 called for larger funding programs, especially to set up large-scale projects in Europe. Private investments, on the other hand, are currently very limited. To push QCom development, further investments by industrial players are strongly desired in Europe.

In the upcoming years, substantial investment in European QCom infrastructure is required to enable large-scale implementation. QKD systems, which are currently being commercialized, are still expensive and often require specialized infrastructure, such as dark fibers. 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 if these change following elections. This lack of certainty represents an investment risk for those institutions and companies dependent on public funding.

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 be lacking competence in developing and producing 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.

Even though this puts Europe QCom 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 of Qcom technologies with conventional technologies is another major challenge that might not be addressed adequately so far. More in-depth knowledge about the relevant security aspects and potential security risks of QCom technologies might still be required. Furthermore, technologies for specific QCom approaches, such

as quantum repeaters, are still at very low maturity levels and need scientific breakthroughs for further development.

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. 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 must be intensified. 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.

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.

Market factors

It is not yet clear in what time frame markets for QCom technologies will emerge. As governmental institutes rely on secure communication networks, there is already a considerable potential market here for QCom technologies 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.

Governmental institutions and public organizations can only implement QCom technologies if these are approved by the respective authority (in Germany: Federal Office for Information Security - Bundesamt für Sicherheit in der Informationstechnik, BSI). At present, no QCom technology has been approved for these stakeholders, as it has not yet been possible to provide sufficient proof of security. As the emergence of this approval-reliant market is controlled by a few national authorities, 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 as potential early adopters have a very important role to play for this field of technology, as there are no signs of any private-sector market emerging. The lack 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?).

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 undermine the concerted efforts of other stakeholders, such as European standardization activities.

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.

The approvals that have to be issued by the corresponding authorities act as a gatekeeper to large parts of the potential QCom market. The definition of certifications for QCom systems and components that could be issued by testing laboratories could provide more clarity for technology providers and potential end users. However, reliable proofs of security are required for the development of certifications and approval protocols. As long as these proofs are not being developed or are not accepted by the respective authorities, they pose a critical bottleneck for the adoption of QCom technologies.

Furthermore, regulations preventing the use of QCom systems developed abroad 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 are still under development. [204] 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 national and European public funding schemes have to comply with competition law regulations. This as well as other bureaucratic processes could delay or prevent the realization of large projects.

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 list of challenges was used to formulate recommended measures for the respective actors. Again, the list of measures does not claim to be exhaustive, as it is based solely on the interview results.

Table 11: Challenges and measures for achieving technology sovereignty in quantum communication technologies within Europe:

Dimension	Challenges	Measures
Cost factors	• High investment cost for infrastructure and QCom technologies • High risk for investments • Reliability of investments	• Continuation of public funding • Incentives for end-users from industry • Investments in European infrastructure
Knowledge factors	• Understanding security aspects • Quantum repeaters • Awareness of QCom	• Education programs for stakeholders from relevant disciplines • Outreach

Dimension	Challenges	Measures
		• 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 • Removing bottlenecks for approvals
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

Most of the experts interviewed said that public funding levels should be maintained over the coming decade to minimize the risks for science and industry. As large and stable funding programs are the main drivers of the current innovation activities, their continuation is of great importance.

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

Scaling up the production 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.

Knowledge factors

As a skilled workforce is needed to innovate and implement QCom technologies, education programs should be developed. 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.

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 needs 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 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.

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 should be identified and informed 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. The demand of public institutions for QCom technologies should be promoted as soon the requirements for the relevant approvals of the respective authorities are have been established.

Potential business models for all stakeholders in the QCom value chain should be discussed and their cooperation encouraged. Networking between science, industry and policymakers should be promoted in order to clearly communicate the different stakeholders' needs.

Institutional factors

Transparent requirements for approvals are important for all European member states. The creation of certificates could play an important role in providing well-defined guidelines for further technology developments and system production.

Complex bureaucratic processes for acquiring funding or at other steps of the QCom value chain 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. 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, including a close exchange among national authorities regarding upcoming decisions and strategies. The activities within EuroQCI, should be continued and extended with the goal of setting up a European QCom infrastructure. 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.

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

7 Conclusions

Quantum communication represents a group of strategically important technologies to ensure 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), while others are still the subject 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, 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 or to become independent of potentially insecure "trusted nodes", on the other hand, 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 obtain 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 removed including the lack of security proof, certification and approval. This requires the close cooperation of different stakeholders from research, industry and public sectors (authorities, policymakers).

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 a huge amount of 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.

8 Acknowledgements

The authors gratefully acknowledge the funding by the Federal Ministry of Education and Research – Bundesministerium für Bildung und Forschung (BMBF), Germany, as well as the coordination of the project execution by the Projektträger VDI/VDE Innovation und Technik GmbH.

Funding reference: 16KISQ116, 16KISQ115, 16KISQ112K

We would like to thank all the experts from academia and industry who supported us by participating in interviews. Furthermore, we would like to thank our colleagues from Fraunhofer ISI: Karin Herrmann for layout work; Paul Städter for research on market studies; Gillian Bowman-Köhler for English language corrections and translations; 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 and Nicolas Spethmann for their valuable input regarding the testbed infrastructure in Germany.

References

References

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

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

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

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

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

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

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

[8] Edler J *et al* 2020 *Technology sovereignty. From demand to concept*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[42] Zhang Y, Bian Y, Li Z, Yu S and Guo H 2024 Continuous-variable quantum key distribution system: Past, present, and future *Applied Physics Reviews* **11**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[76] 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)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[98] Bassoli R, Boche H, Deppe C, Ferrara R, Fitzek F H P, Janssen G and Saeedinaeeni S 2021 Quantum Communication Networks: Design and Simulation *Quantum Communication Networks (Foundations in Signal Processing, Communications and Networking)* ed R Bassoli *et al* (Cham: Springer International Publishing) pp 187–209

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

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

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

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

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

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

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

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

[107] Adroit Market Research 2020 *Quantum Cryptography Market By Component (Hardware, Software, Services), Algorithm Type (Symmetric Key, Asymmetric Key), Enterprise Size (Small and Medium Enterprise (SMEs), Large Enterprise), Encryption Type (Network Encryption, Database Encryption, Application Security, Cloud Encryption), Deployment Protocol (TSL/SSL Protocol, BB84 Protocol), Application (Simulation, Optimization, Sampling) and Region Global Forecast 2021 to 2028* (Adroit Market Research)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[175] Fraunhofer 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)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[203] 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)

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