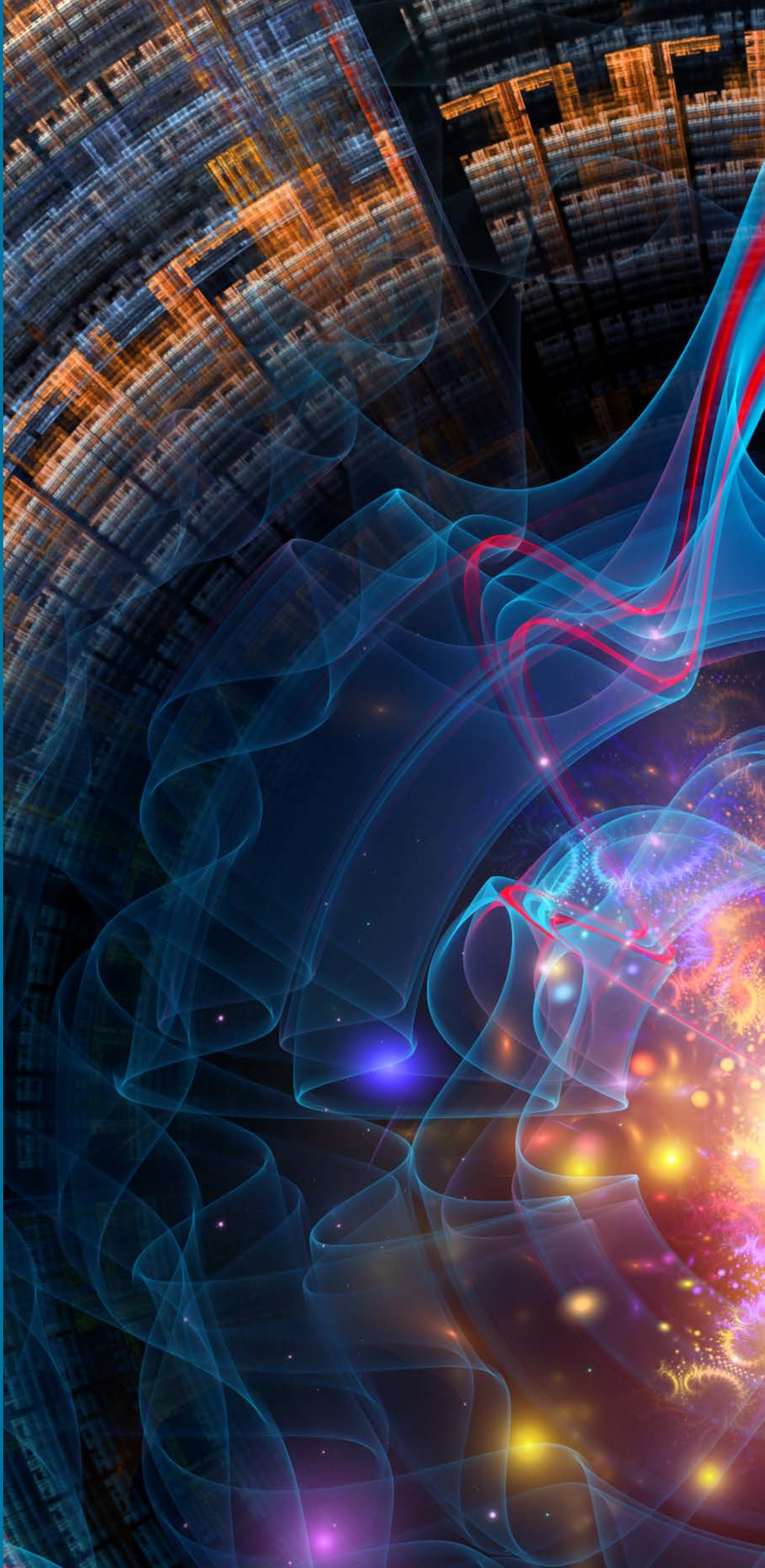
Federal Ministry
of Education
and Research

HIGH-TECH STRATEGY 2025
Talents. Skills. Innovations.

Quantum technologies – from basic research to market

A Federal Government Framework Programme

Table of Contents



1 Introduction

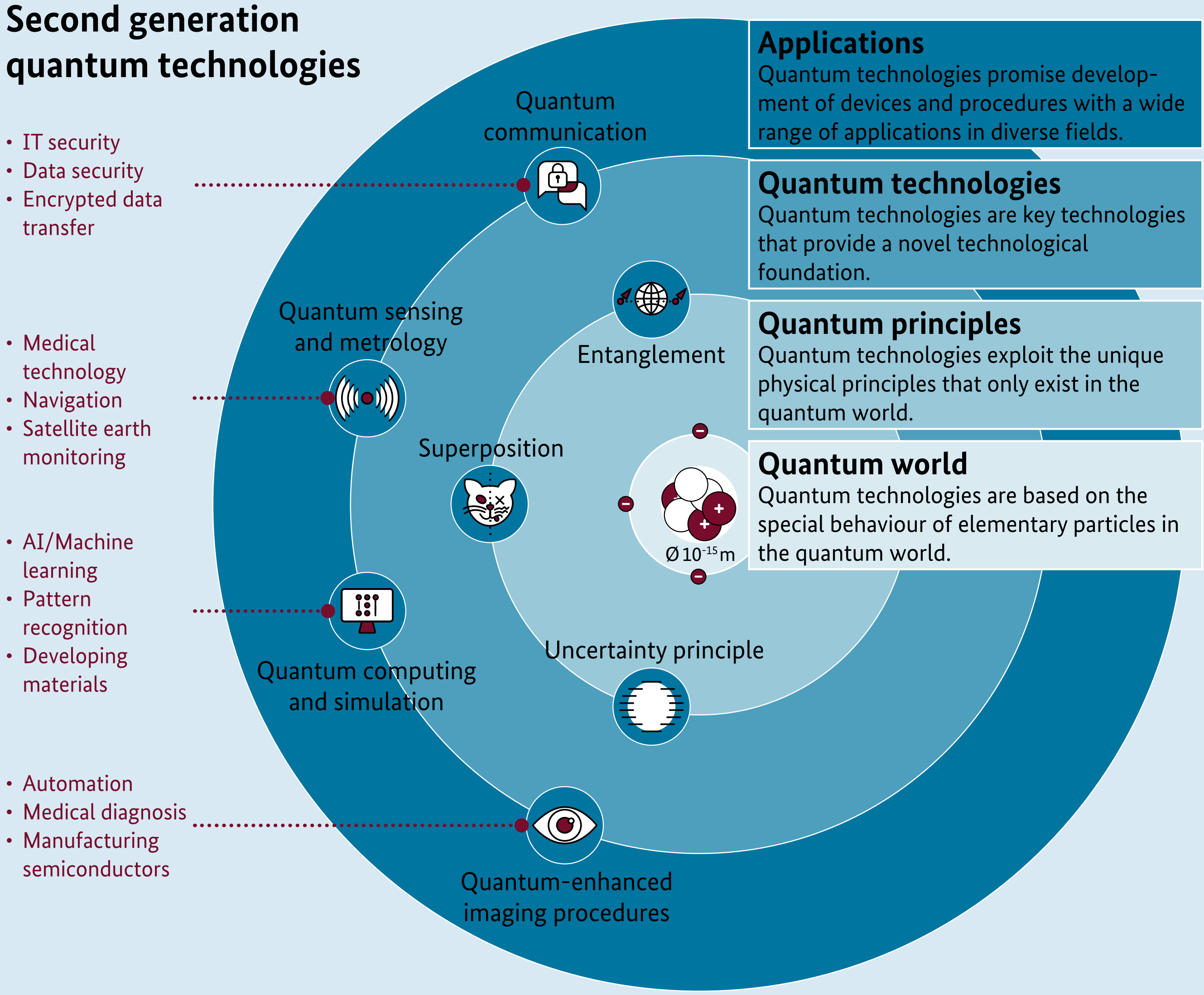
1.1 Quantum technologies – the next revolution

We explore and control our modern world using highly sophisticated digital instruments – cameras, computers, sensors. Digital technologies are a fundamental part of our lives and work.

In reality, though, our world is not made up from ones and zeros: it is composed of quanta. This was first understood by Max Planck and Albert Einstein in the early twentieth century. The carriers of physical interactions cannot be divided into arbitrarily small units; rather, they have a physical "minimum size" – the quantum. Our world is therefore a quantum world, where the rules of quantum mechanics apply at the atomic and subatomic level – strange rules, which sometimes seem counterintuitive to us.

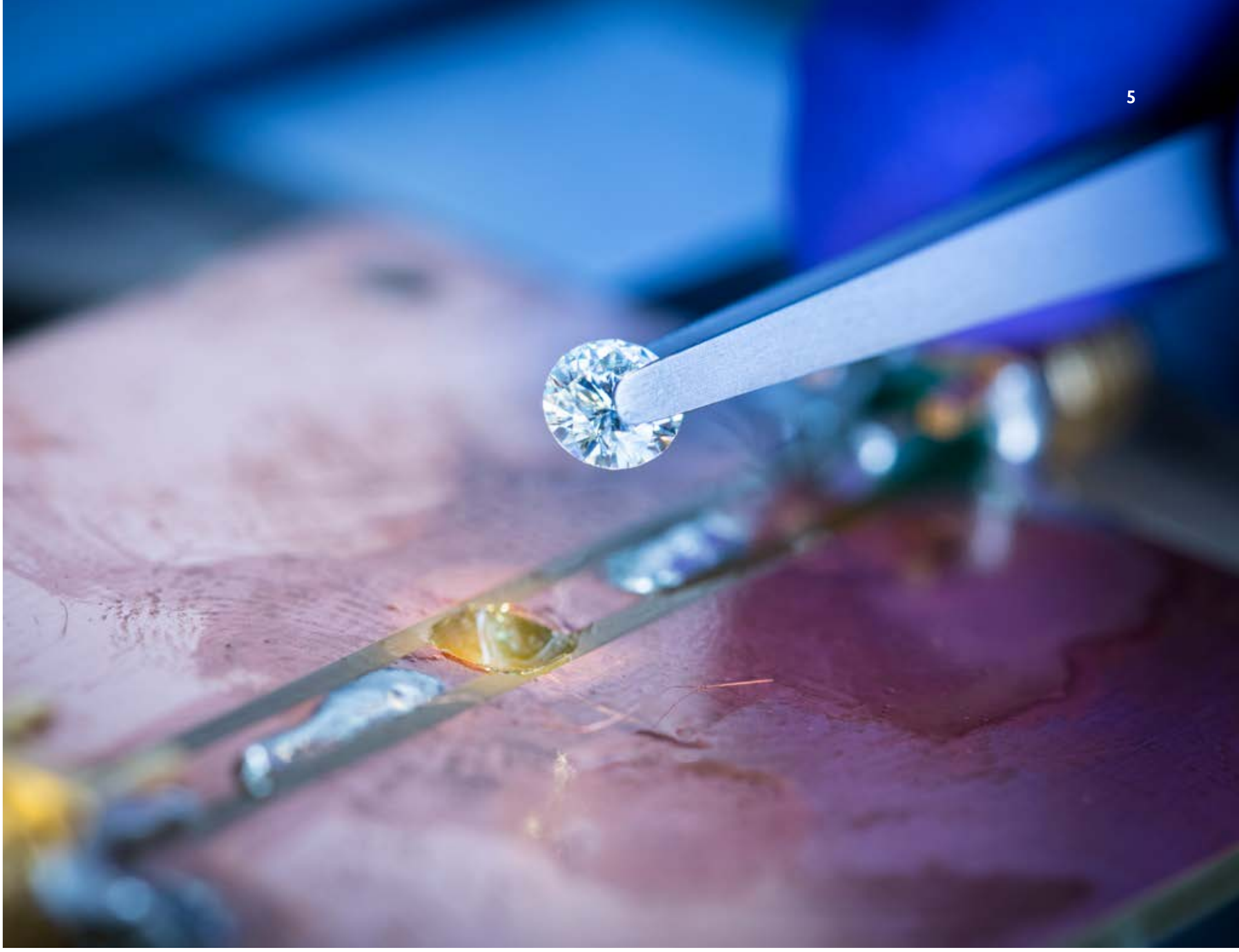
If our world is a quantum world, it follows that we must be able to use quantum systems to help us to understand our world better and organise it more efficiently. This is what quantum technologies are about. What if, in future, we could configure our world on a completely new technological basis, using tools and procedures currently unknown to us – tools and procedures that work based on the rules of quantum mechanics? Might we discover relations that are currently hidden from us? Could we achieve tasks that currently defeat us – for example, because they require too much time and computing power with our current approaches? How could we exploit these new technologies to bring real benefits to our daily life?

Second generation quantum technologies



The speed of an internet connection depends on, among other things, the accuracy of the clock pulses synchronising the network. The best clocks in the world today are so precise that their average deviation amounts to just one second in the age of the universe. Quantum technology could be used to construct this kind of extremely high accuracy clock easily and robustly, so that their use would not be restricted to a small number of measurement laboratories: they could be used to “clock” our communication networks. These new networks would have much higher speeds, making good internet connections more cheaply available. The same would apply for navigation systems: sufficiently accurate clock pulses would increase precision enough that we could, say, steer construction machinery around the construction site. These are just two ways that quantum technologies could transform our working day.

> Our world is a quantum world. The carriers of physical interactions cannot be divided into arbitrarily small units; rather, they have a physical “minimum size” – the quantum. It is the rules of quantum mechanics that apply at the atomic and subatomic level – strange rules, which sometimes seem counterintuitive to us. However, they have major implications for many areas of our lives.



We currently need large-scale equipment to measure magnetic fields accurately – magnetoencephalography equipment (MEG) in hospitals is an example of this. Diamond quantum sensors may make it possible to create miniature MEG devices that could be used for mobile applications, such as controlling equipment to help disabled people during their daily life.

Some classes of problem still cannot be solved satisfactorily using current techniques. For example, analysing financial markets, or optimising journeys and traffic systems. Scientists are investigating whether this type of problem could be solved by creating simulations in special quantum systems. These simulations could be used to help to predict financial crises, or for more efficient traffic control. It might also be possible to develop quantum computers that could be used to run special quantum software. Traditional computers are bound to digital computing programs, which means that some computations would require infinite amounts of time or huge energy resources, or simply cannot be carried out at all. A typical example is the factorisation of large numbers into prime numbers, which is a key element of data encryption. Another example is searching through very large datasets.

The characteristics of quantum systems can be exploited to create innovative applications. For example, artificial diamonds can be used to create very good quantum states for high sensitivity measurement of magnetic fields. These precise measuring instruments – for example, for measuring brain waves – currently only available in hospitals, could be developed and made available in pocket-sized form for personal use.

1.2 What is the status of quantum technology today?

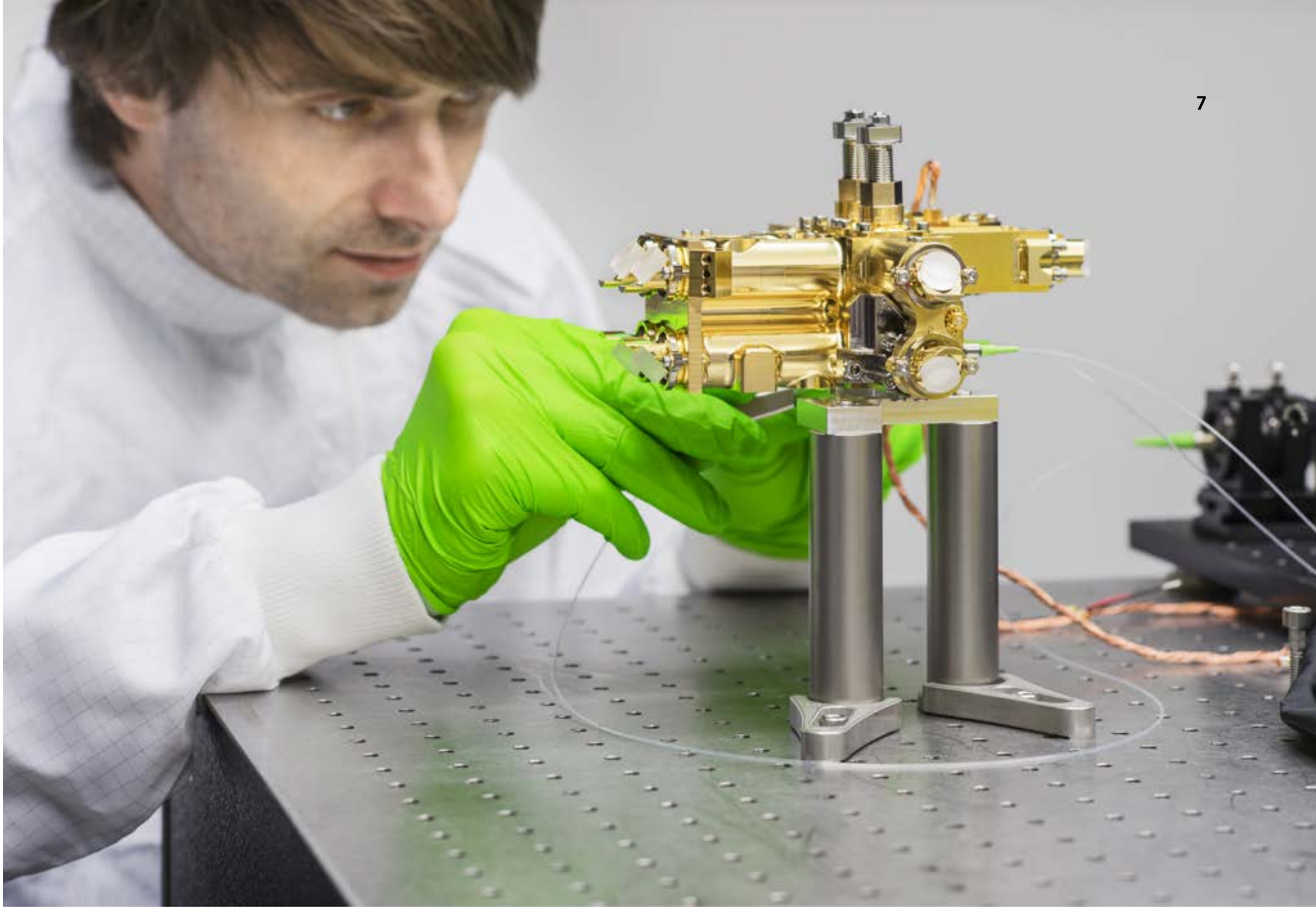
Nearly all of us already use quantum technologies daily: computers, data networks and the majority of medical imaging techniques could not have been achieved without quantum effects. This is because components such as transistors, diodes and lasers all make use of principles of quantum physics. Germany has enjoyed considerable success with these "first-generation quantum technologies", both scientifically and economically.

The laser is an excellent example of this. Starting from a purely scientific phenomenon, institutes and enterprises have developed a device that is used today in research, for manufacturing machinery and vehicles, 3D printing, measurement technology, in communications and all kinds of everyday devices. Many high-performance laser sources and machines are manufactured in Germany.

We are now moving beyond just making indirect use of quantum effects and working on directly controlling them. It is a defined goal of the Federal Government that German institutes and companies will be a part of shaping this transformation and pioneering the "second quantum revolution". Examples of how "second-generation quantum technologies" could be used include creating measuring devices with much higher precision, vastly enhanced data communication security, and building higher-performance satellites and computers. The possibilities in these technologies are so great that they could have major effects on our economy and society, as well as being extremely relevant to security policy. The international race to turn these technologies into industrial reality has already begun, with activities underway in all the leading countries. A few examples:

- In China, quantum technologies are of great interest politically, and consequently benefit from strong political support and are very well financed. The launch of the world's first satellite for quantum key distribution (QKD) in 2016 is an example that has drawn a lot of attention.
- In the USA, institutes and enterprises are currently investing considerable resources into driving forward the development of quantum computers. These activities are partly shaped by economic goals, but also to a large extent by military strategic considerations.
- Japan, Singapore and Canada all set up their own programs some years ago for quantum technology research and space applications.
- The United Kingdom's "UK National Quantum Technologies Programme"[1] supports research, academic training and industrial innovations in quantum technologies.
- In 2016, the European Commission announced a "FET Flagship" project based on the "Quantum Manifesto"[2] drawn up by European scientists. The Quantum Flagship for quantum technologies has four pillars: quantum communication, quantum sensing, quantum computers and quantum simulators. A German-led high level steering committee was established to develop concrete proposals for the project implementation. Its final report was published at the end of 2017.[3]

1 http://uknqt.epsrc.ac.uk/
2 Quantum Manifesto: A New Era of Technology, May 2016; http://www.qutega.de/links/
3 Quantum Technologies Flagship Final Report; http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=34809&no=1



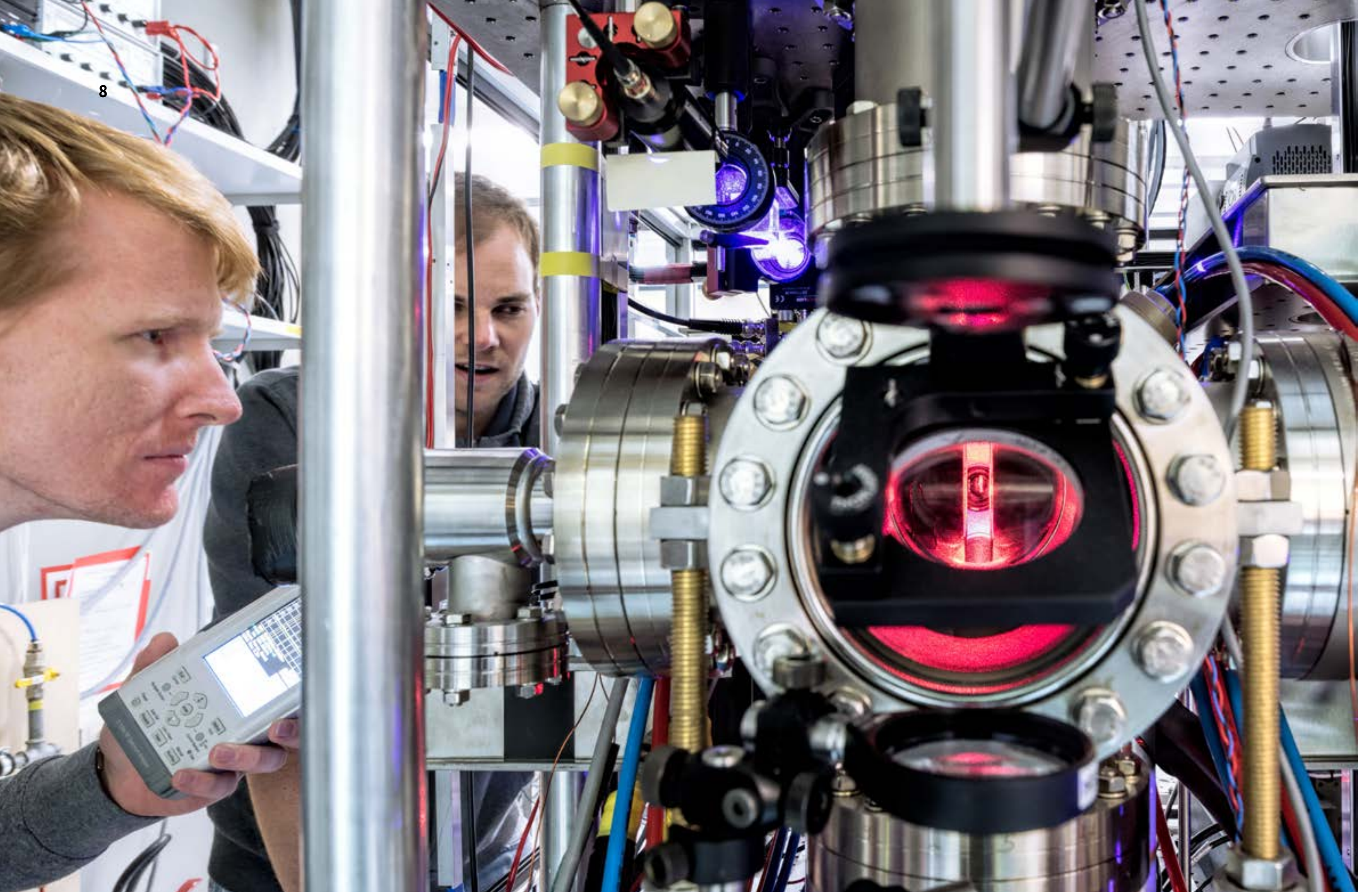
The possibilities of quantum technologies are so great that they could have major effects on our economy and society, and are furthermore extremely relevant to security policy. The image shows one example: a single photon source for inherently secure data transmission. The international race to turn these technologies into industrial reality has already begun.

Germany and the EU have a good basis for developing quantum technologies: Europe is an international leader in quantum physics, boasting around 50% of all scientific publications and almost 40% of the researchers in this field[4], while Germany itself can claim a strong expertise in quantum physics, putting it in an excellent position to become an early leader in transferring the second-generation quantum technologies into applications and helping to shape their international development. Germany's current position is partly the result of the common research and scientific policy of the Federal Government and states, supported by R&D funding organisations, non-university research organisations and departmental research institutes. These organisations and institutes – the German Research Foundation, the Max Planck Society, the Helmholtz Association, the Fraunhofer Society and the Leibniz Association – have been working for many years on basic science, laying the foundations for technical exploitation of quantum physical effects and systems. Their work applies to both the national sphere and for international scientific collaboration. The departmental research institutes provide particular support for research in fields where public functions are affected. The appendix to this document gives details of the fields of activity associated with each of the R&D funding organisations, non-university research organisations and departmental research institutes. German research and industry is also well-positioned in terms of other key technologies needed for building quantum applications, such as microelectronics, nanotechnology and superconductors. Germany's excellent research and technology infrastructure, with its close links to large, medium-sized and small enterprises, represents a strong competitive advantage.

The Federal Government will provide political support and guidance for the transition from science-led quantum physics research to novel applications based on quantum technologies. The Federal Government's goals for the current federal programme are:

- To build on Germany's strong position in quantum physics research and pave the way towards applications using quantum technologies

4 According to a study carried out on behalf of the European Commission, 2,455 authors for quantum physics publications in the period 2013-2015 came from the EU, while there were 1,913 from China and 1,564 from North America. Quantum Technologies Flagship Final Report, p. 3; Source: see footnote 3



- To establish the framework conditions to prepare for new economic opportunities and markets
- To build a solid basis for a leading role in industrial use of quantum technologies
- To work with our international partners to ensure the security and autonomy of Germany and Europe in this important future field
- To inform the population of Germany and involve them in the journey towards a new key technology

The federal programme outlines the starting situation and lists goals and specific initiatives up to 2022. These include on the one hand building up the German research institutes, improving links with enterprises and developing new technologies for government functions, and on the other hand, informing and involving the public in issues relating to quantum technology. The Federal Government will ensure that more people can understand the potential of quantum technology, discuss the issues, and make decisions about what these possibilities mean for them – in terms of education, the workplace, and their own goals.

The Federal Government has allocated a total of 650 million euros during this legislative period for research on quantum technologies. It will be continually tracking developments in this area, reviewing its initiatives and adapting them accordingly.

Germany has a strong position in quantum technologies, with significant expertise available in the research community, particularly in the field of quantum physics. German research and industry also has an internationally competitive position in terms of key enabling technologies (microelectronics, nanotechnology and superconductors) for building quantum technological applications.

2 Research focuses in Germany

The Federal Government began preparations for the programme with a comprehensive agenda process involving industry and research institutions. The process documented the current research status, identified tasks for research and development (R&D), and assessed potential applications. The results are presented through expert papers from the two spheres, science[5] and industry[6]. The following fields of development were identified for quantum technologies:

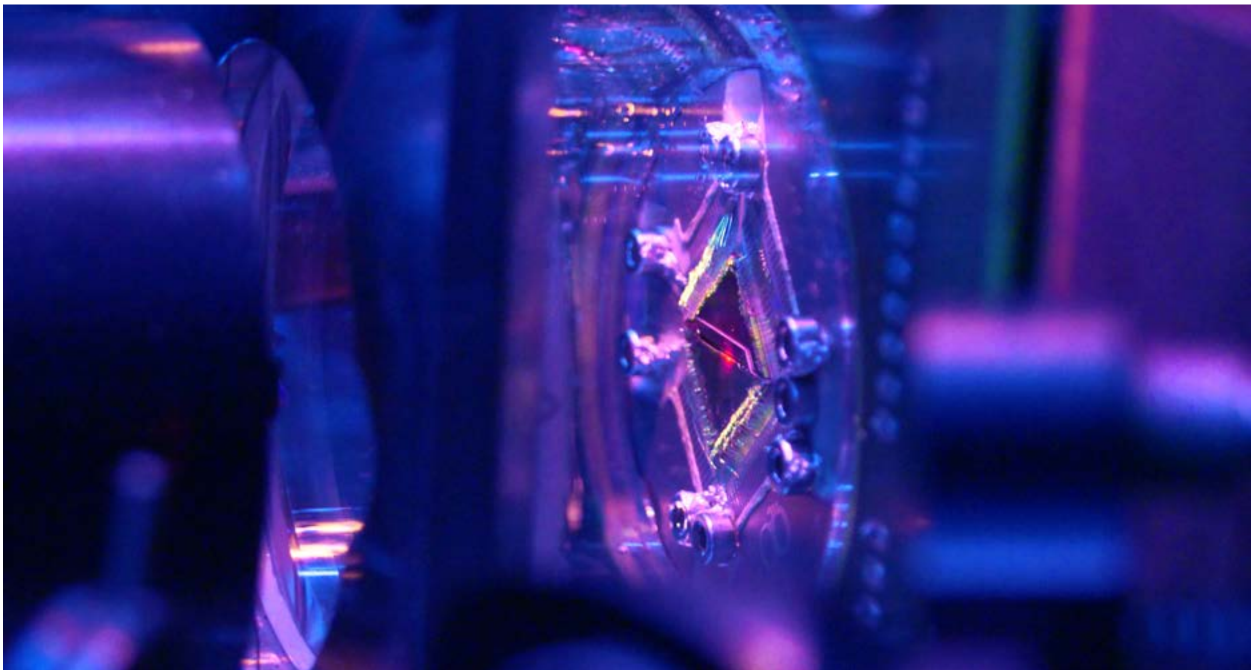
2.1 Quantum computers

Quantum computers are based on completely different principles from traditional digital computers. Unlike digital computer bits, the smallest calculating units in a quantum computer, called quantum bits or “qubits”, are able to interact with each other based on special laws of quantum mechanics, and consequently assume a significantly more complex overall state. We refer to this phenomenon as “entanglement”. This interaction between qubits to form an entangled state is a unique characteristic of quantum computers. Lots of tasks that cannot be solved satisfactorily using digital computers have a large number of mutually interacting conditions, which must be included in a complex calculation. Examples include performing rapid searches through vast quantities of data, or optimising large logistical systems such as traffic networks or timetables. If we can manage to configure the quantum entanglement states in a quantum computer so that they correspond to one of these tasks, the quantum computer could then solve the task much more quickly than a traditional digital computer can. In additional to universally programmable computers, quantum simulators could also be used for practice-relevant quantum phenomena, for example in the fields of chemistry or pharmacy. Although they are less flexible than the universal computer, and only suitable for certain classes of problem, these simulators could deliver benefits for specific applications considerably sooner.

There are incredible challenges associated with building quantum computers and simulators. The quantum phenomenon of qubit entanglement is extremely

5 Concept paper from the National Initiative for Quantum Technologies – Fundamentals to Applications (QUTEGA) http://www.qutega.de/en/home/
6 Supporting quantum technologies – German industry position paper http://www.photonikforschung.de/media/quantentechnologien/pdf/Quantentechnologie_bf.pdf

The quantum computer can be seen as the most far-reaching innovation quantum technology has to offer. The unique operating principles of quantum computers mean they have the potential to solve tasks that traditional computers cannot approach efficiently enough. There are various ways that the necessary “quantum bits” could be realised. For example, the picture shows a solution using individual atoms in particle traps.



sensitive to environmental influences, meaning that these entangled states usually collapse very quickly. The implementation of the typical example application of breaking modern public key cryptography processes would require quantum computers with many thousands of qubits. The immediate focus is therefore on initial applications that could be processed using just a few hundred qubits.

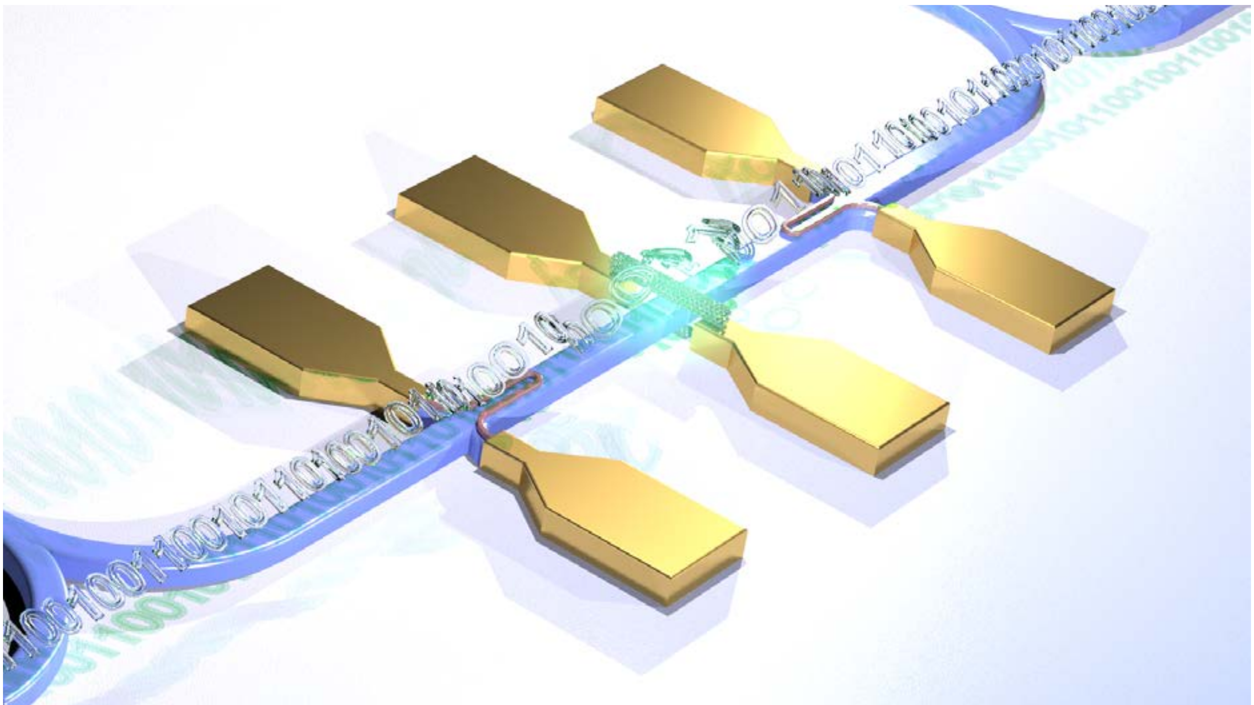
The journey towards realising quantum computers also involves designing special algorithms – this is just as important as developing the hardware. There is no need for quantum computers to actually exist for quantum algorithms to be researched, as the algorithms can be simulated, at least to a certain extent (and up to a certain size), with conventional digital computers. In fact, there is another reason simulations are important: very different hardware platforms and architectures for quantum computers are currently still being discussed, and it is necessary to analyse and compare their advantages or disadvantages for quantum algorithms using traditional computers.

2.2 Quantum communication

Quantum communication uses entangled quantum states for key exchange in data transfer. Entangled quantum objects, e.g. photons, are sent to two physically distant locations. By measuring specific characteristics of the two photons at the two different locations, it is possible to determine whether one of the two photons has been already been measured. If so, the connection has been intercepted. The reason we know this is that unknown quantum states cannot be copied or measured without disrupting them. Disruptions to quantum states are inescapably detected as transmission errors, exposing the eavesdropping attack.

In practical communications, this technology is used for exchanging keys. With quantum cryptography or quantum key distribution (QKD), a key is generated for some secret information based on individual quantum states. This means that security is now based on a physical law of nature, rather than the mathematical assumptions that apply to the cryptographic processes currently in common use. In other words, it has now become possible to establish communication links whose security is founded on physics, not just on

Quantum communication is about exchanging quantum states – between very short distances on a single chip, as shown in the image, or across longer distances along communication routes extending over hundreds of kilometres. It differs from communication using traditional cryptographic processes in that the transmitted data is secured based on a physical law of nature, rather than a mathematical principle.



mathematical calculations. However, there are considerable technical challenges associated with transmission, as quantum states are very fragile.

QKD devices have been commercially available for specific niche markets for some time. Typical customers at present are banks or governments. The vast majority of approaches to quantum key exchange are based on exchanging photons via optical fibres. However, with the current state of the art, it is only possible to create applications based on point-to-point connections over distances of less than 100 kilometres. Free space laser communication represents a way of overcoming the problems of disruptive atmospheric influences, and significant progress has already been made in this area in tests in real conditions.[7] Laser-based communication technologies using quantum cryptography were successfully tested with a flying object under atmospheric conditions back in 2015.[8] There are still a number of open technological questions about implementation over significantly larger distances and building concrete applications, as the weak light signals from quantum communication cannot be processed using normal amplifiers. However, integrating space-based quantum key distribution may prove useful when developing intercontinental links.

As soon as the first quantum computer exists, there will be massive repercussions for data security. These won't be limited to the communication relationships active at the time, as decrypting recorded communications from earlier dates will also become possible. When we consider that cryptographic security is frequently configured with a long lifetime – as on satellites, for example – it becomes clear that we need to be working **now** on encryption processes that are secure against attacks from quantum computers. Approaches to "post-quantum cryptography" are currently being explored in parallel with quantum communications research.[9]

7 https://www.dlr.de/dlr/desktopdefault.aspx/tabid-10081/151_read-19914/#/gallery/24870

8 https://www.dlr.de/dlr/desktopdefault.aspx/tabid-10122/333_read-15527/year-2015/#/gallery/20972

9 As part of the research framework programme for IT security, "Autonomous and secure in the digital world", the BMBF addresses post-quantum cryptography as a research area;https://www.bmbf.de/de/sicher-in-der-digitalen-welt-849.html

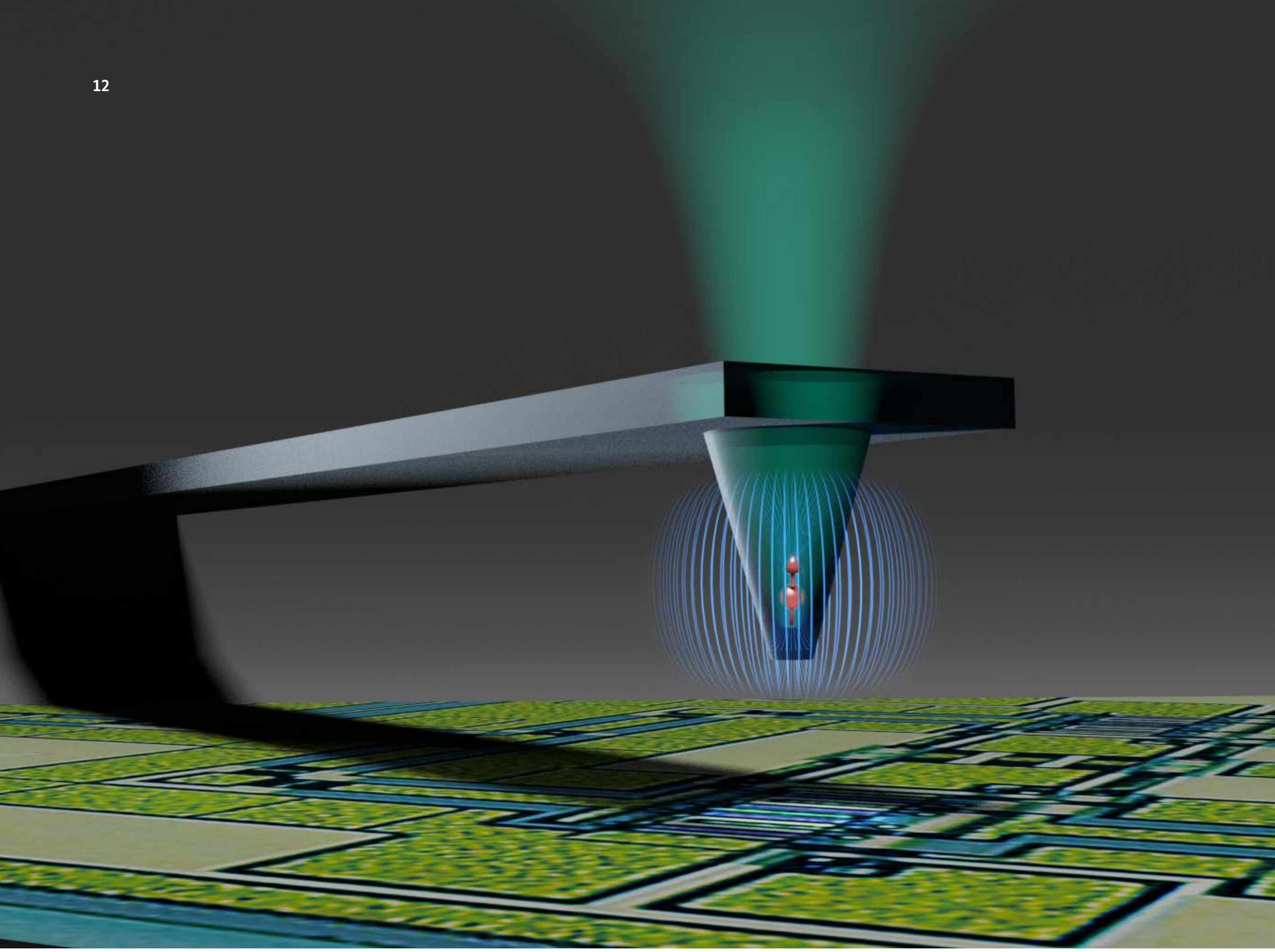
2.3 Quantum-based measurement technology

While the fragility of quantum states and systems presents enormous challenges to developing workable quantum computers and quantum communications technology, it is exactly this fragility that harbours enormous possibilities for measurement technology – fragility to environmental influences is nothing other than high measurement sensitivity. Carefully constructed quantum systems could be used for extremely high accuracy measurements of physical values such as pressure, temperature, position, time, velocity, acceleration, electrical and magnetic fields or gravity.

Atomic clocks based on atomic quantum states have already been in use for decades as time references for precision measurements, for example as part of the European Galileo navigation system, or the global positioning system (GPS) for navigation. Quantum gravimeters based on cold atom interferometry are able to detect even the tiniest variations in the earth's gravitational field, caused by different material compositions in the earth's crust. One possible use of such ultra-precise gravimeters is the discovery of natural resources. Miniaturisation and significant cost reductions may be on the horizon thanks to new quantum sensors, which can assume and maintain their quantum state even at room temperature.

Another application area for quantum phenomena is optical imaging (quantum enhanced imaging): quantum mechanical processes could be used to obtain considerably higher optical resolutions than can be achieved with traditional processes, for example. Quantum lithography exploits the same principle to generate tiny structures.

The economic potential for quantum-based measuring technology is currently thought to lie in defence technology, industrial precision measurement, medical diagnosis, earth monitoring, geology and discovery of mineral depositions, and navigation (especially satellite navigation for air, sea, rail and road transport in conjunction with e.g. automated driving or GPS/Galileo-based apps).



In the long term, we can expect that as quantum-based measurement technology becomes smaller and increasingly integrated, it will come to be involved in a large number of challenging applications for other professional fields and for consumers.

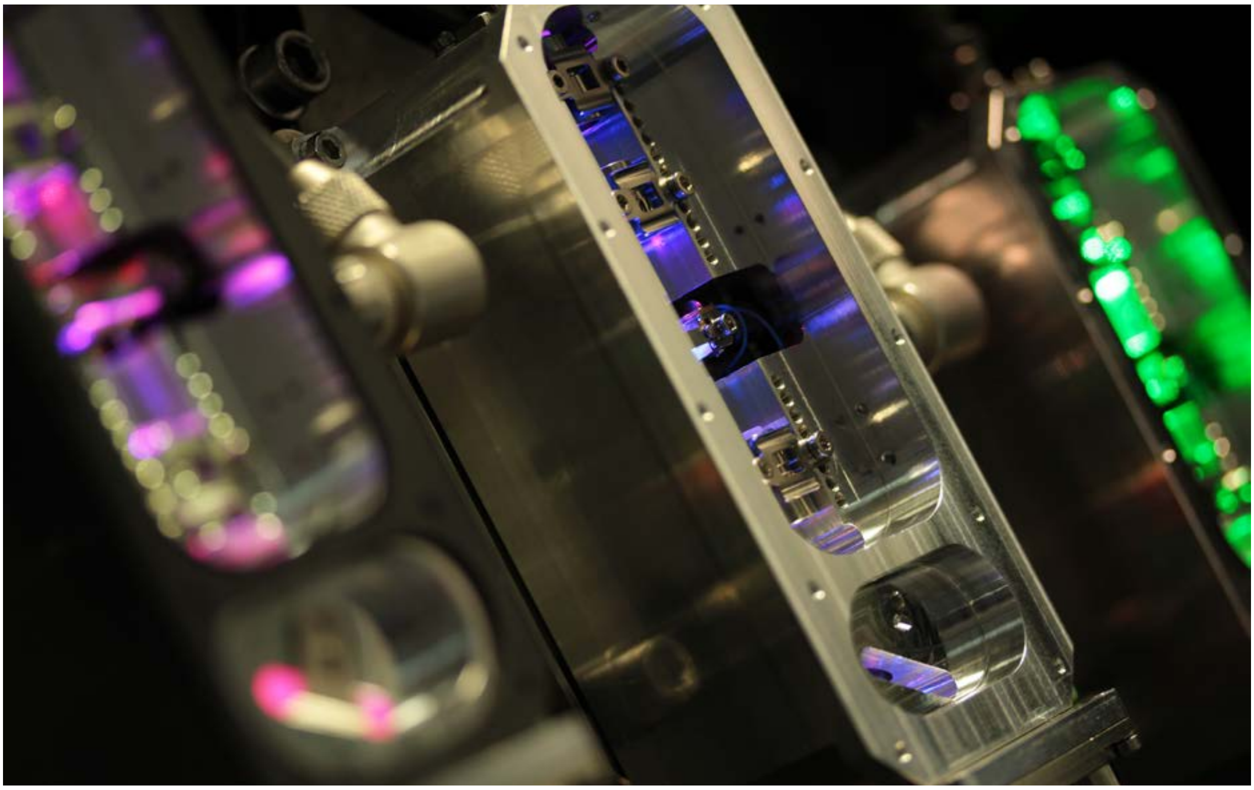
Carefully constructed quantum systems could measure physical values such as pressure, temperature, position, time, velocity, acceleration, electrical and magnetic fields or gravity– with a precision that to date has been inconceivable. This is achieved by exploiting the particular sensitivity of quantum mechanical states. The probe shown in the image uses a diamond sensor to measure the magnetic field.

2.4 Enabling technologies for quantum systems

Quantum computers, quantum communications and quantum-based measurement technology have a significant technical and economic potential, although not fully mature. An interesting high-technology market has in fact already developed as a result of significant investments in relevant research laboratories and projects.

Around 100 to 150 million euros are currently invested annually in Germany for laboratory equipment in the quantum technology field.[10] The country has seen a number of small and medium-sized enterprises emerge in recent years, primarily from ongoing basic research in universities, focusing on this specialised international market and mostly offering highly specialised small-scale production. With this Framework Programme, the rapid growth in international research

10 Supporting quantum technologies – German industry position paper, pp. 5, 7, 17; Source: see footnote 6



An important step towards putting quantum technologies to practical use is the transition from laboratory setups to robust and reliable equipment. The laser module shown in the image replaces a number of individual optical components. Before we are able to create robust and reliable technical systems (small, efficient and compact) on an industrial scale, it is essential that we can master the complexity of a quantum measurement or a quantum computer.

applications in the field of quantum technologies, and the anticipated use of quantum technologies in satellites, we can expect to see the demand for suitable devices and systems growing considerably over the coming years.

A key element of this will be the transition from laboratory-built devices to robust, reliable and cost-effective manufacturing. The first steps along this route are already on the horizon. Alongside quantum technologies, the technical systems will require industrial engineering solutions, as they have to become smaller, more efficient, more compact, and thus more robust and reliable. This field of "enabling technologies" represents a technological backbone for research on and development of individual quantum technologies. We can also assume that – as for other technology markets that have emerged in the past – this will be the area where the first standards and norms for quantum technologies begin to emerge.

It is clear from the above description of current developments in various areas of quantum technology that breakthroughs in quantum technologies could have significant repercussions for many areas of our lives, just as satellite technologies did in the late nineteen-sixties or digitalisation in the nineteen-nineties. Developing quantum technologies is therefore important to research, economics and security policy.

3 Initiatives of the Federal Government

The Federal Ministry of Education and Research (BMBF), the Federal Ministry for Economic Affairs and Energy (BMWi), the Federal Ministry of the Interior, Building and Community (BMI) and the Federal Ministry of Defence (BMVg) all contribute to the development of quantum technologies in Germany as part of their respective functions. The Federal Government's Framework Programme brings these contributions together into an integrated strategy. The strategy development and individual initiatives are coordinated through regular departmental circuits at ministerial level. At the same time, the programme will seek to dovetail with the BMWi's transfer initiative, which aims to support technology transfer using established and novel tools.

3.1 Developing the quantum technology research landscape

Germany has an excellent starting point for basic research in the field of quantum physics. A wide range of research in this area – undertaken by a combination of federally-structured universities, non-university research organisations, departmental research institutes, and market-based research undertaken by enterprises – forms an excellent basis for quantum technologies. In the appendix to this document, R&D funding organisations, non-university research organisations and departmental research institutes provide details about their current research work and strategies for quantum technologies.

In order to develop quantum technologies further and establish the necessary structural conditions, experts from science and industry have defined the following need for action:

> "Research on quantum technologies is taking place on an internationally visible level at many different sites across Germany. This geographic diversity can certainly be considered to be a strength of the German research landscape. [...] At the same time, however, there is sometimes a significant deficit in coordination: synergistic effects are often not sufficiently exploited. We should be working towards structural improvements in order to establish cross linkages and pools of competence."[11]

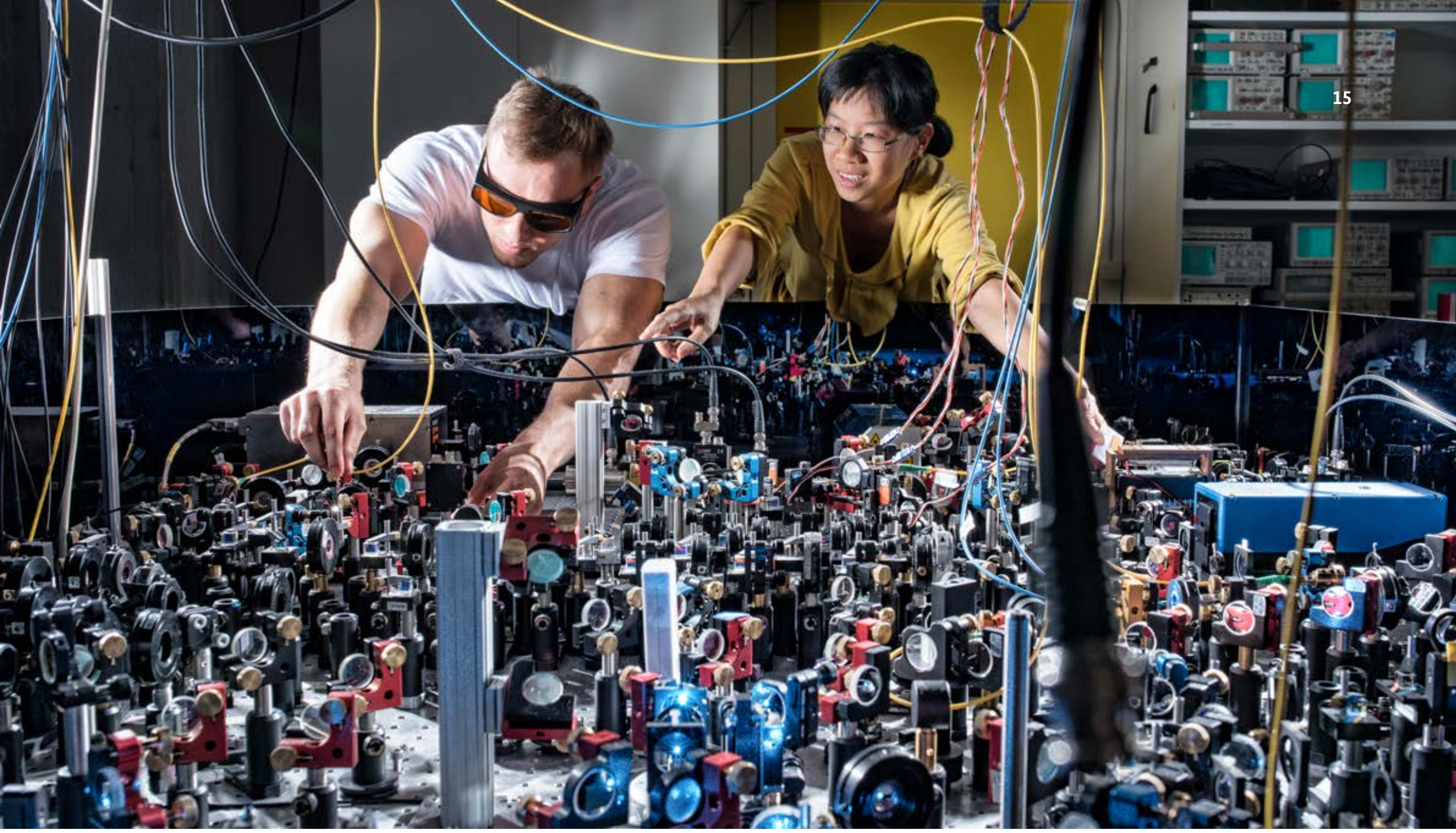
What this means is: larger, international research capacities, with a stronger focus on applications, are required in Germany. The legal framework of the German constitution, which combines principles of scientific freedom and the federal system, stipulates that the necessary decisions must take place in a competitive context and based on expert criteria.

The Federal Government will commission the relevant non-university research organisations and departmental research institutes to develop, on its behalf, proposals for restructuring with the aim of emphasising more applied quantum technology research. The goal for research with core public funding is to increase support for collaborative R&D projects researching topics in quantum physics with particular relevance for applications. There will therefore be a focus on projects that have above-average prospects for technical applications, especially when the step from research to application is being taken for the first time. This must go far beyond the basic demonstration of technical feasibility. The research projects should therefore include concrete applications and involve the users from an early stage, e.g. in collaborative R&D projects between science and industry, or involving public users. It is also important to establish the legal conditions (patent rights, etc.) for any potential commercial or industrial exploitations. The current set of research topics for new quantum technologies[12] must not be considered as an exhaustive list, but as a continuously growing one.

Key indicators for the crucial structural decisions that the non-university research organisations and their institutes will have to make over the coming years will include research successes and the acquisition of third-party funds, alongside competitive criteria such as recruiting qualified young researchers, international collaborations, collaborations with enterprises, or spin-offs. Regardless of these structural developments

11 (Translated from) Concept paper from the National Initiative for Quantum Technologies – Fundamentals to Applications (QUTEGA), p. 35; Source: see footnote 5

12 See Section 2 of this document



Germany's research landscape for basic research on quantum technologies has a highly prominent international position. It is important now to shift the focus to applications and marketing. This means establishing links between the basic research being done within academia and industrial research, so that results that are ripe for transfer to applications do not stagnate at the laboratory stage. The research community must continue its structured evolution while remaining open to unanticipated scientific developments.

in a competitive framework, the departmental research institutes will continue to carry out their specific research tasks as part of their departmental mandates.

3.2 Creating research networks for new applications

Quantum technologies are, of course, very much the domain of scientific research. Nonetheless, there may be direct transitions from basic research to industrial applications, for example in the field of high-precision determination of place and time. Due to the high industrial relevance of these applications, the Federal Government will promote application-oriented research covering all stages, right through to engineering issues. The Federal Government wants to play its part in increasing backing for scientific approaches to quantum technology research with entrepreneurial strategies. It is establishing various initiatives to aid this process:

Research portal for quantum technologies

Growing numbers of enterprises in a variety of sectors are taking an interest in quantum technology. They are gathering targeted information on the subject and evaluating it in terms of their own strategies and opportunities. In addition, the industrial world is already starting to take an interest in quantum applications. Meanwhile, the German scientific community has the competence to systematically test and compare various quantum technology approaches, products and procedures based on the current state of the art in international research; from these results, it is able to offer neutral consulting services to interested enterprises. This ability must be opened up so that it is visible and accessible to industry. This is partly about the accumulated scientific expertise, but also means building targeted knowledge about specific application issues for individual industries.

The Federal Government will contribute here by commissioning an overview ("Who's who") of the German scientific world of quantum technology, which will be published on the online portal, where it can be used to search for contacts and establish initial contact. Once partners have made contact via the search, they can communicate privately to agree on the specific consulting services.

Enterprise-led collaborative R&D projects in potential application fields

The fields of metrology and communication combine with various key technologies to form a basis for quantum applications; these fields are already very well represented in Germany. The Federal Government will continue to drive these areas forward; the first applications in these fields could appear in the relatively short term.

Since 2011, the BMBF has been supporting a wide range of collaborative R&D projects in the field of quantum communication.[13] Altogether, collaborative projects covering more than 70 subprojects in this field have been approved by the BMBF. In 2017, it was possible for the first time to include a possible application scenario involving enterprise participation in the call for proposals[14]. The scenario envisaged the development of systems that could be used to exchange information securely (without eavesdropping) through optical fibres over long distances. The first quantum signal processors, or "quantum repeaters", are now being developed as part of the "Quantum Link Extension" project (Q.Link.X)[15], launched in 2018, with the goal of transmitting quantum signals over more than 100 kilometres via conventional fibre optics.

The BMBF began a new funding phase in 2017 with three pilot projects and three further calls for proposals. These are collaborative projects between science and industry in the fields of quantum metrology & communication and key technologies:

- Pilot project "BrainQSens"[16]: through this collaborative project with industrial participation, launched in 2017, the BMBF has been funding the development of a prototype diamond-based quantum sensor. The sensor will be able to measure neuronal magnetic fields very precisely – similar to the way a MEG works, but much more compact and precise.

The opportunities that quantum technologies can offer German industry must be exploited quickly and effectively. To this end, initiatives have therefore been launched in close collaboration with science and industry, which aim to avoid the limitations of restricted viewpoints. For example, the "BrainQSens" pilot project, in which simplified high-sensitivity magnetic sensors facilitate improved medical diagnostics in brain research. In the long term, this will also provide new, simpler ways to control prostheses and even technical devices as part of daily life.

13 E.g. the Q.com collaborative project: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/q.com

14 https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/quantenkommunikation

15 https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/q-link.x

16 https://www.photonikforschung.de/projekte/quantentechnologien/projekt/brainqsens.html

- Pilot project "Opticlock"[17]: as part of the pilot project "Optical single ion clocks for users", the National Metrology Institute of Germany (Physikalisch-Technische Bundesanstalt) has been working together with industrial enterprises since 2017 to research and develop a demonstrator for a compact, robust optical clock that can be used to synchronise large communication networks.
- Pilot project "QUBE"[18]: the collaborative project "Quantum key distribution with Cube Sat" (QUBE), launched in 2017, is developing hardware for a tap-proof global communication system, using QKD technology integrated into a highly compact, cost-effective satellite platform known as a CubeSat.
- Call for proposals "QuantERA Call 2017"[19]: the ERA-NET cofund initiative "QuantERA" supports collaborative, application-oriented European research on all fundamental quantum technology topics. As the biggest consortium partner, the BMBF provides support to German researchers in 18 of the 26 European projects.
- Call for proposals "Key Components for Quantum Technologies"[20]: quantum effects are sensitive and the devices making practical use of them are generally still large and expensive. The BMBF initiative "Key Components for Quantum Technologies" funds a number of consortia with industrial participation, in order to strengthen existing competences in device development. This is expected to establish a stronger basis for efficient research on quantum technologies and accelerate the exploitation of quantum effects.
- Call for proposals "Quantum Futur"[21]: since 2018, the BMBF has been ensuring the future of quantum technology research & development in Germany by supporting various junior research groups focusing on applied topics in quantum technologies.

Future calls for proposals are in the preparation stages. Funding collaborative projects not only stimulates exploration into areas of research, it also promotes networking between science and industry. These networks constitute an important foundation for the long-term evolution of technologies into new, commercially significant products. The effects are not limited to enterprises and research issues in the industrial sector; they are also relevant to issues originating from other sectors – finance, for example.

Centre of Excellence for Quantum Technologies at the PTB

An important basis for industrial developments will be created with the establishment of a Centre of Excellence for Quantum Technologies at the National Metrology Institute of Germany (Physikalisch-Technische Bundesanstalt, PTB). The PTB combines internationally recognised expertise in quantum metrology and sensing with a statutory mandate to support German industry in the field of measurement. To fulfil this mandate, it must build and operate key infrastructures to meet current needs and provide essential services. One of the key objectives for the Centre of Excellence is to support industry with transferring research results into applications, focusing particularly on start-ups and small & medium-sized enterprises (SMEs). The BMWi is supporting the establishment and development of the Centre of Excellence and considers it to be part of the ongoing work for the transfer initiative. The key specialisms of the centre are:

- Components and technology: development and assembly of e.g. single photon sources and oscillators, or industry-ready clocks, measurement devices and sensors
- Calibration and services: building measuring stations that can define and calibrate the components and technologies listed above, e.g. as a service for SMEs
- User platforms ("user facilities"): making fibre optic networks and technology platforms available for prototype development and small batch production
- Business incubators, training, public relations, support for technology transfer: providing and operating an incubator laboratory for transferring quantum technologies to applications; training centres for engineers

17 https://www.photonikforschung.de/projekte/quantentechnologien/projekt/opticlock.html
18 https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qube
19 https://www.quantera.eu/calls-for-proposals/call-2017
20 https://www.bmbf.de/foerderungen/bekanntmachung-1372.html
21 https://www.bmbf.de/foerderungen/bekanntmachung-1371.html

Lead market initiative in laboratory and equipment technology

As has been the case for other technologies in the past, many applications for quantum technology will probably find their first markets very close to the research environment:

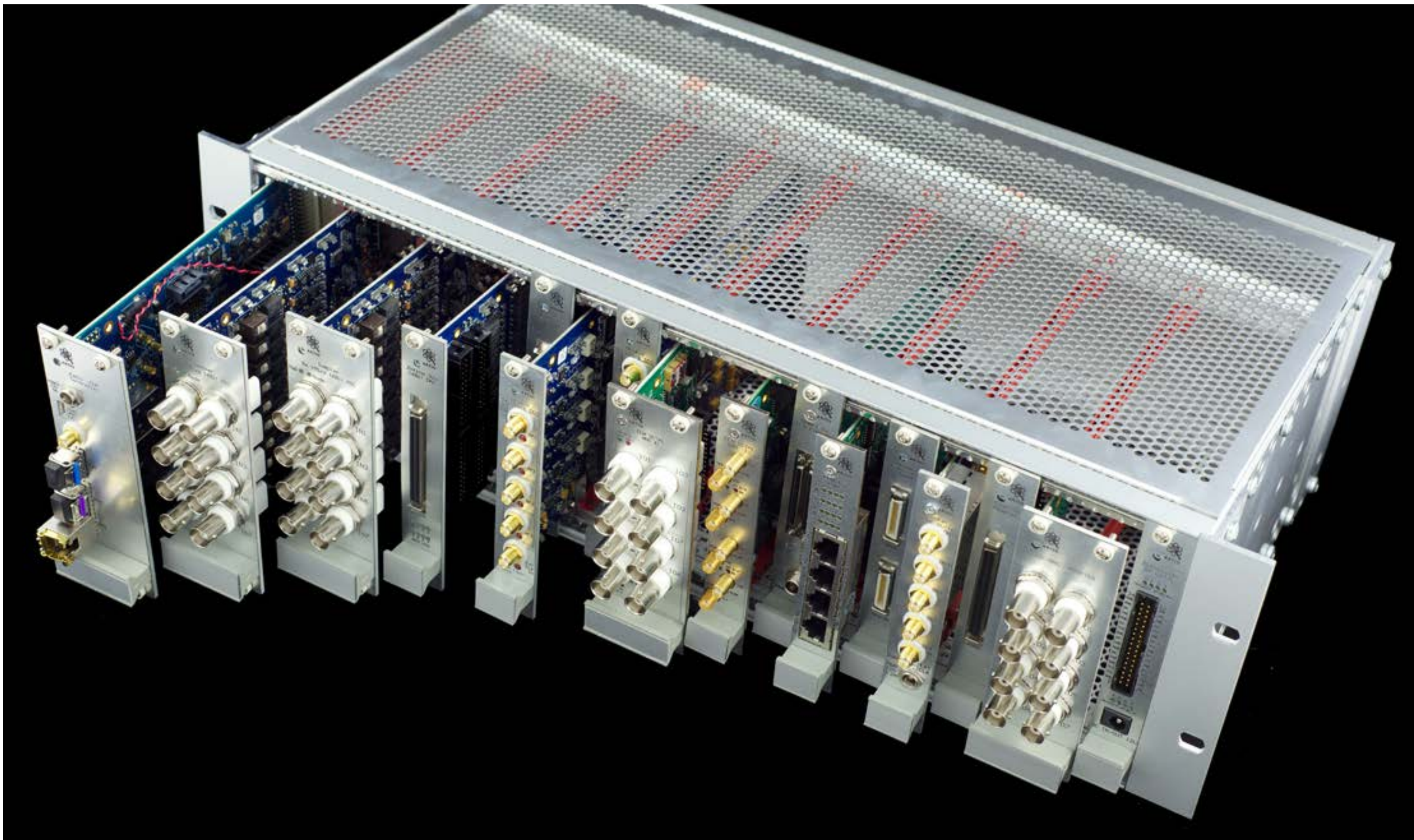
> "The largest known market for quantum technologies is currently public academic research. We can also expect a significant non-public market in the security sector, which we perceive as still being very strong in the research and development arena. There is a demand from both markets for a wide range of "quantum-enabling technologies"; in Germany this demand is largely being met by SMEs. Based on numbers from the United Kingdom, our current estimate is around 30,000 people worldwide and an annual research budget of over 1.5 billion. Germany's share of this is estimated to be around 6 to 10%."[22]

Example applications might include laboratory equipment, laser systems, vacuum or cryogenic equipment, optical components, specialised cameras, detectors with suitable display electronics, radio frequency sources and general measurement technology, integrable control electronics or specialised software.

The research projects and other initiatives listed here could lead to more procurement processes for this type of product. The Federal Government aims to commu-

Hardware for quantum devices can be viewed as a standalone market, since the laboratory equipment for the international research institutes alone represents a substantial market volume. This opens up excellent sales opportunities for German enterprises on the international markets – even for very high-tech products like the control system for an optical single ion clock, pictured. This is helped by the fact that the use of these technologies is not limited to quantum technologies; they can also be used for all kinds of other work in the field of experimental research.

22 (Translated from) Supporting quantum technologies – German industry position paper, p. 4; Source: see footnote 6



nicate and coordinate these developments in order to ensure that the lead markets for quantum technologies that emerge will be accessible to SMEs and spin-off companies or start-ups.

Lead markets also require standards. The Federal Government will therefore give support where necessary for the development of research-oriented standards in R&D funding projects.

Boosting innovation in the quantum technologies sector

The Federal Government supports innovation in business by creating framework conditions that promote innovation, in conjunction with a broad spectrum of funding opportunities: both market-oriented, sector specific programmes and those open to all kinds of technology in all sectors. Various aspects of start-up support, for example, are offered through "EXIST"[23], the "High-Tech Gründerfonds"[24] and the "INVEST – Venture capital grant"[25]. Various venture capital opportunities are available from ERP special funds (European Recovery Programme) for the later growth phases, a time when young enterprises often struggle to get the financial resources to develop their innovations. Grants are allocated jointly with the KfW bank or the European Investment Fund (EIF) and private investors. Example funding programmes for skills development and networking are "go-Inno"[26] and "go-cluster"[27]. Funding initiatives for pre-competitive research and development include "WIPANO"[28], the collaborative industrial research programme (IGF)[29] and "INNO-KOM"[30]. Market-focused research and development is funded as part of the Central Innovation Programme for SMEs (ZIM).[31] Financial support for innovation and digitalisation projects is available through the "ERP Digitalisation and Innovation Credit programme".[32] The National Programme for Space and Innovation[33] funds targeted projects for developing quantum technologies towards future aerospace applications.

This broad, cross-technology and multidisciplinary funding landscape is a key pillar of innovation in Germany. Young enterprises and SMEs can benefit particularly.

If we want to develop applications for quantum technologies, something which is often driven by start-ups and SMEs, it is essential that we keep developing this landscape and make it as effective as possible. The Federal Government will set up appropriate consulting services on innovation. To complement this multidisciplinary funding landscape, there are plans to launch initiatives focused specifically on quantum technology and designed for start-ups and SMEs – for example, by providing suitable infrastructures (see Centre of Excellence for Quantum Technologies at the PTB). The call for proposals "KMU-innovativ": Photonics and Quantum Technologies"[34] is a funding opportunity aimed specifically at SMEs. Proposals are invited twice a year, with the first call going out in July 2018.

Technology transfer from market to applications based on quantum technologies is one of the key interests of the programme. This includes ongoing development of the necessary quality infrastructure and its essential elements (measurement, accreditation, compliance assessment, standards and calibration).

23 https://www.exist.de
24 https://high-tech-gruenderfonds.de
25 https://www.bmwi.de/Redaktion/DE/Dossier/invest.html
26 https://www.innovation-beratung-foerderung.de/INNO/Navigation/DE/go-Inno/go-inno.html
27 http://www.go-cluster.de; https://www.clusterplattform.de
28 https://www.innovation-beratung-foerderung.de/INNO/Navigation/DE/WIPANO/Patentierung-Unternehmen/patentierung-unternehmen.html
29 https://www.aif.de/innovationsfoerderung/igf-industrielle-gemeinschaftsforschung.html
30 https://www.innovation-beratung-foerderung.de/INNO/Navigation/DE/INNO-KOM/inno-kom.html
31 https://www.zim.de
32 https://www.kfw.de/inlandsfoerderung/Unternehmen/Innovation/F%C3%B6rderprodukte/ERP-Digitalisierungs-und-Innovationskredit-(380-390-391)/
33 https://www.bmwi.de/Redaktion/DE/Dossier/luft-und-raumfahrt.html
34 https://www.photonikforschung.de/projekte/kmu-innovativ/foerdermassnahme/kmu-innovativ-photonik-und-qt.html

3.3 Establishing industrial competitiveness through lighthouse projects

There remains a (varying) gap between scientific research results and industrial implementation. In this context, there is a need for German industry (large enterprises, SMEs and start-ups) to evolve from a simple observer and supplier into a strategic force for developments in the field of quantum technology. Experts from German enterprises have proposed[35] that lighthouse projects could help support this process. The projects would be designed to demonstrate to interested parties from the public, politics and enterprises that quantum technologies are not just abstract scientific concepts, they are about new technologies and processes with repercussions and potential for a wide range of economic sectors. The Federal Government is taking up this proposal, and the BMBF will lead two initial lighthouse projects.

35 Supporting quantum technologies – German industry position paper, p. 21; Source: see footnote 6

Quantum communication competition

In quantum communications research, it is currently possible to formulate important objectives in terms of technical parameters. For example, improving the coherence times for quantum memory is a key factor towards an ultimate goal of sustainable secure communication. Parameters of this kind also represent an essential step for secure authentication of system users. At the moment, users are generally authenticated by means of hardware components, security tokens or chip keys. However, powerful quantum comput-

Secure communication protocols represent an important basis of our society's economic system. Research, development and implementation of components and systems with actual usable value is therefore an issue of pressing urgency. Major lighthouse projects, such as satellite-based quantum communication with ground stations (shown in the picture), send a powerful message about the launch of quantum technologies. They have the potential to strengthen competitiveness for system implementations and infrastructure solutions.

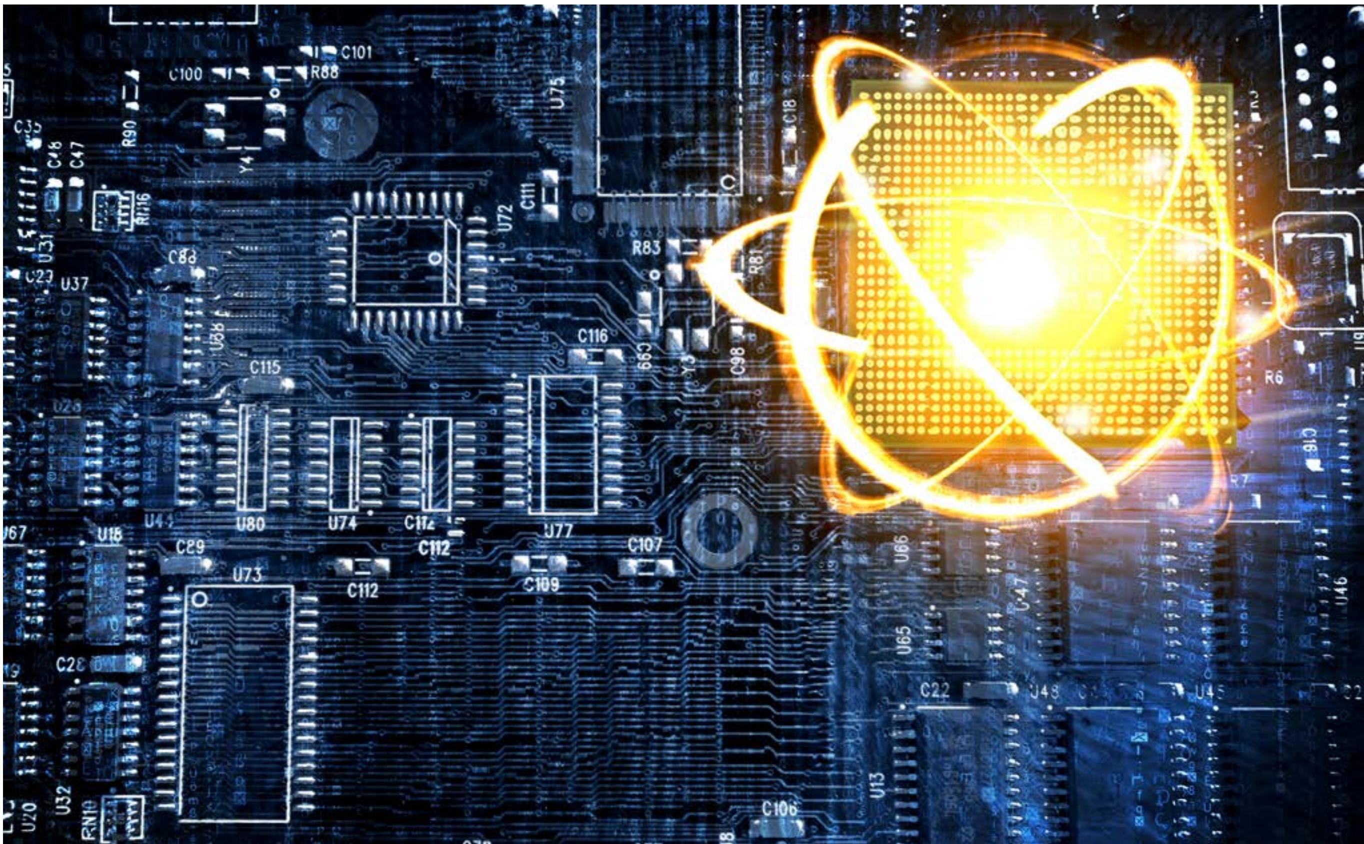
ers pose a threat to the security of these conventional authentication methods. Quantum tokens could represent a technical alternative for quantum communication in the future. By improving key components of this kind, we also create added value. The BMBF will therefore be working with scientists and industry in a process to identify a "grand challenge" in this field: the goal will be to implement new solution concepts for improving technological key factors in quantum communication, in the context of a competition. The idea is to pursue concrete technological objectives, while at the same time generating structural synergy effects for academic and industrial research.

European mission for quantum computing

The race to transform quantum computing from an idea into reality has been gaining pace rapidly in recent years, as proven by major investments in the USA and China. However, even the most promising of the many concepts being investigated in this field are still in very early development stages. We do not yet know which ideas will ultimately prove themselves, and the effective added value by comparison with traditional microprocessors remains unclear. For this reason, Europe hopes to develop a role as a system provider or supplier for industry, and has the full intention of bringing its own approaches to participate in the race. The Federal Government is implementing a three-pronged initiative to help with this:

- Definition of a research programme with content led by users and system creators from science, industrial interests, and public consumers. The research programme will be organised such that the participating partners will be rights-holders who can become shareholders in potential spin-off companies.
- Organising and funding up to three clusters of excellence for quantum computing in Germany. Involving international partners will be an essential

Building an universal quantum computer is a project characterised by major risks, but equally one that has huge application potential. Although developments in quantum computing over the last decade have remained almost exclusively inside the research facilities, it is now becoming increasingly urgent to involve potential users. Tasks and challenges can be defined in the context of close collaborations; research can then focus on finding targeted algorithms to solve these tasks and evaluating hardware limitations.



prerequisite for subsequent transition into European scientific and, most importantly, industrial structures. The clusters, with substantial involvement from commercial enterprises, will research the most promising approaches for quantum computing, identify practical applications and develop hardware platforms to demonstrate them. Important developments in the technical periphery and subsystems will be exploited as soon as IP has been secured, and made commercially available to researchers worldwide. Key indicators for the success of the clusters will include: development of industrially relevant skills in quantum information technology, international networking, commercial strategies and the involvement of industrial partners.

- Founding (spin-off) companies in the field of quantum computing. The companies will be responsible for transferring research results into industry. This transfer can take place on a gradual basis and within subfields, and should be oriented towards an international market. The public sector can keep share rights in the spin-offs that receive funding, and thus benefit from a suitable organisational form with experience in start-up and share management. Involving strategic investors is also a part of this process.

3.4 Ensuring security and technological sovereignty

Quantum technologies for satellites

Quantum technologies will find increasing use in earth monitoring, satellite communications and satellite navigation. These fields are relevant to sovereign security interests and are crucial foundations for a highly developed industrial society. Quantum technologies in these fields are on the brink of application. The USA and China are working intensively on modernising their satellite infrastructure on the basis of quantum technologies. It will be important to likewise modernise Europe's satellite infrastructure quickly and systematically, in order to ensure Europe's technical sovereignty in this field and avoid dependencies. German science and industry have a key contribution to make to this.

Earth monitoring is a part of environmental, security and defence policy, not to mention numerous industrial sectors – the search for raw mineral deposits, land use planning, town planning, traffic management, and agriculture and forestry, to name a few. Tap-proof satellite communication is as essential for the civil sector as for the military. Satellite navigation is used for precise positioning (e.g. for air, road, rail and sea transport), for international communications, energy supplies and bank transfer systems, and the electronic stock exchange, and will in future be essential to our universal time standard. By developing the Galileo system, Europe has built its own navigation system that can complement America's GPS and has strategic importance for Europe's sovereignty in both the civil and military domains. When the quantum technologies developed to date are put to use, we can predict a tenfold improvement in measurement accuracy for the distances, positions and times used in satellite technology, which represents a vast performance improvement for satellite-based applications.

This dramatic advance in satellite navigation performance is essentially the consequence of new quantum-based methods for measuring time and frequency, in conjunction with quantum-based optical signal transmission. Prototypes are already being developed for highly precise optical single-ion clocks. It is crucial that we now carry out targeted development of these new technologies, and ensure that they can withstand the enormous stresses of a rocket launch and operate satisfactorily in the extreme temperatures and powerful radiation they will be subjected to in orbit. This is an essential prerequisite for Germany and Europe to be able in future to make use of satellite systems using the latest and best technologies.

The German Aerospace Center (DLR) has decades of experience and proven competence in satellite development. In order to achieve the breakthroughs needed to put quantum technologies into orbit and secure Germany's role as a technology pioneer in this sector, the Federal Government is reviewing the options for developing institutional research activities at the DLR and its cooperative partners. The PTB in particular represents a significant strategic development partner, with unique features in the field of quantum metrology and sensing, as well as its sovereign tasks in the time and frequency transmission sector. Potential projects

There is a wide range of application possibilities for quantum technologies on satellites. For example, using quantum states offers much greater measurement accuracy, which could enable environmental parameters to be measured in much greater precision than ever before. However, creating components robust enough to operate in the space environment represents considerable practical challenges.

will cover in particular the fields of geodesy, metrology and sensor technology, developing quantum precision instruments suited for use in space and designing future Galileo satellites. Two new institutes and a Galileo centre of excellence could be set up at the DLR for this purpose. The DLR would provide qualified contract awards to support the parallel development of an industrial basis in satellite quantum technologies.

In recent years, funding initiatives under the umbrella of the "National Programme for Space and Innovation" have enabled Germany not merely to maintain its leading international position in the field of quantum optics, but in fact to increase its lead in some areas. The collaborative project "QUANTUS" established a network of facilities that in the last decade has not only achieved externally visible milestones for the early stages of space-related quantum technologies, but has also reached beyond the basic physical research questions to cast a growing spotlight on the applied aspect of quantum technologies. In parallel to gradually bringing the technology to maturity, long-term testing of the newly developed technologies has already begun in the Low Earth orbit (on satellite platforms and the international space station). The first practical space applications are also looming over the horizon – optical clocks for precision navigation, quantum gravimeters for accurate measurement of the temporal changes to the earth's gravitational field.

Secure communications and data

In the face of the many threats to Germany's internal and external security, it is vital to equip the federal security authorities and German Armed Forces (Bundeswehr) with the best possible skills and technologies to ensure they can fulfil their legal and constitutional mandates, while at the same time establishing Germany as a leading security location where the confidentiality and integrity of IT systems and digital communications can be guaranteed.

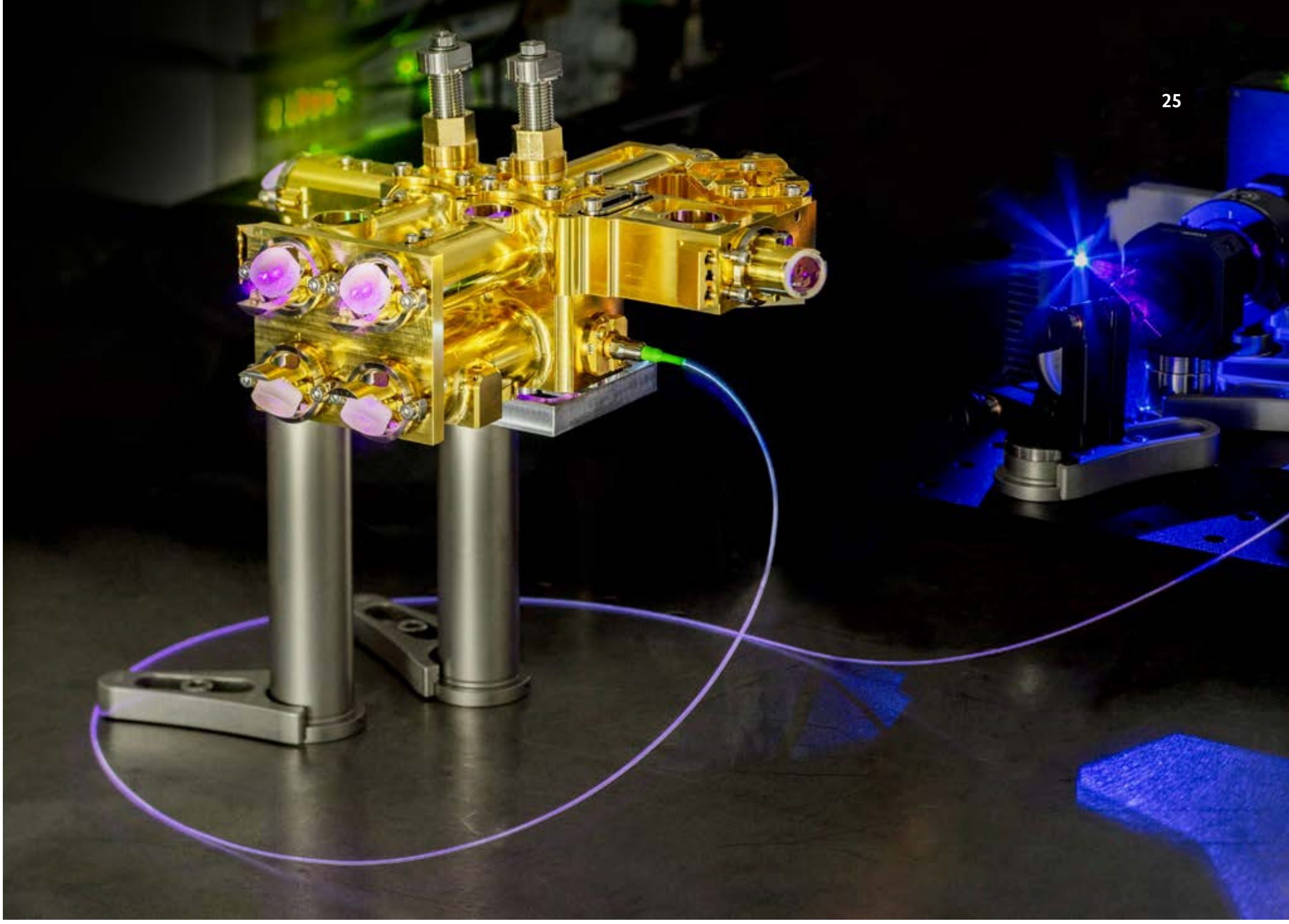
Establishing effective defence against cyber-attacks and guaranteeing high quality standards in the field of cybersecurity will depend on increased participation in the continuous dynamic innovation process that cybersecurity technology is currently enjoying, plus a deeper involvement in relevant key technologies. The Federal Ministry of the Interior, Building and Community (BMI) and the Federal Ministry of Defence (BMVg) see quantum technology as having a particularly high potential for innovation and applications, due to the prominent role it will play in the advancing digital transformation, encryption of digital communication, and machine-assisted operations in general. The federal security agencies and German Armed Forces therefore consider active, needs-oriented funding for research, innovation and development in the field of quantum technology to be of particular importance. Targeted funding initiatives could also facilitate the development of concrete dual-use applications and spillover effects.

The Federal Government believes that it is particularly important to develop quantum-resistant cryptographic systems; these systems must be capable of resisting attacks from quantum computers as well as traditional techniques, while also able to work with existing communication protocols and networks. The Federal Government intends to be active in this domain in order to ensure that Germany keeps its position as the world's leading country in the field of encryption. This means meeting the challenge of moving to new cryptographic infrastructures, requiring a focus on a kind of "crypto-agility".

Quantum communication, including quantum key exchange, is considered to be secure because eavesdropping attempts are observed as data losses. However, turning quantum communication from theory into reality is dependent on finding suitable technical solutions – adapting fibre optic communication, for example. The Federal Government wants to accompany this research.

At the same time, breaking traditional cryptographic techniques could open up new possibilities for law enforcement authorities. The new technologies emerging may raise the possibility of reopening criminal processes (providing they have not yet passed the statute of limitations) that involved encrypted digital evidence that could not be investigated at the time, but could be decrypted using the new techniques and assessed. The field must therefore also be tracked from the perspective of the law enforcement authorities. The responsibility for researching and developing technical solutions for security authorities that come under the BMI's business area lies with ZITiS (the Central Office

Achievements in transforming quantum technologies into reality have enormous repercussions, particularly for data security. Building on progress in the field of quantum cryptography, we will be able set up secure communication networks. However, future third parties could also have access to quantum computers for decryption – and our important communications must continue to remain secure in this scenario.



Technological approaches to quantum key exchange are primarily based on photonics. The fundamental reason for this is that not only can photons (light particles) be generated and prepared with comparatively low technological costs, they can also be transported over large distances without losing their quantum characteristics. Single photon sources (such as those shown in the image) are used to generate these specially prepared photons.

for Information Technology in the Security Sphere). ZITiS defines its key fields of interest as telecommunications monitoring, digital forensics, crypto-analysis and big data analysis, all of which will be affected by progress in quantum computing. ZITiS is planning to work with the CODE research institute to make use of a quantum computer at its future site at Bundeswehr University Munich. This interface will facilitate ongoing exchanges with the BMVg, since the encryption of existing IT security systems is of great importance to both departments.

The BMVg has defined its strategic focus over the next few years based on the "Cyber and Information Technologies" remit of the German Armed Forces: the key themes will be defence-related research and technology, including developing potential military applications for quantum technology. The strategy will be twofold. One aim is to systematically address the German Armed Forces' skills requirements for applied basic research from the perspective of informatics, in particular IT security, in close cooperation with various in-house facilities. The other aim is for the BMVg to use its own research funds to develop specific technical fields – such as quantum technologies – that are considered useful for the expected needs and operational capability of the German Armed Forces, and make these technologies available more quickly. These projects will be given institutional reinforcement in future through establishment and expansion of the BMVg's own centres of excellence and its research and innovation centres. In particular, a new Agency for Innovation in Cybersecurity is to be established. It will be operated jointly with the BMI and provide funding to high-risk projects with big innovation potential.

Projects that are particularly relevant to the German Armed Forces include, for example, application-oriented scientific research on secure data transmission, based on systematically developing secure communication techniques based on quantum cryptography. In the field of quantum computing and simulation, encryption and decryption of the security systems currently in use in computers and information technology is of strategic importance. Bundeswehr University Munich has taken an initial step here by signing a cooperation agreement with IBM for the foundation of an IBM quantum hub at the CODE Cyber Defence research institute in Munich. Another area of interest is applications that could be used to create complex military simulations for mission planning, exercises and training. Finally, in the domain of positioning, navigation and time determination, there is considerable interest in a number of scientific research and application-ready solutions based on quantum sensing and metrology that are already close to reaching the required maturity even for military conditions.

A test route for quantum cryptography through fibre optic cables is one of the things to be built in the PTB's forthcoming Centre of Excellence for Quantum Technologies. This will be used, among other things, for building a recognised testing structure and the development of corresponding standards. Recently the PTB was able to boast a demonstration of the most accurate frequency transmission in the world over optical fibres, between Paris and Braunschweig. This link, which is accessible about every one hundred kilometres, can be extended to form a test environment for quantum encryption over long distances. A node in London was added not long ago, and another node in north Italy is planned for the near future. European metrological institutes have suggested that the link could form the foundation of a European fibre backbone for frequency distribution, which could also be used for quantum encryption. Space-based technologies for quantum key distribution - where there is much less weakening in the signal - could prove the ideal counterpart to terrestrial developments and allow larger distances to be included in the picture.

Quantum key exchange via satellites makes an interesting complementary approach. Space travel technology has an advantage over fibre optic communications in that it is able to cover distances much greater than just 100-200 kilometres. The DLR space administration funding budget therefore provides for an intensified focus on satellite-based quantum communication.

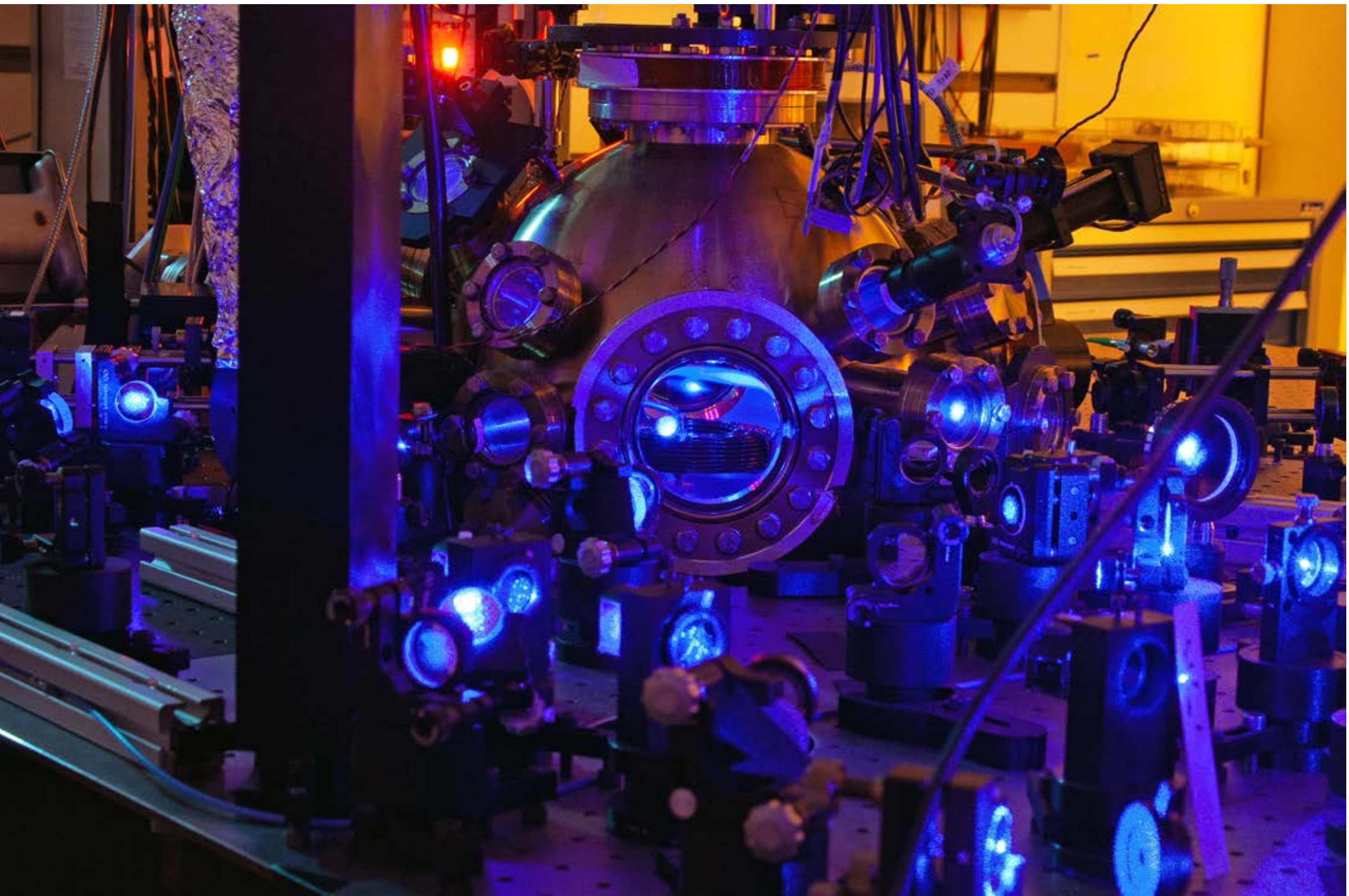
3.5 Shaping international collaboration

Metrology and standards

Despite growing competition in the scientific, industrial and security spheres, it is important for research on quantum technologies to remain open to collaborative work. The Federal Government will therefore work to strengthen quantum technology collaborations, both within Europe and further afield. Projects will cover the early stages of application development, standardisation and public remits.

> Defining standards demands extremely high accuracy measurements, which can then be used as a reference for other devices. The international time standards have for decades been based on monitoring atomic quantum states, and accuracy requirements have been continually becoming more exacting. Atomic clocks based on quantum systems, like the one shown in the image, act as time references for precision measurements, such as the Global Position System (GPS) or cycle frequency for a faster internet.

The National Metrology Institute of Germany (PTB), is collaborating intensively with leading international metrology institutes in the fields of quantum metrology and sensing. Collaboration partners include the National Institute of Standards and Technology (NIST) in the USA, the National Metrology Institute of Japan (NMIJ) and the National Institute for Physical and Chemical Research (RIKEN) in Japan, the Laboratoire national de métrologie et d'essais (LNE) and Systèmes de Référence Temps Espace (SYRTE) in France, the Istituto Nazionale di Ricerca Metrologica (INRIM) in Italy, and the British National Physics Laboratory (NPL). An important topic for these collaborations is developing the next generation of optical clocks and optical resonators. With recent demonstration of the most accurate frequency transmission in the world over fibre optics, between Paris and Braunschweig, it has



become possible for the first time to compare optical clocks rapidly and accurately. The collaborations will be strengthened over the next few years.

International collaborations studying quantum effects will be essential to revising the International System of Units (SI) with new, quantum-based, definitions for the units for mass (kilogram), amount of substance (Mol), temperature (Kelvin) and the units used in electrical applications. The PTB is helping to drive this work forward internationally.

Scaling up European research

To fight for their place in the competition for minds and investments, Germany and Europe need first-class civil research infrastructures. Germany will reach out to key partner countries with the goal of developing joint projects to boost Europe's visibility and attractiveness for research on quantum technology. Germany and Europe must attract outstanding individuals, of any origin and gender, with particular expertise and interest in researching and developing quantum technologies.

As part of its contribution to collaborative research in Europe, Germany is a member of the ERA-NET programme "QuantERA"[36]. In the framework of the programme, the BMBF and 31 other partners from the EU, Israel, Turkey and Switzerland have been working together since spring 2018 to support collaborative research projects linking institutes and enterprises from the participating countries. Germany is represented in (by far) the lion's share of the "QuantERA" projects.

The EU research project into quantum technologies ("EU Quantum Flagship") aims to make Europe into a leading region for industrial implementation of quantum technologies. Germany has accompanied this major European project closely right from the start – for example, providing personal and financial support to the High Level Steering Committee, which set out a comprehensive position paper with its recommendations at the end of 2017.[37] The programme of activities and call for proposals for the first phase of the European flagship project were published at the end of 2017. Numerous German applicants participated successfully in these processes. Launch of the projects began in autumn 2018, with the start of the main phase currently scheduled for 2020. A further goal is to build a close link, through joint projects, with the successful "European Metrology Programme for Innovation and Research" (EMPIR) or its successor.

3.6 Getting Germany's population involved

Establishing foundations for understanding quantum technologies

New technologies always raise questions concerning their ethical foundations and the ecological, economic, political and social consequences of the new applications. These questions are discussed among the general public. Decisions about them come to parliament. As part of this programme, the Federal Government will contribute to establishing the necessary specialised foundations.

To this end, it is essential to make the topic of quantum technology as accessible as possible for the general public. Current navigation systems are based on satellite technology – but it is not necessary to understand satellite technology to use a navigation system. Likewise, it is in no way necessary to have studied physics to make use of quantum technologies. In future, generally accessible approaches and specific information about applications of quantum technologies must become a part of general education and schooling, and be included in courses other than physics, such as engineering studies. The Federal Government intends to be involved in establishing the necessary basis for professional training, informed discussions and responsible use of these technologies.

The Federal Government has already taken the first step: since 2016, it has been working with experts in an agenda process, inviting recommendations that will be implemented as a part of this programme:

- Teaching: quantum physics is currently taught from a theoretical viewpoint, almost entirely mathematically. It is important to develop concepts for a more intuitive approach, using teaching tools that demonstrate quantum effects as directly as possi-

36 https://cordis.europa.eu/project/rcn/207196_en.html; https://www.quantera.eu
37 Quantum Technologies Flagship Final Report; Source: see footnote 3

There remains a need to provide clear explanations about the fundamental physical principles of quantum technology – quantum characteristics such as superposition and entanglement are still highly inaccessible to the layman. It is thus essential to open up dialogues with the general public. This could begin at school: the image shows a model quantum cryptography experiment which won an award in the national "INVENT a CHIP" competition. The physical background and related principles could also be explained and communicated as part of exhibitions.

ble and allow a practical, even playful, approach to quantum physics.

- Access: technical museums and exhibitions in Germany should include more experiments and applications of quantum technology.
- Participation: building things for oneself is another way to discover routes into new technologies and promote responsible use. The Federal Government will therefore develop quantum technology initiatives oriented towards makers, such as open technology platforms for DIY enthusiasts and SMEs. Competitions have been used successfully in other technical fields to increase visibility, improve understanding and boost motivation for young academic and industrial talent – for example, "Start Coding" for programmers, or "RoboCup" for robotics. The Federal Government will review how competitions of this kind could be established in the quantum technology arena.

Sparking interest in quantum technology among the next generation

An understanding of quantum technologies is founded on the same key qualifications that are important for our economic status: mathematics, information technology, natural sciences and technology (MINT). The Federal Government, German research organisations and industry are committed to working together to promote the acquisition of knowledge and skills in MINT topics, demonstrate different perspectives and combat the impending threat of a skills shortage. Two promising routes for improving the skills situation are capitalising more on our native potential (e.g. with early career orientation towards MINT subjects in schools), and encouraging immigration of specialists from abroad. International specialists are already making an important contribution to MINT fields. According to the OECD, Germany is among the countries with the most liberal immigration regulations for academically qualified specialists from third countries.[38] The official information portal "Make it in Germany"[39] provides guidance to interested specialists and enterprises, as well as individual advice through the "Live and Work in Germany" hotline. KOFA is a competence centre for recruiting specialists[40]: it offers SMEs advice on how to increase their attractiveness as employers and remain competitive by attracting a skilled workforce.

The importance of bringing new talent into scientific fields is another key concern for the Federal Govern-

38 OECD (2013), Recruiting Immigrant Workers: Germany, OECD Publishing, p. 15; http://dx.doi.org/10.1787/9789264189034-en
39 https://www.make-it-in-germany.com/en
40 https://www.kofa.de

ment. For this reason, it finances – directly or indirectly – a large part of the German programme for supporting young scientific talent. This includes institutional funding for scientific and intermediary organisations, alongside major projects such as the new “Tenure Track” programme for supporting junior academics[41], the Excellence Initiative and the “Pact for Research and Innovation”. The ruling parties declared an intention in their coalition treaty to create predictable, reliable career paths within the university system and to work with the scientific organisations on concrete goals towards encouraging young talent.

41 https://www.bmbf.de/de/wissenschaftlicher-nachwuchs-144.html

In a complex field like quantum technology, highly educated experts are urgently needed in both the scientific and industrial spheres. A high level of education is essential not just for research, but also in order to use these quantum technologies. It is therefore important to introduce students of the related engineering subjects to quantum technologies during their studies. One example of how this can be done is the BMBF’s “Quantum Futur” academy – a practical week of seminars, creative innovation workshops and insider views of research institutes and enterprises.

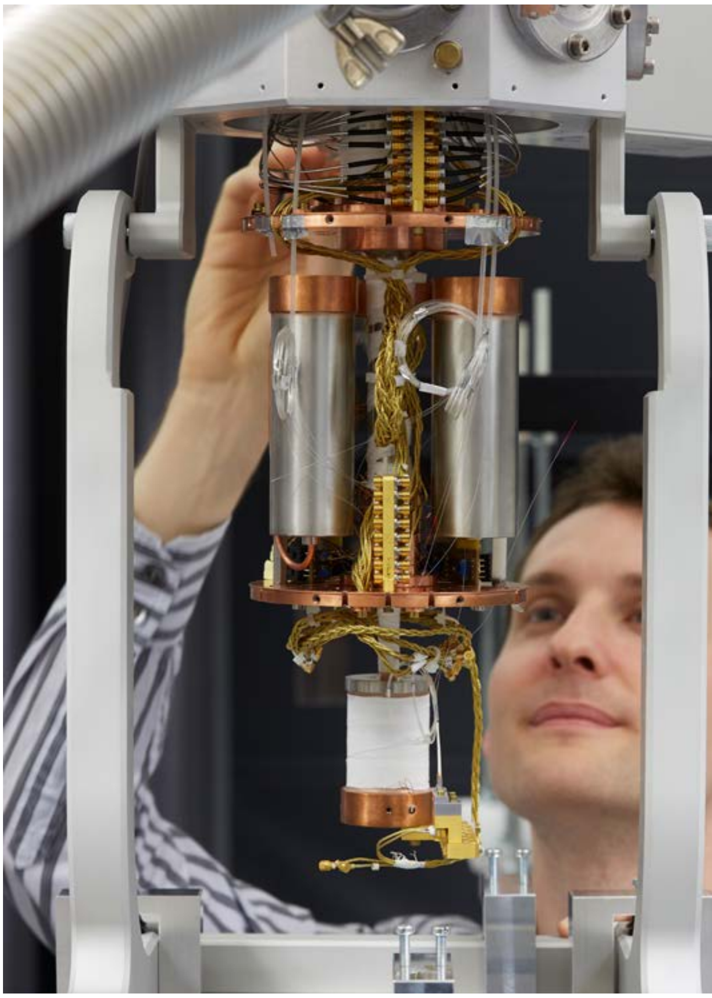
Successful, widespread implementation of quantum technologies in industry and applications in the public domain are only possible if we have enough specialists with expertise in quantum technology. Quantum technologies lie on the boundary between challenging subdisciplines from physics, engineering and informatics – all disciplines for which Germany has traditionally been an attractive location. We need to be combining these subdisciplines and establishing appropriate interdisciplinary and international research projects and study programmes. The following initiatives have been planned in this context, or have already begun:

- In 2017, the BMBF called for junior research groups to be set up[42], thereby publishing its first initiative targeted specifically at training future executives in quantum technologies. This is a way for the BMBF to support excellent young talent with driving forward research projects that can bridge the gap between basic research and innovative applications.

42 https://www.bmbf.de/foerderungen/bekanntmachung-1371.html

The young scientists should qualify for leadership roles in industry and science. Around 25 million euros were made available for the first groups in 2018. The junior research groups will hold regular joint workshops where they can exchange information and ideas and network with each other. A second round of selections will be held in 2020.

- In March 2018, the BMBF teamed up with partners from science and industry to hold the first "Quantum Futur" academy. This is a one-week event for advanced university students. A programme of lectures, practical work and expert panels at management level provides insights into the latest developments and individual opportunities in quantum technologies. As well as holding the "Quantum Futur" academy again in 2019, the BMBF is working on developing the concept further, with plans to run similar initiatives at a European level. These will be launched from 2020 and aim to establish Europe's profile for encouraging fresh talent in quantum technologies.
- R&D funding projects for topics in quantum technology are already making a visible contribution to supporting young talent in this field. Dozens of Bachelor's, Master's and doctoral theses have been completed through collaborative projects and technology development projects from the DLR's space administration programme. Young scientists and engineers have furthermore been able to build on their doctoral and postdoc work in these projects, thereby establishing a good position for a subsequent scientific career path or qualifying themselves for later work in industrial environments. Over the next few years, the national aerospace programme will continue this successful strategy for supporting young talent.
- The Federal Government plans to create a catalogue of best practices for integrating quantum technologies into courses other than physics, and support trials of new concepts. The goal here is to create stronger links between departments and develop programmes of activity to complement e.g. PhD research training.



The applied research projects that are already on the horizon will absorb most of the available human resources in the quantum technology community. Innovative young scientists are able to build up their own working groups and widen the professional arena. Junior research groups in the quantum technologies field therefore represent expansion of the existing research landscape in terms of both minds and topics.

4 Resource planning

The costs of research, development and applications of quantum technology are currently primarily financed in the context of core funding from research organisations or as part of individual project funding initiatives. Germany currently has quantifiable resources of around 100 million euros per year. Adding the new initiatives described in this programme (see Section 3), the Federal Government will have scheduled resources of around 650 million euros for the period from 2018 to 2022. The programme is expected to continue until 2028. Federal Government and parliament will make decisions about its focuses, responsibilities, content and financial structure going forward from 2022 based on scientific and commercial developments in the field of quantum technologies and their applications.

Quantum technology promises huge opportunities for Germany to grow as an industrial centre. In order to develop these technologies as early as possible and bring them to bear fruit, it is important for industry and science, policy and society to work together.

5 Appendix: R&D funding organisations, non-university research organisations and departmental research institutes

5.1 German Research Foundation

The German Research Foundation (DFG) began many years ago to fund research directly related to quantum technologies. It is worth noting here that the topics in proposals will often come to assume a prominent role. It is virtually impossible to make predictions about future developments, since the applicants have a free choice of application topics and initiatives and the DFG does not make any particular specifications here. The responsible department does not consider there to be any indication that we should expect a decline in the resources applied for in this research field or the volume of funding.

In 2018, the DFG funded research directly related to quantum technology with grants worth 52.9 million euros annually. Of this, 35.6 million euros are allocated to coordinated programmes (research groups, priority programmes, special research domains, post-graduate programmes, clusters of excellence). The remaining 17.3 million euros represent individual funding (material grants, research grants, the Emmy Noether programme, the Heisenberg programme, Reinhart Koselleck projects), prizes and the "International Scientific Contacts" programme.

This data is based on projects that were receiving ongoing funding on 30 April 2018.

5.2 Max Planck Society

The Max Planck Society (MPG) was an early supporter of basic research on quantum technologies, in the sense of the second quantum revolution. The Max Planck Institute (MPI) of Quantum Optics in Garching was founded in 1981. The experimental branch of the MPI for Gravitational Physics in Hanover was founded in 1993, followed in 1994 by the Dresden MPI for the Physics of Complex Systems and then in 2009 the Erlangen MPI for the Science of Light. In addition to this, the Max Planck Institutes for Solid State Research (Stuttgart), the Chemical Physics of Solids (Dresden), the Structure and Dynamics of Matter (Hamburg), Microstructure Physics (Halle), and the Fritz Haber Institute in Berlin are all working to some extent on aspects of this topic. In light of the basic research on quantum technologies taking place across these institutions, the MPG considers itself a pioneer in quantum technologies and a supporter of the current specialist programme for quantum technologies.

The MPG views quantum technologies as a strategically important topic, not only in relation to the basic research, but also in light of their potential economic benefits. Germany is well-positioned in terms of basic research and can take on a leading role in the international race for quantum technologies. Reaching this position involved a long-term strategy, and the programme will make it possible to implement this strategy. The MPG brings key expertise to participate in this process, particularly in the fields of:

- Quantum computing and quantum simulation (Berlin, Dresden, Garching, Halle, Hamburg and Stuttgart)
- Quantum communication, including satellite communication (Garching and Erlangen)
- Quantum metrology, in particular ultrasensitive interferometer sensor technology (Hanover and Erlangen)

The MPG sees its contribution to the national strategy as primarily in progressing and broadening world-class basic research. This includes opening up new subfields, patenting new ideas, and participating in national and international research networks. The MPG is also keen to be involved in creating applied technologies based on fundamental phenomena from the second quantum revolution. This work will involve bodies such as the independent Max Planck Research Groups and the International Max Planck Research Schools.

Representatives of the MPG made significant contributions to the concept paper drawn up by the scientific community (QUTEGA) and are keen to support initiatives that look beyond the established programme and make use of the research grant instruments recommended within the paper, for example setting up consortia and junior research groups. These consortia should build on proven expertise in their various fields to bring maximum innovation to specific locations or across the board.

5.3 Fraunhofer Society

The Fraunhofer Society perceives quantum technologies to be an important opportunity for the future of Germany and Europe as a key high-tech location. To secure its place in the international race for applied quantum technologies, the Society has designated an investment of around 20 million euros for funding extensive research activities; the funding is part of a prioritised strategic initiative from the "Fraunhofer Agenda 2022". A transfer and exploitation structure is to be established for the German and European economic area, building a multidisciplinary pool of expertise drawn from twelve Fraunhofer institutes. The digital transformation and sovereignty of the digital society in Germany and Europe are key drivers for this funding strategy.

The central funding project in the prioritised strategic initiative is the "QUILT" flagship project ("Quantum Methods for Advanced Imaging Solutions"), coordinated by Fraunhofer IOF and Fraunhofer IPM and involving four more Fraunhofer institutes (ILT, IMS, IOSB, ITWM). Internationally leading experts in quantum optics will be working with the Institute for Quantum Optics and Quantum Information (IQOQI) at the Austrian Academy of Sciences and the Max Planck Institute for the Science of Light (MPG-MPL) to develop application scenarios and demonstrators in the field of quantum imaging. Key focuses of this work will be ghost imaging for biomedical imaging and optical remote sensing, in conjunction with production techniques based on quantum optics for the high-resolution lithography field. The advisory board for the flagship project will also involve key actors from the optics and photonics sector of German industry.

The central initiative for exploiting quantum sensors takes the form of a focus project involving the three Freiburg institutes, IAF, IPM and IWM. The project was launched in 2018 and is jointly funded by the State of Baden-Württemberg. It is anchored in one of the leading regions for quantum sensing within the German and European research area and aligned with the centres of excellence at the Universities of Stuttgart and Ulm. The project is tackling one of the most promising directions for quantum sensing, developing it and maturing it into applications. Its main research focuses are on processes for producing customised NV defect centres in diamond lattices and manufacturing optical magnetometers based on manipulating spin states in vapour cells. These can be used to make high-resolution measurements of the tiniest currents and magnetic fields, with spatial resolution right down to the lowest nanoscale. A wide spectrum of application scenarios is envisaged – from microelectronics and medical technology to geodesy or chemical and biomedical analysis. The project focuses on analysis and development of micro- and nanoelectronic components, and its objectives align with the competence pool "Research Fab Microelectronics Germany".

Fraunhofer/Max Planck research partnerships also have an important role to play in collaborative work with Partners of Excellence in the field of research on quantum sensing and metrology. The Fraunhofer IAF is working with the MPI for Solid State Research (MPG-FKF) and the University of Stuttgart on high-resolution magnetic field sensor technology for nuclear magnetic resonance spectroscopy at nanoscales. The Fraunhofer IPM and the MPI for Quantum Optics (MPG-MPQ) are carrying out collaborative research on ultra-precise spectroscopy for quantum metrology using frequency combs. Partners at MPQ are laying the foundations for a variety of quantum sensing applications in high-precision synchronisation technologies combined with high-resolution measurements of acceleration and gravity.

The "Attract" programme offers an opportunity for excellent scientists working in cutting-edge research to bring their skills to the Fraunhofer Society to work on selected research focuses. A spin-off research group (Quantum Technology Laboratories GmbH) from the IQOQI adds a quantum communication focus alongside the quantum optics activities in the Fraunhofer IOF flagship project. The research group is working on entangling photon pairs through several characteristics, in order to improve transmission efficiency for satellite-based and fibre optic quantum communication networks. This will strengthen collaboration between the Fraunhofer IOF and the IQOQI as an internationally recognised centre for quantum information theory. A joint laboratory to be operated by the two facilities is currently under development.

Enabling technologies as modular quantum tools

Many applications based on quantum technology can be developed as modular combinations of various enabling technologies. The full technological spectrum for universal quantum tools is being addressed via the fields of expertise and portfolios at the Fraunhofer institutes, based on the prioritised strategic initiatives from materials science, photonics and microelectronics, and information and communication technologies. A few front runners can be identified among the current development projects:

- Single photon technologies: sources for deterministic photons, entangled photon pairs and platforms for integrated parametric frequency conversion (Fraunhofer CAP-UK, HHI, IAF, ILT, IMM, IOF, IOSB, IPM, ITWM)
- Photonic interfaces, integrated wave guide technologies and microoptics (Fraunhofer CAP-UK, HHI, IAF, ILT, IOF)
- Materials engineering and high-precision manufacturing processes for quantum media in the form of isolated quantum dots and extended vector and matrix arrangements of quantum dots with tailored characteristics (Fraunhofer IAF, IMM, IWM).

These elements will form a basis for modular technology platforms enabling systematic, comprehensive system integration in diverse application areas. Enabling technologies envisaged include:

- Spectrally tunable single photon sources
- Photonic platforms and photonic integrated circuits for controlling and displaying isolated quantum centres and quantum arrays in quantum information processing and quantum sensing
- Detectors and microelectronic environmental architectures for recording, amplifying and digitalising tiny signals

The Fraunhofer institutes are contributing to progress in the enabling technologies with research in the fields of informatics, mathematics, and materials modelling. Key themes here are virtualising quantum physical processes in order to optimise modular applications, and securing traditional communication networks within existing security architectures. Particular focuses have been defined for both areas:

- Modelling complex quantum systems in terms of decoherence and energy level structure, theoretical analyses of quantum transmission mechanisms and quantum information transport (Fraunhofer ITWM, IWM, SCAI)
- Using AI and machine learning methods to analyse complex interactions between individual components in modular quantum technologies, towards system optimisation and test scenarios (Fraunhofer ITWM, SCAI)
- Embedding quantum key distribution in traditional cryptographic protocols, linking quantum communication networks to traditional security architectures (Fraunhofer AISEC, SIT)
- Post-quantum cryptography (Fraunhofer AISEC, SIT)

These modular technologies establish a basis for the Fraunhofer Society's general strategy of exploitation. The pool of enabling technologies will be developed synergistically through coordinated research activities, and targeted towards specific application scenarios. This development strategy is the basis of a broad infrastructure for technology transfer and exploitation.

Infrastructure for technology transfer and exploitation

Competences in quantum technologies will be pooled within the prioritised strategic initiatives, creating an organisational framework for an extensive infrastructure for technology transfer and exploitation. Multidisciplinary research projects in varied application domains at the institutes will be linked together. This approach is aligned with the European Commission's FET Flagship Initiative and it is envisaged that European goals will be actively supported via an exploitation structure developed by the Fraunhofer Society.

Quantum imaging research field

The Fraunhofer IOF in Jena is coordinating the "QUILT" flagship project at one of Germany's leading centres for the optics and photonics industry. The participating institutes (ILT, IMS, IOF, IOSB, IPM, ITWM) are engaged in research projects focused on the high application potential of entangled photon pairs for optical imaging, spectroscopy and lithography. The central goal of the flagship is to identify and demonstrate the added value that quantum optic processes can offer against the latest developments in competitive traditional technologies. This will address a significant issue for traditional imaging processes: they cannot easily be applied with extremely short- or long-wave light sources or challenging non-homogeneous media. The possibility of transmitting information between physically and spectrally separated photon pairs by using entanglement is the starting point for the added value in the quantum optics approach. In the fields of ghost imaging and hyperspectral imaging, challenging spectral ranges and distorting media could be made accessible to established optical procedures using mature detector technology and standard optical techniques. Meanwhile, projects in the field of optical microscopy and remote sensing will tackle resolution quality, material-specific detection and phototoxicity, image quality, penetration depth and coverage in scattered tissues and atmospheric distortions. This approach brings vital innovation to established application fields for biomedical imaging and medical diagnostics, materials testing, process and environmental analysis, security technology and automatic mobility.

Quantum sensing research field

Sensors play a central role in the German and European digital economy. Research at the Fraunhofer IAF in collaboration with the Fraunhofer IPM, IWM, IMM and CAP-UK is focusing intensively on solid state technologies that could facilitate widespread use of customised quantum sensors at room temperature and in variable environments. This research will address a major obstacle for quantum sensors: due to their extreme sensitivity to environmental conditions, quantum sensors often need costly platforms. The need for cryogenic cooling and a vacuum environment means that many sensors have very restricted application ranges, despite advantageous performance features. A technique for synthesising NV defect centres in diamond lattices makes it possible to manufacture nanoscale sensors, and customise their characteristics for diverse applications. This work is complemented by a project to make optical magnetometers using vapour cells industry-ready. These can be used to make high-resolution measurements of the tiniest currents and magnetic fields, with spatial resolution right down to the lowest nanoscale. The applications for this technology are in development and analysis of high-density storage media and low-dimensional semiconductor components. A fundamental new quality assurance tool for micro- and nanoelectronic circuits will also be created, thanks to the high spatial resolution, which is capable of showing tiny currents such as gate leakage currents. This work links in very closely to the mission of Research Fab Microelectronics Germany. With a sensitivity in the region of from a few hundred to just a few nuclear spins, nanoscalar NMR spectroscopy will open up new avenues for chemical and biomedical analysis. The structure and function of chemical and biological systems could be made visually accessible by detecting nuclear and electron spins. The highly sensitive spectroscopy could represent a way towards visualising single molecules within larger structures such as protein systems. Contactless measurements of nerve pathways and brainwaves could form a basis for innovations with considerable scope for medical technology. By developing a non-invasive recording and pattern recognition system for brainwaves, we could create a fundamental entry point for interactions between man and machine. Geodesy and GPS-free navigation can be achieved by measuring tiny changes in the earth's magnetic field. There is immense scope for applications based on these developments in a number of sectors: the semiconductor industry, mineral resources, IT, medical technology, security technology, and chemical and biomedical analysis.

Quantum communication research field

As high-performance information technology gains influence in global networks, research on data security and confidential communication routes has huge implications for the sovereignty of the digital society in Germany and Europe. Secure communication networks represent critical infrastructure for a modern information society. A complete overhaul of our traditional security architectures is urgently required if we want to guarantee strict confidentiality in future communication networks. The Fraunhofer IOF and HHI are currently following the ESA roadmap towards satellite-based quantum key distribution (QKD), a fundamental step towards building a quantum communication network in the European area (ARTES and ScyLight). The research is focused primarily on creating standardised technologies for optical satellite links between primary geographical communication points and fibre optic networks. The underlying motivation for these developments is fundamental security in data transmission with entangled light particles as the information carrier. The security guarantee offered by quantum physics is fundamentally different in nature from the mathematical strategies for cryptographic algorithms that are used in today's technologies. Traditional approaches to security are at risk from new attack methods and depend heavily on the resources available to the attacker. With the transition to a quantum physics based approach to security, quantum communication will make a fundamental contribution to the confidentiality of digital information and transmissions, setting new standards for a sustainable security strategy. Competences from the Fraunhofer AISEC and SIT will be brought together to couple quantum communication technologies to traditional security architectures. Supporting studies will investigate the interactions between quantum and traditional information technologies.

Quantum computing research field

Developments in the field of quantum computing in the European research area are characterised by the formation of large research consortia to tackle this important topic area. Bringing together key expertise in pools of competence allows Europe to remain competitive with international groups and intensive national research funding outside Europe. RWTH Aachen and the Jülich Research Centre are collaborating with the QuTech Institute and the Technical University of Delft in the "JARA" consortium (Jülich Aachen Research Alliance), which is contributing fundamental research work to the international efforts to implement this key technology. Linked to these activities, the Fraunhofer ILT is working with Fraunhofer CAP-UK to develop quantum transport mechanisms for distributed quantum computing. The main research focuses are: the complex interaction between spectrally tuned single photon sources, integrated wave guides and microoptics, parametric frequency converters and embedding quantum emitters in suitable media and environments. Important new knowledge is being acquired and technological foundations for quantum information processing are being established. Links to other research fields can be established through these projects: findings from quantum communication and quantum sensing are important to the field of photonic technologies and these fields act as platforms for exchange with quantum computing research.

5.4 Helmholtz Association

Current activities and competences

The Helmholtz Association is working on a wide range of issues related to quantum technologies: from fundamental quantum phenomena to materials research; from component development to implementing functional technical systems. The key actors currently working on topics related to quantum technologies are the German Aerospace Center (DLR), the Jülich Research Centre (FZJ), the Helmholtz Centre in Berlin (HZB), the Helmholtz Centre in Dresden-Rossendorf (HZDR) and the Karlsruhe Institute for Technology (KIT). These five research centres are tapping into existing synergies in diverse research areas and interdisciplinary cooperative projects in order to answer contemporary research questions.

Through the two programmes "Future Information Technology" (FIT) and "Supercomputing and Big Data", the FZJ, HZB and KIT are jointly researching system and infrastructure oriented concepts for quantum information processing, which will drive forward the long-term development of quantum computing technologies from basic research all the way to applications. The goal is to develop scalable architectures and quantum algorithms to model real problems. A lighthouse project in this area is the future-oriented topic of scalable, solid state quantum computing; this is currently being financed by the Helmholtz Association's Initiative and Networking fund (FZJ, RWTH Aachen, KIT). The Karlsruhe Nano Micro Facility (KNMF) at KIT and the Helmholtz Nano Facility (HNF) at the FZJ are providing important infrastructure here. The DLR is also working with the FZJ in the field of quantum computing applications for air and space travel.

Complementing the quantum computing activity, FZJ and KIT also have research focuses in the field of quantum materials, and HZB is also carrying out basic research in this area as part of the "FIT" programme. Example projects include topological materials for realising Majorana qubits, synthesising molecular quantum components, growing pure semiconductor crystals for spin qubits, and developing new or improved superconductors for qubit applications. The Helmholtz centres (e.g. KIT) are building on the basic research to develop highly advanced architectures and physical platforms ("quantum simulators"); the ultimate goal will be universal quantum computers. Experiments on complex materials carried out through the HZDR materials research programme "From Matter to Materials and Life (MML)" are contributing towards research on quantum states such as spin liquids or coherent control of quantum systems at the nanometre scale.

Another key research area is that of quantum communication and quantum key distribution (QKD), which aims to facilitate long-distance transmission of quantum processor states via optical networks ("flying qubits") and to exploit the potential of the smaller quantum processors emerging from quantum computing research to create nodes in quantum communication networks. Quantum communication is not just relevant to the key technologies research field – it is also an element of the DLR's aerospace research activities in the aerospace travel and transport research field, where it is oriented towards satellite-supported quantum communication. The DLR is also engaged in research on quantum metrology, a topic highly relevant to security-critical applications as well as its commercial applications (which include e.g. earth monitoring, navigation and communication – for example, high-precision time determination for the next generation of navigation satellites). Another research interest is quantum sensor technology using cold atoms and Bose-Einstein condensates for atom interferometry, e.g. for inertial measurements of acceleration and rotation rates in space.

Selected research activities

The research activities at the Helmholtz Association have been designed to complement each other. During the current funding period, quantum technologies will be primarily researched in the context of the programmes listed in the table on p. 38.

The programme activities relevant to quantum technologies have received around 60 million euros of basic funding from the BMBF and federal states, in addition to resources from the Initiative and Networking fund.

Long-term research structure for quantum technology topics in the Helmholtz Association

In order to guarantee long-term research on quantum technologies in the Helmholtz Association and maintain a leading role in the international research arena, all participating research centres support continued institutional funding for research activities. Their activities will extend from pure basic research to preliminary work on first industrial applications. There will also be an ongoing effort to continue forging links between the research topics, regardless of the way the themes are anchored into their various research fields.

Overview of the relevant research activities within the Helmholtz Association

Research area	Programme/topics	Participants
Energy and key technologies	Future Information Technology (FIT) – Topics: Controlling Spin-Based Phenomena, Controlling Collective States	FZJ, HZB
Key technologies	Supercomputing and Big Data (SCBD) – Topics: Computational Science and Mathematical Methods, Data-Intensive Science and Federated Computing, Supercomputer Facility, Science and Technology of Nanosystems (STN) – Topics: Condensed Matter, Molecular Spin Qubits, Quantum Optics, Quantum Theory, Quantum Simulation	FZJ, KIT
Aviation, space travel and transport	Space – Topics: Communication and Navigation, Space System Technology	DLR
Materials	From Matter to Materials and Life (MML) – Topics: Quantum Condensed Matter: Magnetism, Superconductivity and Beyond, Nanoscience and Materials for Information Technology	HZDR, DESY, FZJ, HZB, HZG

The research field “Key Technologies” (to be renamed “Information”) will see an intensified focus on information technology topics, particularly quantum computing, in the next funding period. Feasibility testing will be particularly important here, alongside research on quantum materials for high-performance quantum information hardware. Planned expansions to the sites in Jülich and Karlsruhe will build on the existing research infrastructures: the FZJ is working on a dedicated extension to the Helmholtz Nano Facility (HNF) and developing a user infrastructure for quantum computing (JuNIQ), while KIT is planning to found an Institute for Quantum Technologies housing a Quantum Hardware Foundry, where materials concepts and component environments will be developed. Meanwhile in the materials research field, the research on quantum materials will be focused more tightly towards understanding and making use of the fundamental interactions and processes in e.g. topological materials and spin liquids. In addition to this, atomic qubits will be manufactured in semiconductor materials with nanometre precision, for example for use in quantum sensor technology. This work will make use of the HZDR research infrastructures, which will be developed further for the purpose.

The DLR has set out a three-pronged approach to developing quantum technologies for aerospace applications:

1. The planned DLR Institute for satellite geodesy and inertial sensing in Hanover will develop application-oriented quantum sensors for high-performance earth monitoring missions; the goal here is to establish precision geodesy in space and develop optical quantum engineering processes for space applications.
2. The Institute for Quantum Technologies will focus on topics such as quantum metrology, quantum sensing, quantum information technology and matter wave optics, with a view to aerospace applications.
3. This will be complemented by quantum technology approaches for the next generation of satellite navigation systems, to be developed at the Galileo centre of excellence.

The programme structure is a part of the ongoing dialogue between the Helmholtz Association and the grant authorities in preparation for the fourth programme period. The strategies formulated in 2017 allowed the Association and research departments to boost research activities in quantum technologies; these activities must now be anchored in the research policy guidelines. The programme developed on this basis will be evaluated by an external assessment group as part of the 2019 strategic evaluation.

Integration in the German and international research landscape

The participating Helmholtz Research centres aim to form a complementary structure of non-university research institutes, whereby joint projects will forge links between the research activities and universities or other non-university research facilities – for example, as part of the national QUTEGA initiative or the European FET Flagship on Quantum Technologies. Partnerships with universities and links to research networks will also be pursued as part of the German Excellence Initiative.

For example, the FZJ has founded the JARA Institute for Quantum Information in partnership with RWTH Aachen, as part of the Jülich Aachen Research Alliance (JARA). Other partners, e.g. CEA in Grenoble, have also been asked to participate in the EU Flagship project. The DLR Institute in Hanover is linked to the Quantum Engineering and Space-Time Research Cluster of Excellence (QUEST). Other participants include the Center of Applied Space Technology and Microgravity (ZARM), the PTB, TU Braunschweig, the Hanover Institute of Technology (HITec) and the Laboratory of Nano and Quantum Engineering (LNQE) at Leibniz University Hanover – this latter is also linked through the regional network with the Max Planck Institute for Gravitational Physics and the University of Bremen. The DLR Institute for Quantum Technologies in Ulm will also carry out work to complement the activities of the Center for Integrated Quantum Science and Technology (IQ^{ST}) at the Universities of Ulm and Stuttgart and the Max Planck Institute for Solid State Research in Stuttgart. The HZDR is also working together with TU Dresden and the University of Würzburg as part of the proposed Cluster of Excellence for Complexity and Topology in Quantum Matter (ct.qmat); the research strives to understand, control, and exploit fundamental new states of quantum matter. This is complemented by a number of applications from the HZDR within the European FET Flagship on Quantum Technologies.

KIT has formed an alliance with the universities of Basel, Freiburg and Strasbourg to found the "European Campus EUCOR", where a pool of interdisciplinary competences in the field of quantum technology is to be established. Another KIT joint project, with CNRS Grenoble, has established the GREKIT laboratory, specialising in the fields of superconductors and quantum technology. Applications in the context of the EU Flagship project will also be possible through these consortia.

Further work is emerging from collaborations between the Helmholtz centres and a variety of international research facilities – the QuTech Institute at TU Delft, ETH Zurich, the Interuniversity Microelectronics Centre (IMEC), the Skolkovo Foundation, the Russian Quantum Center, the National Institute for Quantum and Radiological Science and Technology in Japan, the Weizmann Institute in Rehovot and, last but by no means least, the DLR and the NASA Ames Research Center.

Since the German and European research activities around quantum technologies must position themselves in an internationally competitive environment, it is essential to strengthen international collaborations with key institutions, at the same time as recruiting scientists from all over the world. The Helmholtz Association is therefore calling for a joint talent initiative that will ensure national and European research activities maintain their leading position in the long term.

Collaborations with industrial partners and potential application examples

Although research on quantum technologies over recent years has made significant progress in developing technologies ripe for implementation, there is still scope to establish a stronger research basis for the transition from scientific results to application-oriented research. In a similar vein, project-oriented research programmes could offer partners from industry an ideal opportunity to work with research institutes on developing future applications for quantum systems.

Example applications that have already sparked considerable interest from industry have come from e.g. the aerospace and security domains. Quantum communication is used for secure information transmission based on quantum key distribution, while quantum sensors have applications for satellite-supported earth monitoring, exploration, and navigation with gravimeters and atomic clocks (Airbus, OHB, SpaceTech, etc.). Industrial firms such as Bosch, Siemens, TRUMPF, or Volkswagen are primarily interested in optimising processes using quantum annealing. Quantum information systems in aviation applications have enormous potential, e.g. optimising flight paths in the heavily utilised transatlantic airspace, incorporating wind-optimised trajectories.

In order to ensure a dynamic research ecosystem from basic research through to launching applications on the market, we need over the coming years to be intensifying the process of transferring research results into engineering research and the corresponding technical trades.

5.5 Leibniz Association

The Section D departments – maths, natural science and engineering – of the Leibniz Association institutes are carrying out diverse research and development work in the field of quantum technologies. The institutes involved are:

- The Ferdinand-Braun-Institut, Leibniz-Institut für Höchstfrequenztechnik (FBH) in Forschungsverbund Berlin e.V (Berlin Research Association), Berlin
- Leibniz Institute for Solid State and Materials Research Dresden (IFW), Dresden
- IHP GmbH – Innovations for High Performance Microelectronics, Frankfurt/Oder
- Leibniz Institute for Crystal Growth (IKZ) in Forschungsverbund Berlin e.V., Berlin
- Leibniz Institute of Photonic Technology (IPHT), Jena
- Max Born Institute for Nonlinear Optics and Short Pulse Spectroscopy (MBI) in Forschungsverbund Berlin e.V, Berlin
- Paul-Drude-Institut für Festkörperelektronik (PDI) in Forschungsverbund Berlin e.V, Berlin
- Weierstrass Institute for Applied Analysis and Stochastics (WIAS), Leibniz Institute in Forschungsverbund Berlin e.V, Berlin

The quantum technology research topics at these institutes are mainly based on photonic technologies; they range from basic issues such as quantum coherence through to diverse topics in the "enabling technologies" domain – materials, components, modules, ... – and beyond to systematic problem formulations in the fields of quantum sensor technology, metrology and communication. The institutes boasting the largest number of quantum technology topics are FBH, IHP and IPHT, who cooperate closely with industrial partners in all their fields and also plan to offer application- and industry-ready solutions for quantum technologies.

The research activities at the institutes are still primarily restricted to their own networks and local connections, or close collaborations with the local universities. A strategy process was recently initiated at the level of the Leibniz Association, and the first result of this is the application for a Leibniz Science Campus in the Berlin area, "Photonic Quantum Technologies Berlin" (QuantecB). Research activities at this campus will be focused on quantum technologies within the Leibniz Association; in addition all the Berlin universities are actively researching in the field of photonic quantum technologies. The other relevant Leibniz Institutes, which are all located in the Berlin area, will be closely involved in the medium term with the development of the Science Campus.

In more detail, the eight institutes in Section D of the Leibniz Association are working on the following topics in quantum technologies:

The Ferdinand-Braun-Institut, Leibniz-Institut für Höchstfrequenztechnik (FBH) is researching electronic and optical components, modules and systems based on compound semiconductors, with a particular focus on high-frequency transmitters and light sources from the infra-red to UV range. It is an internationally recognised centre for III-V compound semiconductors, with all competences along the value chain from design to characterisation of semiconductor components, modules and systems.

The goal of the FBH's work on quantum technologies is to create mobile, energy-efficient electro-optical modules in various application areas with relevance to society, and bring them to maturity for field use. A prerequisite for this is reliably available miniaturised electro-optical modules with the desired functionality, which can be optimised with relation to size, weight, power consumption and costs (SWAP-C). FBH has a full mastery of the technologies central to this process – laser technology, III-V semiconductor technology and micro-integration technology – and is continually developing them further.

Following an internal competitive process within the Leibniz Association, the FBH has been awarded a permanent one-third increase in its core funding (approx. 4 million euros) from 2019. The institute will use this funding to develop a new research field: "integrated quantum technologies". The Institute for Physics at Humboldt University will be very closely involved with this. Three of its departments and two junior research groups are working on quantum technologies and already have very close links with the FBH. Combining the system expertise from HU Berlin with the technological skills and transfer expertise from the FBH – in particular, relating to semiconductor light sources – is expected to yield rapid realisation of mature modules and systems for photonic quantum technologies in industrial and space applications.

In June 2018, the FBH spearheaded a collaborative project with the MBI, the Heinrich Hertz Institute, the Fraunhofer Institute for Telecommunications and the three Leibniz Association universities in Berlin to apply for the Science Campus "Photonic Quantum Technologies Berlin" (QuantecB). The partners will pool their research and education in photonic quantum technologies here, focusing particularly on quantum communication and metrology. A range of highly relevant issues will be worked on: from basic experiments (e.g. on quantum coherence) through to solutions for a variety of technological issues in the field of "enabling technologies" – for example, creating photonic modules on mobile platforms – and systematic problems such as building and applying light sources for entangled photons that can be used in IR spectroscopy and microscopy. In the quantum communication field, a fully-operational quantum network is to be built, with secure links between the three Berlin partner universities and a testbed for investigating quantum components in fibre optic networks under realistic conditions. In addition to the research programme, an academic programme will be added to the existing Master's course in "Optical Sciences" at Humboldt University.

The Leibniz Institute for Solid State and Materials Research Dresden (IFW) is engaged in modern materials science based on a foundation of natural sciences, thus spanning the field from scientific insights in physics and chemistry to technical production of new materials and products. The IFW's research is investigating in particular semiconductors, magnetic materials and components which it may be possible to use in quantum technologies. A central question here is whether there are limits for the size of semiconductor quantum systems. This is not just about miniaturising – how well quantum structures scale up to ever larger networks is equally interesting. These studies will form a jumping-off point for investigations into the technical limits for the field of quantum information technology.

IHP – Innovations for High Performance Microelectronics is concentrating on researching and developing silicon-based systems and high-frequency circuits and technologies. Its work includes investigating new materials associated with these. It takes a vertical approach linking research on materials, technologies, circuits and systems along a single innovation chain. The resulting expertise can then be integrated into quantum technology research and development at various levels. The hardware systems are crucial elements here: they act as carriers, storage, transmitters and receivers for quantum information. Specific research focuses at IHP relevant to quantum technologies are based around developing new material systems from Group IV semiconductors, (cryogenic) SiGe/III-V microwave circuits for manipulating quantum systems, electronic-photonic integrated circuits on a SiGe or III-V base for controlling and manipulating light, and energy-efficient wireless sensor nodes based on cryptographic data protocols.

The Leibniz Institute for Crystal Growth (IKZ) is carrying out basic scientific and technical research on producing, growing, processing and defining physical and chemical characteristics of crystalline inorganic solids, especially semiconductor crystals, oxide crystals and fluoride crystals. The IKZ is able to research unique materials and make them available for quantum technologies. It has established a new centre for laser materials, where new types of crystals are available for generating and controlling light; without these, photonic quantum technologies would be impossible. The IKZ can also produce isotope Si-28 crystals with a very high purity, which represent a potential material basis ("semiconductor vacuum") for quantum computing.

The Leibniz Institute of Photonic Technology (IPHT) studies the scientific basis for highly sensitive, high efficiency and high-resolution photonic techniques and systems. The quantum detection department at IPHT is investigating nanometre-scale movements of electrical charges in organic materials such as cells, tissues and proteins. Its measurements help to answer fundamental biological questions and can be used to draw conclusions about potentially pathological alterations. Other research work into quantum technologies at the IPHT includes i) quantum photonics with light confinement, ii) single photon counters with superconductors, iii) superconducting qubits in digital circuits, iv) using optical magnetometers to detect axions v) superconducting quantum sensors.

The Max Born Institute for Nonlinear Optics and Short Pulse Spectroscopy (MBI) conducts basic research in the field of nonlinear optics and ultrafast dynamics arising from the interaction of laser light and x-rays with matter, and pursues applications that emerge from this research. The MBI operates a comprehensive experimental infrastructure for nonlinear spectroscopy and structural research in the ultrafast time range of atto- to picoseconds. Other quantum technology research is particularly relevant to creating a detailed model of the dynamics and coupling of coherent elementary excitations: two-dimensional THz spectroscopy, monitoring the field-driven transport through THz charge carrier emissions, and photon echo processes in the infra-red spectral range.

The Paul-Drude-Institut für Festkörperelektronik (PDI) is working on basic research in materials science and physics, towards micro and opto-electronic components based on new types of basic principles. The research has a particular focus on low-dimensional systems in nanostructured semiconductors. Low-dimensional systems have potential uses for quantum technology. For example, the PDI is researching polariton lattices in semiconductor microcavities, which may prove to be suitable for quantum simulations. This involves localising individual polaritons in the lattice structures.

The Weierstrass Institute for Applied Analysis and Stochastics (WIAS), Leibniz Institute in Forschungsverbund Berlin is researching applied analysis and stochastic processes in order to help solve complex problem loops from economics, science and technology. WIAS is a leading partner in the internationally recognised Berlin Applied Mathematics. WIAS partners from science and industry use its models and numerical processes for diverse applications. The mathematical methods are palpably relevant as "enabling technology" for quantum technologies – for example, they can be used for static or dynamic simulations of electro-optical modules for quantum metrology.

The research and development activities in the field of quantum technologies at these institutes will grow considerably over the next few years. The institutes will also be intensively driving the strategy process for the field, with the objective of making quantum technologies one of the key focuses for the Leibniz Association. It is the intention of the institutes to build on their varied competences and close collaborations with universities, technical colleges and industrial enterprises to act as a solid bridge for transforming basic research results into practical applications, particularly in photonic quantum technologies.

5.6 National Metrology Institute of Germany (Physikalisch-Technische Bundesanstalt, PTB)

The statutory mandate of the Physikalisch-Technische Bundesanstalt (PTB), Germany's national metrology institute, includes traceable measurements and providing services, including in the field of quantum technology. Examples of quantum technologies relevant for the PTB include high precision quantum standards for electrical variables (resistance, voltage), high precision sensors for magnetic fields, pressure, or temperature, single-electron pumps with a high degree of non-classical characteristics, and single photon sources and detectors for quantum radiometry and quantum cryptography. Other significant PTB research results include ultrastable and highly accurate clocks with a wide range of applications in communication, navigation and geodesy. The PTB has systematically scaled up its work on developing quantum metrology and quantum sensor technology during its regular strategic planning – this is due to the enormous commercial potential and anticipated demand from research and industry.

This accumulation of quantum technology competence at the PTB has been significantly reinforced by the systematic establishment of a successful research network in Lower Saxony and across the globe. Through the network, innovative concepts have been implemented and quantum technologies successfully transferred into industry, generally as part of public funded projects (e.g. special research areas, and a Cluster of Excellence). A sustainable R&D infrastructure has also been developed through links created between the PTB research programme and the other partners (Leibniz University Hanover, the Max Planck Institute for Gravitational Physics, the Center of Applied Space Technology and Microgravity, Laser Zentrum Hanover, Technical University Braunschweig). Two new research buildings have also been created: the "Hanover Institute of Technology" (HITec) at Leibniz University Hanover and LENA (the Laboratory for Emerging Nanometrology) at TU Braunschweig. Here, universities and the PTB pool their expertise and collaborate on developments in metrology and quantum sensor technology for applications beyond the laboratory. Joint appointments to junior professorships will strengthen the expertise in the field of key components for quantum technologies and boost research on exploiting quantum effects in nanostructures and optical nanomaterials in metrology and sensor technology. There are furthermore numerous research projects and networks at the European and international level working on the various aspects of metrological quantum technologies and their industrial applications (see Section 3.5), including the MPQ (Garching) and MPIK (Heidelberg) Max Planck Institutes.

This long-term strategic development facilitates comprehensive support for industry and means major projects can be carried out in conjunction with other research facilities. Some of these activities are described below, along with how a new Centre of Excellence for Quantum Technologies to open at the PTB will provide added value for the external partners.

The activities cover the fields described in Section 3 – components and technology, calibration and services, and application platforms on the one hand; business incubators, training, public relations and technology transfer on the other.

Electrical quantum metrology

The PTB is the only national metrology institute in the world with complete production lines for superconductor and semiconductor quantum standards and electrical quantum standards based on graphene layers. The PTB has been able to build on this foundation to establish its position as a global leader in the field of electrical quantum standards. It has already carried out successful technology transfer projects in cooperation with and to support German SMEs. Today's quantum-based electrical measurement technology only covers a small number of electrical variables over narrow value and frequency ranges, and relies on expensive apparatus which requires expert knowledge to operate. If industry is to profit in the medium term from the intrinsic advantages of quantum-based electrical measurement technology – high precision measurements round the clock with no need to pause for recalibration – it is essential to simplify operating conditions and improve usability via automation. The planned Centre of Excellence will position the PTB to systematically investigate and develop new materials to simplify the operating conditions for electrical quantum standards. Furthermore, a permanently financed Centre of Excellence will make it possible to dynamically drive progress in developing highly integrated electrical quantum circuits, thereby making them accessible to a wider range of variables, values and frequencies. At the same time, work on improving user-friendliness and automation of quantum-based electrical measurement technologies can be developed in the context of close collaborations with industrial partners.

The first steps towards implementing the Centre of Excellence for Quantum Technology represent an important contribution towards opening up production technology for superconductor and semiconductor quantum standards. This will boost technology transfer activities in this field, in parallel with paving the way for building user platforms for small batch production of quantum systems based on solids.

Quantum metrology for time and frequency, quantum computers and quantum simulation

The PTB is a worldwide research leader in the development of optical atomic clocks and their associated peripherals – microstructured atom traps, ultrastable lasers, fibre optic routes for frequency transmission and portable optical clocks. Collaborations with German SMEs in the context of technology transfer projects and the BMBF quantum technology pilot project "Opticlock – Optical single ion clock for users"[43] have been building on this foundation, and some individual components and entire portable clock systems have already been developed. The first applications for transportable clocks in the field of geodesy have been demonstrated through public-funded projects. Microstructured ion traps for scalable optical clocks will also be developed and manufactured at the PTB, using techniques from the semiconductor industry. German industry is currently particularly active in the field of key components for quantum technologies. This includes developing lasers and specialised active and passive optical components. There is a significant need here for a transfer of system competences, supported by high-level measurement technology, validation and characterisation of components. Relevant processes, for example in the field of developing atom traps, are complex and require not only expert knowledge but also a costly apparatus infrastructure, which SMEs are not able to implement without support. Through the Centre of Excellence, the PTB will position itself to work with industry on developing time and frequency based components, thereby opening up new applications. PTB validation of key components, prototypes and manufactured devices would provide a major boost for German industry's competitiveness on the international stage in this field. Providing production capacity in Germany and Europe for atom traps and their subsequent transfer into industry is also highly relevant to developing quantum computers based on trapped atoms.

The establishment of strategic partnerships with e.g. the Fraunhofer institutes, who have appropriate competences in materials and optics, will set the stage for miniaturising key active and passive optical components, and integrating them into quantum sensors.

43 http://www.opticlock.de

There are also key links into the planned activities at the DLR Institute for satellite geodesy and inertial sensing in Hanover, as well as in the field of optical free radiation transfer of data (DLR), time and frequency (PTB).

In addition, key components for quantum technologies will be developed with reference to operating stability, long-term deployment, and operation by inexperienced users; at the same time, the existing measurement infrastructure and characterisation setups will be extended in collaboration with industry.

Measuring tiny magnetic fields

One quantum technology that is already being applied makes use of the principle of superconducting quantum interferometers (SQUID – Superconducting Quantum Interference Device) to carry out ultrasensitive magnetic field measurements and highly sensitive measurements of physical variables that are changed by magnetic currents, e.g. electrical current. SQUID magnetometers have been in use for years to measure the tiny magnetic fields generated by neural activity in the human brain (MEG – magnetoencephalography). The PTB, and other institutes, are making progress on other new biomedical analysis and diagnostic methods that use these quantum sensors.

In addition to SQUID magnetometers, SQUID current sensors have become an enabling technology that can be used in quantum communication for single photon detectors – as well as numerous experiments in the context of basic research.

The PTB has an internationally unique infrastructure for superconductor thin layer technology and special measurement techniques. It operates an equipment centre funded by the DFG, where external users can have access to quantum-based magnetic field measurement techniques for ultra-low magnetic fields.

Superconductor sensor developments have already been commercialised to a limited extent by the PTB as part of a technology transfer in response to the demand for suitable components and complete systems. This infrastructure will be extended in the Walther-Meissner building currently under construction at the Berlin campus.

A Centre of Excellence will make a crucial contribution to systematically bringing superconductor technology to a wider, primarily industrial consumer base and providing support to SMEs who are developing products in this field. One of the hurdles here is that, unlike semiconductor sensor technology, standardisation is still at a very early stage when it comes to the technological processes, electronic parameters, measurement procedures, calibration instructions, and so forth. Via the Centre of Excellence, users and companies can be briefed with appropriate skills, calibration instructions, information about handling the sensors, etc. SMEs who are active in this field, or who would like to be, are generally not able to afford an extremely costly infrastructure with production technology in clean rooms, magnetic or high-frequency shielded cabinets, reference systems, and sensitive electronic measurement technology – certainly not when they are setting out. A centre of excellence represents a valuable starting point for these companies.

It is not crucial to the practical use of superconductor sensor technology to have a sensor chip with the maximum values: the essential is a complete, robust, measurable system. For this reason, it is important to bring together competences from the fields of sensor electronics, cooling technologies, electromagnetic shielding and peripheral measurement technology. These special expertises can be efficiently developed, maintained, and shared through the Centre of Excellence.

Quantum communication, quantum cryptography and quantum radiometry

The PTB calibrates single photon detectors, for example silicon and indium gallium arsenide single photon avalanche diodes, or superconducting nanowire detectors with the smallest measurement uncertainty in the world. In addition to this, the PTB is developing absolutely characterised single photon sources as new standard radiation sources for radiometry and quantum communication. For comprehensive implementation of quantum communication and quantum cryptography, it is essential to have a precise characterisation of the sources, detectors and transmission channels. This means that if industrial products are to be distributed in this field, it is important that they can be anchored in national standards. Through the Centre of Excellence, the PTB will be in a position to offer manufacturers and users traceable and reliable measurements in the fields of quantum communication, quantum cryptography and quantum radiometry. An additional consequence of this is that consumers will be able to test components of quantum cryptography and begin to familiarise themselves with the use of such components as part of their working day.

In this way, the Centre of Excellence will drive development of the field of metrology into the domains of quantum communication, quantum cryptography and quantum radiometry; this will result in better characterisations of the components that are being used. New single photon sources will also be developed as standard sources, thereby guaranteeing the metrological basis of a comprehensive implementation of quantum communication.

5.7 Federal Office for Information Security

Primary activities

The Federal Office for Information Security (BSI) began studying the effects quantum computers could have on contemporary IT security infrastructures some years ago. To help to clarify the German position on this issue, the BSI carried out a feasibility study into cryptographically relevant quantum computers.[44]

In parallel with this, a study on lattice-based cryptography was carried out as preparatory work for decision making about future cryptographic algorithms for resisting decryption attacks using quantum computers. The BSI is pushing forward standards development for the future migration to new algorithms and in order to achieve cryptographic agility. It is furthermore actively supporting standardisation of hash-based signatures for quantum-secure software downloads.

In particular, the BSI is actively supporting the following research elements:

Quantum computing and simulation: the security of modern digital infrastructures is fundamentally dependent on public key cryptography. The procedures that are commonly used are based on the assumed difficulty of certain mathematical problems. The public key procedures that are used today (provided they are implemented correctly and with the right key size) cannot be broken with the currently available tools. However, algorithms have been described that could break these procedures using quantum computers, and thus destroy the basis of modern public key cryptography. With symmetric procedures, the key length needed to protect against potential attacks from a quantum computer will approximately double ("Grover's algorithm").

In order to counter this phenomenon, the BSI is supporting research in the field of "post-quantum cryptography". This is focused on using "traditional" computers to develop and explore cryptographic procedures that will not be breakable with quantum computers. Quantum cryptography, by contrast, is working in the other direction: to exploit quantum effects for cryptographic applications.

The BSI is heavily involved with the international standards selection process for post-quantum cryptography, which is being led by the National Institute of Standards and Technology (NIST) in the USA. A number of implementation and standards requirements for future crypto-agile products have already been derived. One of the key themes is the use of "hybrid" processes, which combine traditional procedures with suitable quantum computer resistant solutions. The BSI is also supporting the standardisation of protocols for hybrid key exchange and signing. It provides advice to manufacturers of cryptographic products and is introducing a migration process for the high-security domain.

Over the next few years, the study mentioned at the beginning of this section will be updated based on the latest research and developments in quantum computing. The primary result of the study is an evaluation model that can be used to classify the current technologies for building quantum computers in terms of what stage of development they have reached. This study forms the basis of the BSI's future work in this area.

Several information research groups are currently working intensively on the security and feasibility of post-quantum cryptography. As part of the Horizon

44 https://www.bsi.bund.de/qcstudie

2020 programme, the EU is currently funding the European projects "PQCrypto" – which numbers the BSI among its advisory board members – and "SAFE-crypto".

TU Darmstadt has carried out a study commissioned by the BSI on "The evaluation of lattice-based cryptographic procedures". The goal of the study was to draw up an analysis of recent publications on lattice-based public key procedures (key exchange, signature and encryption).

The BSI is sponsoring the implementation of quantum computer resistant cryptographic algorithms in selected crypto libraries[45]. It is not yet possible to predict what new cryptographic attacks could be possible using quantum computers or quantum simulators. However, applications are beginning to emerge for side-channel attacks and possible ways of combining traditional cryptographic attacks with quantum-based attacks. These developments are being closely tracked by the BSI, funded as research topics and covered in the BSI's technical guidelines.

Quantum computing: the topic of quantum computing is extremely interesting from a cryptographic point of view. The interaction between quantum computers and algorithmic developments is particularly relevant in the light of emerging quantum computer supported cryptographic attacks. The BSI is actively involved in research projects in this area.

Quantum communication: quantum communication, in particular using quantum mechanical effects to assist the distribution of cryptographic keys (QKD), is a technology that promises secure data transfer on the basis of physical principles rather than mathematical assumptions. QKD requires a second, classical, authentic channel. In order to be able to evaluate the security of quantum communication products, the BSI is working together with manufacturers, testing centres, the scientific community, bodies such as the PTB, and consumers to develop testing criteria. Its framework covers criteria for evaluating of security against side-channel attacks.

Random number generation: secure random number generation is a secondary field highly relevant to quantum projects. It has been listed as an important research field, as pseudo-random number generators are subject to criticism. The BSI provides comprehensive technology-neutral criteria for evaluating random number generators (AIS 20, AIS 31). AIS 20 and AIS 31 are mandatory in the German certification scheme (Common Criteria) and in principle also applicable for evaluating quantum random number generators. The BSI supports the development of quantum random number generators that meet the current requirements for physical random number generators, and if necessary will develop specific additional requirements for certification and authorisation of quantum random number generators.

Collaboration: in order to properly address the effects of quantum technology on IT security, it is important for numerous actors from the diverse scientific fields (physics, computer science, mathematics), industry and the authorities to work together. The BSI will continue to develop and build up its contacts in this collaboration network.

5.8 Agency for Innovation in Cybersecurity

On 29 August 2018, based on a proposal from the Federal Minister for Defence and the Federal Minister of the Interior, for Building and Community, the cabinet agreed the foundation of an "Agency for Innovation in Cybersecurity" in the legal form of a GmbH. The agency's purpose is to finance and support ambitious research projects with high innovation potential in the field of cybersecurity and related key technologies, in order to meet the country's needs in terms of internal and external security. The agency will support innovative projects that are distinguished by radical technological novelty and could consequently have game-changing repercussions.

45 https://www.bsi.bund.de/DE/Themen/Kryptografie_Kryptotechnologie/Kryptografie/Kryptobibliothek/kryptobibliothek_node.html

Published by
Bundesministerium
für Bildung und Forschung /
Federal Ministry of Education
and Research (BMBF)
Division Quantum Systems; Postdigital Computers
53170 Bonn
Germany

Orders
in writing to
Publikationsversand der Bundesregierung
P.O. Box 48 10 09
18132 Rostock
Germany
Email: publikationen@bundesregierung.de
Internet: www.bmbf.de
or by
Phone: + 49 (0) 30 18 272 272 1
Fax: + 49 (0) 30 18 10 272 272 1

September 2018

Edited by
BMBF

Layout
ecosense – media & communication
Cologne, Germany

Printed by
BMBF

Photo credits
Cover, p. 2, p. 3: © panthermedia.net/agsandrew
p. 4: © BMBF
p. 5: © IQST @ Universities of Stuttgart & Ulm
p. 7: © Fraunhofer IOF
p. 8: © IQST @ Universities of Stuttgart & Ulm
p. 9: © University of Siegen
p. 10: © University of Münster
p. 12: © Fraunhofer IAF
p. 13: © TOPTICA Photonics AG
p. 15: © IQST @ Universities of Stuttgart & Ulm
p. 16: © rocketclips/fotolia
p. 18: © QUARTIQ GmbH
p. 20: © Enno Kapitza for DLR
p. 21: © zapp2photo/fotolia
p. 23: Satellite: © SpaceTech GmbH/Earth: © PaulPaladin/fotolia
p. 24: © sdecoret/fotolia
p. 25: © Fraunhofer IOF
p. 27: © Physikalisch-Technische Bundesanstalt
p. 29: © Leibniz-Gymnasium Dormagen
p. 30: © VDI Technologiezentrum GmbH/Bert Willer
p. 31: © University of Paderborn
p. 32: © Jacob Lund/fotolia