Metis

Study

Quantum technologies: Implications for security and defence

No. 25 | May 2021

The views expressed in Metis Studies are those of the authors. They do not reflect the opinion of the Bundeswehr, the Federal Ministry of Defence, or the Bundeswehr University Munich. The primary target audience of Metis Studies are practitioners. Metis Studies are based on analyses of scholarly literature, reports, press articles and expert interviews with academics, think tank analysts and policy-makers. References are omitted. Inquiries about sources can be directed at the author(s) via email.

Institute for
Strategy & Foresight

Summary

Strange as they may appear, the special properties of quantum mechanical processes have been studied for more than a hundred years. Thanks to advances in our ability to manipulate them, we can now increasingly utilise them for technical applications. There are high hopes pinned to this development but the chances of success are still uncertain. This study presents the state of research in four areas of quantum technology, looks ahead at possible security and military implications, and concludes with a number of recommendations for action.

Quantum this, quantum that

Will weapon systems equipped with quantum sensors soon engage in quantum-encrypted communications with quantum computers via a quantum internet and thus bring about a military quantum jump? Google's October 2019 announcement that it had successfully demonstrated "quantum supremacy" (see below) over classical supercomputers fanned the smouldering embers of the debate surrounding the disruptive potential of quantum technology when used for military purposes. Since then, many a neologism has been coined with the "quantum" prefix.

The truth is that quantum technology is rather unlikely to revolutionise security policy by 2030. At least this is what expert surveys conducted in 2020 suggest. According to these surveys, there are numerous other, more mature emerging and disruptive technologies that are currently much more relevant in terms of military strategy than quantum technologies (Fig. 1).[1]

It is also true, however, that breakthroughs in quantum-based computing, sensor technology and encryption methods *could* indeed entail a considerable increase in capability with wide-ranging security implications and that measures to counter such potential developments are still at a theoretical stage of development.

Overall, it therefore seems that, in addition to keeping a calm eye on developments in the field of quantum technology from a security policy perspective, we should also start contemplating active measures in certain areas.[2]

Why quantum computers?

The success of the classical computer is based on miniaturisation. Production costs decreased while performance increased. But we are now approaching a physical limit.

The current industry standard for processors is based on components that measure as little as 7 nanometres (nm) along the edge. That is equivalent to 7 billionths of a metre, which is twelve times smaller than a single coronavirus, 1,200 times smaller than a red blood cell, and 12,000 times smaller than a human hair. Future chip generations will have components with feature widths of two nm.

Theoretically, however, this extremely successful miniaturisation strategy of classical computers can only continue until the smallest functional components on a chip eventually only consist of a single atom. After that – at least according to what we know today – their design is likely to reach its absolute limit. This is because in the subatomic realm, quantum mechanical effects come into

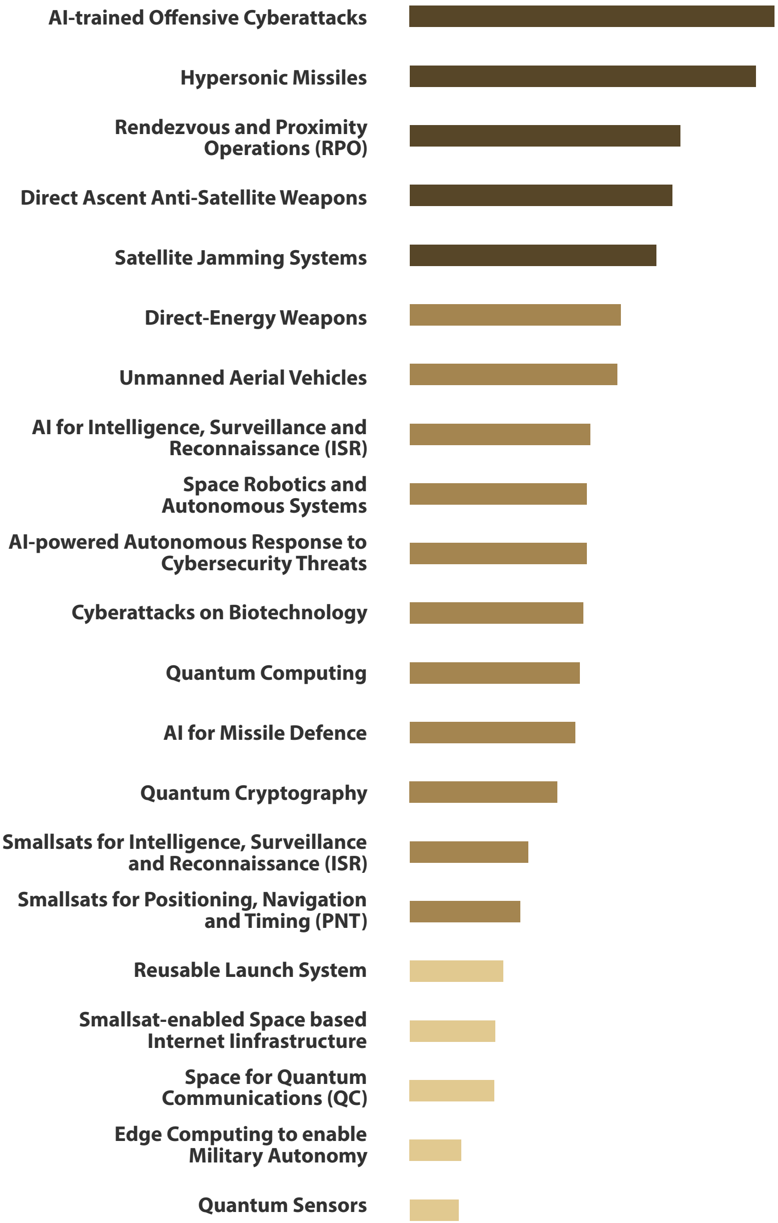
[1] Marina Favaro based these expert surveys on the Systematic Technology Reconnaissance, Evaluation, and Adoption Methodology (STREAM), which was developed by the RAND Corporation and which serves to systematise, prioritise and assess current and future technologies on the basis of a range of effects and implementation criteria.

[2] See "Great powers and digitisation: What are the implications for world order?", Metis Study No. 8 (October 2018).

conflict with the functional principles of computers, as we know them, which are based on classical physics.

Not least because of this, interest in quantum computers has been growing since the 1990s. They have since made their way from the theoretical research stage through experimental practice to data processing centres and cloud-based computing for limited commercially available trial applications.

***Fig. 1** New and emerging technologies ranked in order of their potential to disrupt strategic stability.* | Source: Marina Favaro, in: The 2020 UK PONI Papers, Royal United Services Institute



Research in the field of quantum mechanics was already fundamental to the development of modern 20th-century technologies such as microelectronics and laser. However, as with computer chips, these technologies utilised macro-physical phenomena. Quantum technology, on the other hand, relies specifically on physical effects on the scale of individual atoms and below. Quantum computers therefore continue the principle of miniaturisation on the next lowest level by utilising the fundamentally different physical principles that apply on that level for computer operations.

Superposition is the first such phenomenon used for this purpose (Fig. 4). It involves superposing different states. Quantum computers use superposition in quantum bits (qubits), which, unlike classical bits with their two discrete states (1 or 0), can take on all states between 1 and 0 at the same time. Quantum computers thus offer enormous parallel computing performance compared with classical computers. They are also better at scaling – at least in theory – because ideally every additional qubit doubles the computer's performance, which thus grows exponentially. With computing tasks of exponentially increasing complexity, quantum computers develop solutions *quickly* (in seconds or minutes) where even the biggest classical supercomputers would need too much time (tens of thousands of years). This is what is commonly understood by the term "quantum supremacy" – and it is something Google claims to have demonstrated in 2019 with its 53-qubit quantum processor Sycamore, using a purely academic computing problem specifically tailored to the strengths of quantum computers.

The second phenomenon utilised in quantum computing is entanglement (Fig. 5). Entanglement means that two or more particles are linked with each other, i.e. they can represent the same state, even over long distances. The numerous possibilities for flexibly manipulating such entangled qubits contribute to the speed with which a quantum computer is able to handle complex computing problems.

Quantum computers also produce large quantities of data with high error rates, however. These high error rates occur partly because the smallest variations in temperature, for example, disrupt the delicate quantum-mechanical states of qubits. And so the challenge is to increase the number and lifespan of qubits while implementing more effective error correction mechanisms in order to achieve the desired computation result, i.e. to discern the correct signal from the loud "data noise" of the quantum computer. Noisy intermediate-scale quantum (NISQ) technology for quantum computers with 50 to 100 qubits is currently regarded as an interim solution on the way towards developing less noisy computers with more qubits, the idea being that this will finally allow for broader and truly practice-relevant applications of quantum computing. From the current perspective, it seems that would probably require up to 1 million qubits. At present, IBM is aiming to exceed the 1000-qubit mark by 2023. And so there is still a very long way to go.

To make things even more difficult, the two currently dominant designs – circuits made of superconductive metals (used by companies such as Google, IBM and Rigetti Computing) and ion traps (used by companies such as Honeywell and IONQ) – scale poorly in practice. This is due to the control systems for the fragile and rigorously protected qubits. The design based on superconductivity (Fig. 2) uses microwaves for programming purposes but must keep all its qubits cooled down to almost absolute zero, i.e. -273 °Celsius – a complex and expensive process. In contrast, systems with qubits from charged atoms kept suspended in a vacuum by magnetic fields work at room temperature but need laser systems for programming, which cannot be miniaturised beyond a certain point.

In summary, it is clear that the already incipient practice of simultaneously using both classical computers and quantum computers that are limited to highly specialised test applications will continue for the foreseeable future. This is because there are numerous difficult hurdles to overcome before quantum computing can be used on a widespread basis (by miniaturising mass-producible architectures). It could well be that none of the two designs described above will win the race and that one of the many alternatives currently being developed will instead prevail as a hardware platform for quantum computers. Sceptics note that quantum computers could face the same fate as atomic fusion. Decade after decade, that technology has been predicted to finally have its breakthrough. But this breakthrough never seems to materialize.

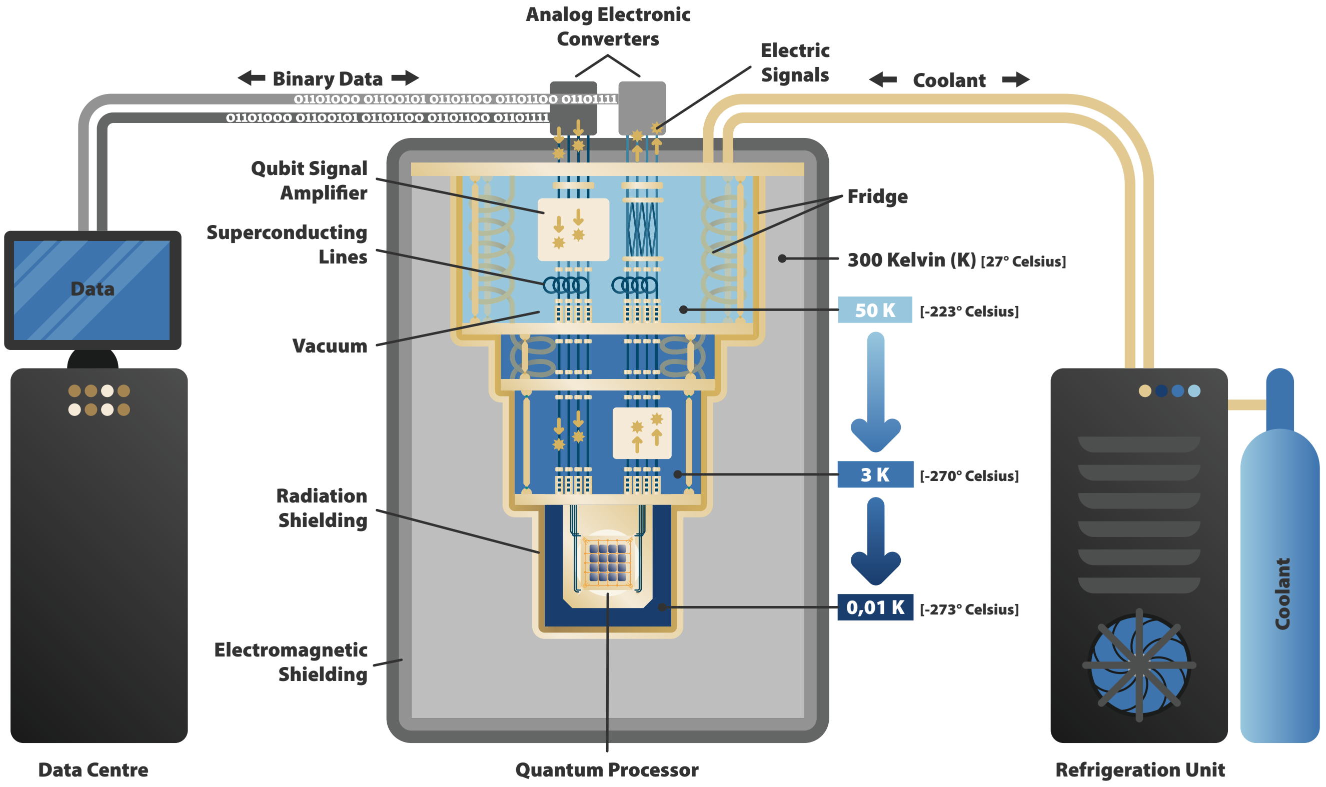


Fig. 2 Schematic representation of superconducting quantum computing. | Source of template: VectorMine on shutterstock.com

Fig. 3 ***Scientist in an IBM quantum lab.*** | Source: flickr.com/photos/ibm_research_zurich/; Credit: Connie Zhou for IBM

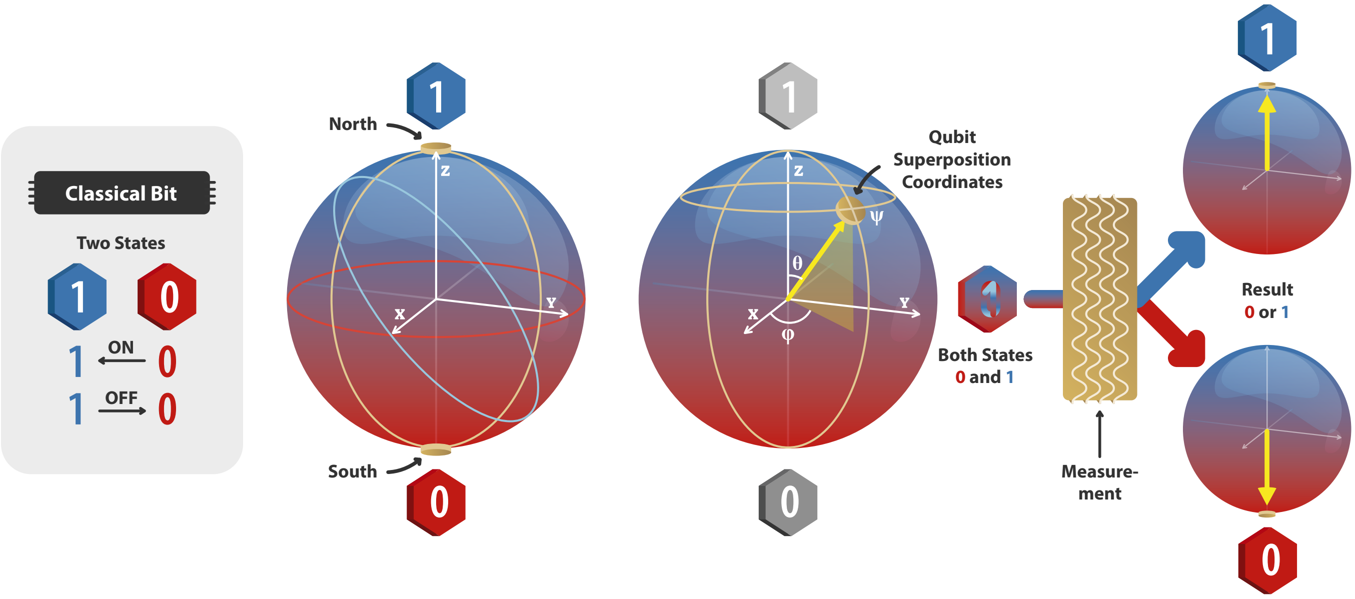


Fig. 4 Schematic representation of computing with qubits. | Source of template: VectorMine on shutterstock.com

Security implications

The drivers behind the development of quantum technology are scientific and commercial in nature. But breakthroughs in the field could also develop far-reaching implications in terms of security and defence – not in the form of a singular event, as with the development of the atom bomb, but due to their broad effect. If its promise were to become reality, the role of quantum technology would be that of a massive trend amplifier in the pursuit of information supremacy. It could affect the entire spectrum of leadership, information, communication, computer systems, intelligence, surveillance and reconnaissance. Concrete prospects include increased precision, efficiency and automation.

Cryptocommunications

The quantum phenomenon of entanglement can be used to encrypt communications. In this context, it is often said that quantum-entangled communications are impossible to intercept without obvious disruption and so *unnoticed* listening would be physically impossible. This sounds promising and is correct in theory.

But it is tricky to put it into practice and the technology is not yet fully operational. Previous demonstration projects either worked only via short fibre-optic cables or required a large number of repeaters (for which researchers consider satellite constellations the most efficient solution). In addition, quantum-encrypted communications prove vulnerable to side-channel attacks, which target not the cryptographic system itself but its practical implementation in an application environment in order to get to the information unnoticed via side channels.

Even if there were to be a breakthrough towards widespread application of quantum-encrypted communications soon, i.e. by the end of this decade, the implications would be manageable – at least from a narrow security perspective, i.e. one focused on military aspects.

Sensor technology

Sensor technology is the area of quantum technology with the highest number of concrete, already usable applications. Unlike quantum computers, quantum sensors do not require large numbers of entangled pairs of particles. Considerable advances over the last two decades when it comes to the production and manipulation of the quantum states of particles also mean that research has got a better handle on “noise”, which of course affects precise measurements. Much like in the field of computers, a variety of different physical principles and designs are also being pursued simultaneously.

With quantum sensors, mass, time, place, speed, acceleration and electromagnetic field strength can be measured more accurately – by several orders of magnitude – than with classical sensors. Spatial resolutions in the nanometre range are possible. Quantum clocks make it possible to synchronise processes precisely. Quantum gyroscopes for inertial navigation systems and quantum sensors for measuring earth's magnetic field can make autonomous mobility possible without having to rely on GPS or other satellite navigation systems. Compact quantum magnetometers that work at room temperature are currently being developed. These could be used in areas ranging from submarine detection to brain-computer interfaces.[3]

Speculations regarding a powerful Chinese quantum radar that could soon render stealth technology obsolete (as security policy circles in Washington feared a few years ago) cannot be confirmed, at least not on the basis of available open sources. This was recently emphasised again by the Pentagon's Defense Science Board.

The broad field of quantum sensor technology is the one approaching military usability the fastest. However, it is impossible to predict with any certainty which sensor technology will be ready to go into production when and which will find its way into the field of security and defence. Because of the sheer number of areas of application that could be affected by quantum sensor technology, this study cannot possibly predict the many possible implications.

Cryptanalysis

Established cryptographic methods take advantage of the fact that certain mathematical problems cannot be solved in a reasonable time frame with classical computers. As outlined above, quantum computers have the potential to introduce a paradigm shift in this respect by very quickly decrypting databases that, by present standards, have been securely encrypted. Stored data sets that so far have been impossible to decipher could also suddenly be disclosed.

At the moment, this is just a theoretical scenario. Nevertheless, ideas for quantum-computer-resistant encryption methods for the world of classical computers and the internet are already being discussed. In 2016, for example, the National Institute for Standards and Technology (NIST) in the US already initiated a process to develop and standardise such methods and make them available. The first results for such quantum-computer-resistant encryptions are expected in 2022/2023.

We cannot entirely rule out that the previously mentioned sceptics are right and that some of the promises associated with quantum computers will be a long time coming – if they come at all. But in view of the progress that has been made in just under three decades, of the prototypes and special applications that already exist, of the investments already made, and, last but not least, of all the talent and time that has been dedicated worldwide, it is much more likely a question of "when" rather than "if".

Based on this assumption, we can infer far-reaching security implications when it comes to cryptanalysis. Any and all sensitive communication would then have to be comprehensively protected as quickly as possible by changing over to quantum-computer-resistant encryption methods.

[3] See "Conventional arms control and emerging technologies", Metis Study No. 20 (September 2020).

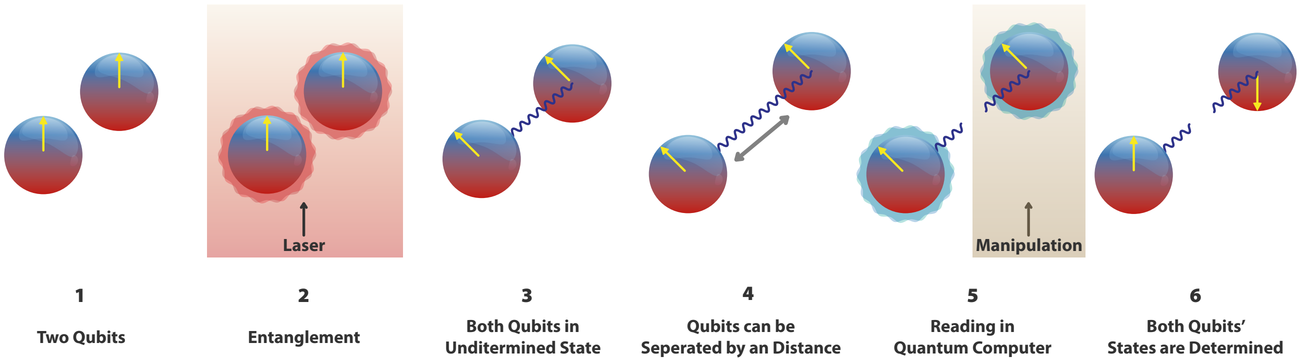


Fig. 5 Schematic representation of entangled qubits. | Source of template: VectorMine on shutterstock.com

Summary and recommendations for action

The US, China, the UK and India have launched support programmes for quantum technology, while the EU is running a flagship project and intends to provide funds of up to €1 billion. Partly in order to counter the economic crisis caused by the COVID-19 pandemic, the German Government in June 2020 agreed on a stimulus package that also includes specific provisions for quantum technology. Sums totalling €650 million are being made available in the current legislative period alone. Research in Europe and Germany in particular has thus far kept pace with world leaders in the field, thanks to government funding, traditionally good scientific training, and a number of existing technological centres of excellence.

In the fields of security and defence, the hype around quantum technology outlined earlier will soon subside for the time being. At least that is what previous experience with other new technologies suggests. And since social and political factors such as culture and regulation are in constant interaction with technological development and application, development will not be linear anyway.

At the same time, however, this study has shown that a wait-and-see approach is not an option and that important questions need to be addressed now. There are three recommendations for exploring possible courses of action in the short, medium, and long terms.

- Quantum-computer-resistant cryptography will become the standard. The German Federal Ministry of Defence needs to act now to plan and assess how long it would take to implement appropriate encryption methods in its area of responsibility. If a breakthrough in quantum computers – and hence an end to classical encryption – were to happen before this process is completed, the consequences for classified information would be disastrous. It is important to remember that any data already collected by our enemies by that point – even if currently still encrypted – would then also have to be considered compromised.

- In the medium term, the Bundeswehr should systematically explore the concrete impact that any breakthroughs in the field of sensor technology could have on the military. It should do this on a national level but also with partners in the EU and NATO as well as with institutions of applied research and industry. What new capabilities could a potential enemy gain through individual applications and which of the Bundeswehr's own capabilities could become obsolete? What would the implications be for planning, procurement and interoperability? What sort of instruments of arms control and export policy can we develop in order to exert influence? Scenario workshops provide a possible format for such discussions.

- What is needed in the long term is a broad national conversation about what a breakthrough in the field of quantum computers would mean for the future of humanity. As we have established, the end of classical encryption is just one possible consequence. The availability of quantum computers could also bring about a revolution in pharmacy and materials science, to name just two examples. However, progress in the field of artificial intelligence, which, thanks to machine learning, is already booming [4], would likely also be accelerated. This would make it possible to conduct efficient simulations and to optimise countless procedures. Against this backdrop, the international research community has already begun to discuss "quantum ethics": what legal, political and social frameworks are needed to deal with the existential risks that the quantum era might entail?

[4] In this context, artificial intelligence is understood as the multitude of different computer-based technologies and methods used to automate tasks that have thus far required the use of human intelligence.

Metis

IMPRINT

Publisher

Metis Institute
for Strategy and Foresight
Bundeswehr University Munich
metis.unibw.de

Author

Dr. Frank Sauer
metis@unibw.de

Creative Director

Christoph Ph. Nick, M.A.
c-studios.net

Image credits

Cover: IBM Q Quantum Computer. | Source:
flickr.com/photos/ibm_research_zurich/;
Credit: Graham Carlow

Original title

Quantentechnologie: Implikationen für Sicherheit und Verteidigung

Translation

Federal Office of Languages

ISSN-2627–0609